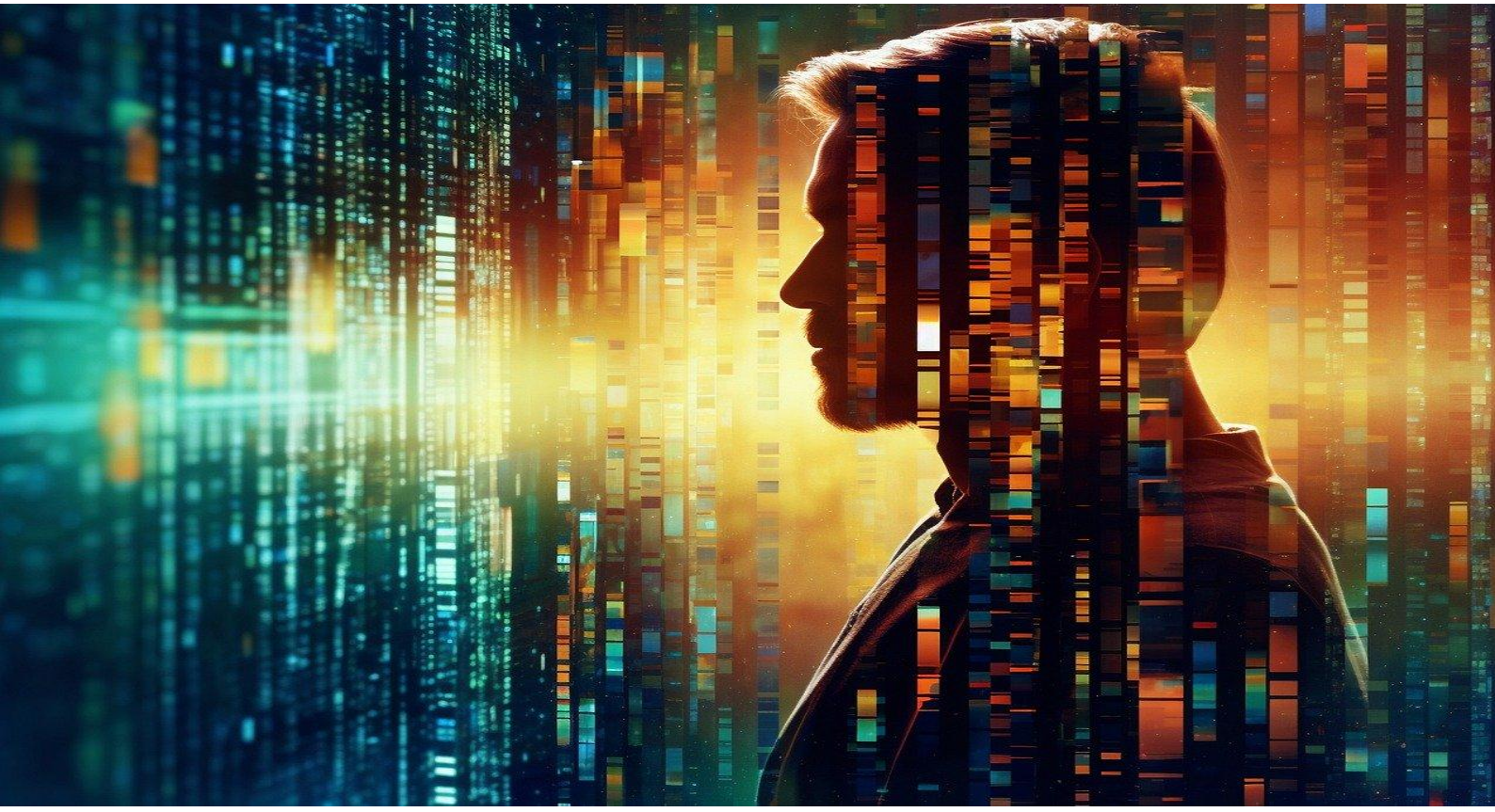
INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

GUIA

CONFLITO DE INTERESSES NA FUNÇÃO DO ENCARREGADO DE PROTEÇÃO DE DADOS – DPO



Elaboração:

Selma Carloto

Autora e coordenadora de diversas obras e artigos de Lei Geral de Proteção de Dados, Compliance Trabalhista e Inteligência Artificial. Professora autora de Proteção de Dados da Fundação Getúlio Vargas (FGV). Pós-doutora pela Universidade Federal do Rio Grande do Sul (UFRGS). Doutora em Engenharia da Informação, Inteligência Artificial, pela Universidade Federal do ABC (UFABC). Doutorado em Direito do Trabalho pela UBA. Mestre em Direito do Trabalho pela Universidade de São Paulo (USP) Faculdade de Direito. Professora convidada da Fundação Getúlio Vargas da FGV Direito Rio e professora da FGV de MBA. Presidente da Comissão de Temporalidade do Instituto Nacional de Proteção de Dados (INPD).

Mario Toews

Sócio fundador da Datalege Consultoria Empresarial; profissional com mais de 25 anos de experiência como gestor de TI de grandes empresas como Renault do Brasil e Renault Argentina, Arauco, Martini Meat e Britânia; coordenou diversos projetos de implementação de Sistemas, ERPs, Business Intelligence e Infraestrutura; reorganizou as áreas de TI, conduziu a atualização tecnológica e a implantação de políticas de segurança da informação em diversos níveis. Graduado em Análise de Sistemas com Especialização em Direito Digital, Pós-Graduação em Gestão Administrativa e MBA em Gestão Estratégica de Empresas pela FGV. Diretor de Segurança da Informação e DPO substituto do INPD (Instituto Nacional de Proteção de Dados). É instrutor certificado (ISFS, PDPF, PDPP, DPO, ISO, ISMP, Kanban, AICP) pela Exin Internacional.

O Conflito de Interesses na Função de Encarregado (DPO) com Base na Resolução 18 da Autoridade Nacional de Proteção de Dados (ANPD) e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia

Sobre o INPD:

O Instituto Nacional de Proteção de Dados tem como missão disseminar o conhecimento sobre proteção de dados e privacidade, fomentar debates, pesquisas, eventos e viabilizar o diálogo entre titulares de dados, empresas e Poder Público, influenciando a construção de um ecossistema sustentável e respeitando direitos humanos.

Imagem de Capa: Franganillo, em pixabay.com

Histórico de versões:

Versão 1.0	28/10/2024
Versão 2.0	09/09/2025
Versão 3.0	23/09/2025

Sumário

Introdução

Este guia tem como objetivo apresentar detalhadamente as funções e atribuições do Encarregado pelo Tratamento de Dados Pessoais (DPO), conforme a Resolução CD/ANPD nº 18, de 16 de julho de 2024 da Autoridade Nacional de Proteção de Dados (ANPD) e o artigo 38 do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. A Resolução da ANPD estabelece parâmetros para a atuação do DPO no Brasil, em consonância com as diretrizes europeias, e destaca a importância de garantir a independência desse profissional para evitar conflitos de interesse.

De acordo com o art. 2º, II, do Regulamento sobre a atuação do encarregado, o conflito de interesse corresponde a qualquer situação que possa comprometer ou influenciar, de modo impróprio, a objetividade e o julgamento técnico no desempenho das atribuições do encarregado. Tal previsão busca estabelecer parâmetros que assegurem uma atuação pautada pela ética, integridade e autonomia técnica, prevenindo interferências externas indevidas. Nesse sentido, evitar conflitos de interesse é elemento essencial para a conformidade do agente de tratamento com a legislação de proteção de dados. Ressalta-se, ainda, que a verificação deve ser feita em cada caso concreto e, se confirmada a ocorrência, pode ensejar a aplicação de sanções ao agente de tratamento (ANPD, 2024).

A Autoridade Belga de Proteção de Dados (DPA) multou uma empresa de logística em €50.000 por nomear o chefe dos departamentos de conformidade, auditoria e gestão de riscos como o Encarregado de Proteção de Dados (DPO), gerando um conflito de interesses e violando o artigo 38(6) do GDPR. A DPA concluiu que a acumulação dessas funções impediu o DPO de atuar de forma independente, comprometendo a supervisão adequada do processamento de dados pessoais. A empresa foi instruída a resolver essa situação dentro de três meses (Hunton, 2020).

A Autoridade de Proteção de Dados da Bélgica também multou um banco em 75.000 euros por violar o Artigo 38.6 do GDPR, uma vez que o DPO também ocupava posições de liderança em três departamentos. A combinação dessas funções gerou um claro conflito de interesses, comprometendo a independência do DPO, o que foi considerado negligência grave pela DPA, visto que a função de DPO já estava bem estabelecida desde 2018 (Wim Nauwelaerts, 2022).

Decisões recentes do Tribunal de Justiça da União Europeia (TJUE) reforçam a importância da independência do DPO, conforme previsto no Artigo 38(3) do GDPR. O tribunal reafirma que, embora os Estados membros possam estabelecer proteções adicionais contra a demissão de DPOs, essas proteções não podem comprometer os objetivos do regulamento, especialmente em situações em que o DPO assume outras funções dentro da organização que possam gerar conflitos de interesse (McCann FitzGerald LLP, 2023).

Nota editorial / Isenção de responsabilidade

Este guia foi elaborado por autores convidados e não reflete, necessariamente, o posicionamento institucional do INPD. O material tem caráter informativo e educacional e não substitui aconselhamento jurídico ou regulatório. Exemplos e referências internacionais (p.ex., decisões de autoridades europeias) são utilizados como boas práticas comparadas, devendo cada organização avaliar o caso concreto à luz da LGPD, da Resolução CD/ANPD nº 18/2024 e de seu contexto operacional.

1. Nomeação e Atribuições do Encarregado

A Resolução CD/ANPD nº 18 reforça que a nomeação do encarregado deve ser formal, clara e documentada.

Conforme a Lei Geral de Proteção de Dados (LGPD) o encarregado (DPO) atua como elo de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Esse papel é essencial para garantir que os direitos dos titulares sejam exercidos de maneira eficaz e que o controlador esteja em conformidade com as normas de proteção de dados (Resolução CD/ANPD nº 18, 2024, art. 3º).

De forma similar, o GDPR da União Europeia, no artigo 37, estabelece a obrigatoriedade de nomeação de um DPO quando as atividades de tratamento de dados pessoais envolvem monitoramento regular e sistemático em larga escala ou dados sensíveis (Regulamento (UE) 2016/679). Tanto a LGPD quanto o GDPR enfatizam a necessidade de que o DPO tenha autonomia e capacitação técnica para desempenhar suas funções, conforme previsto na Resolução CD/ANPD nº 18 (art. 10) e no artigo 38 do GDPR.

2. Conflito de Interesses na Função do Encarregado

A Resolução CD/ANPD nº 18 dispõe que o encarregado deve exercer suas funções de maneira independente e livre de influências que comprometam sua objetividade. O conflito de interesses, conforme definido no art. 18 da Resolução, deve ser evitado, especialmente quando o encarregado ocupa simultaneamente outras funções na organização.

Essa medida é essencial para garantir que o DPO possa desempenhar seu papel de supervisão e fiscalização de forma imparcial, sem ser influenciado por decisões que envolvam diretamente o

tratamento de dados pessoais. A independência do DPO é fundamental para assegurar que ele tenha a autonomia necessária para agir em conformidade com a legislação, sem interferências que possam prejudicar sua avaliação.

No âmbito da União Europeia, o **artigo 38(6)** do GDPR permite que o DPO desempenhe outras funções dentro da organização, desde que tais funções não gerem conflitos de interesses. Esse artigo reforça que o DPO deve estar livre de qualquer envolvimento em decisões que possam afetar sua imparcialidade na supervisão do tratamento de dados. A função do DPO é assegurar que os dados pessoais sejam processados de acordo com as normas de proteção de dados, e para isso, é imperativo que ele mantenha uma postura independente em relação às áreas de decisão sobre o tratamento de dados pessoais.

Tanto a Resolução da ANPD quanto o GDPR concordam que, para o DPO desempenhar suas funções adequadamente, ele deve estar desvinculado de responsabilidades que possam gerar comprometimento na tomada de decisões objetivas. O conflito de interesses, portanto, deve ser rigorosamente evitado para garantir a integridade do tratamento de dados pessoais e a proteção dos direitos dos titulares.

O Grupo do Artigo 29, instituído pela Diretiva 95/46/CE como órgão consultivo independente da União Europeia para proteção de dados, definiu em suas diretrizes que a designação de um encarregado de proteção de dados (DPO) deve evitar potenciais conflitos de interesse, especialmente para funções de alto nível, como diretores executivos, financeiros, de marketing, recursos humanos ou TI, que participam diretamente na definição das finalidades e meios de tratamento de dados pessoais. A orientação também adverte sobre o risco de conflito se o DPO, quando este for designado para representar a organização ou seus subcontratados em processos judiciais envolvendo questões de proteção de dados, pois essa função compromete a imparcialidade necessária ao cumprimento das normas de privacidade (WP243, 2017).

3. Impacto no Cenário Brasileiro

No Brasil, a Resolução CD/ANPD nº 18 segue uma linha semelhante, ao estabelecer que o encarregado deve atuar com ética e autonomia técnica (art. 18). O caso belga serve como um alerta para as empresas brasileiras que optam por acumular funções de conformidade ou auditoria com as atividades de DPO. Conforme o artigo 18 da Resolução, o encarregado deve informar qualquer situação que possa configurar conflito de interesses, e a organização é responsável por garantir que essa função não seja comprometida.

Esse cenário exige que as empresas brasileiras realizem uma análise criteriosa ao designar o encarregado. Nomear uma pessoa que exerça simultaneamente funções em áreas de conformidade,

risco ou auditoria pode gerar conflitos de interesses e resultar em sanções pela ANPD, caso essas funções interfiram na autonomia do encarregado.

4. Multas da Autoridade Belga (DPA)

As decisões da Autoridade Belga de Proteção de Dados (DPA) demonstram como a não conformidade com os requisitos de independência do Encarregado de Proteção de Dados (DPO) pode acarretar penalidades substanciais. Um dos casos mais destacados envolveu a imposição de uma multa de **€50.000** a uma empresa por nomear um DPO que também atuava como chefe de auditoria, conformidade e gestão de riscos. Essa combinação de funções gerou um conflito de interesses, violando o artigo 38(6) do GDPR, que exige que o DPO não tenha envolvimento em atividades que possam comprometer sua imparcialidade. O fato de o DPO tomar decisões relacionadas ao processamento de dados nas áreas sob sua responsabilidade impediu que ele supervisionasse essas atividades de forma independente (DPO Centre, 2024).

Outro caso significativo resultou em uma multa de **€75.000** aplicada a um banco. Nesse caso, o DPO acumulava funções nos departamentos de Gestão de Riscos e Investigação, o que também comprometeu sua independência e violou os artigos 38(3) e 38(6) do GDPR. A DPA ressaltou que o DPO deve ter acesso direto à alta administração e participar de todas as discussões relevantes sobre proteção de dados, sem conflitos de interesses. A ausência de salvaguardas adequadas para garantir a independência do DPO foi considerada uma grave falha de governança (Nauwelaerts, 2022).

Esses casos destacam a responsabilidade das organizações em garantir que o DPO tenha autonomia para desempenhar suas funções de maneira imparcial, sem conflitos que possam comprometer sua capacidade de supervisão. A não conformidade com essas exigências pode resultar em multas consideráveis e reflete a necessidade de uma governança adequada para garantir a proteção de dados pessoais (Hunton, 2024).

5. Conflito de Interesses no Caso X-FAB Dresden GmbH & Co. KG. Recorrido: FC

O Tribunal de Justiça da União Europeia (TJUE) esclareceu os critérios que caracterizam um conflito de interesses no papel do DPO no caso **X-FAB Dresden GmbH & Co. KG v. FC**. O DPO, que também ocupava o cargo de presidente do conselho de trabalhadores, foi demitido sob a

justificativa de que suas responsabilidades adicionais comprometiam sua independência funcional. A decisão do tribunal enfatizou que, de acordo com o artigo 38 do GDPR, o DPO não pode exercer funções que o envolvam na determinação de finalidades e meios de tratamento de dados, pois isso criaria um conflito de interesses que prejudicaria sua capacidade de monitorar a conformidade com o GDPR de maneira objetiva.

O TJUE reafirmou a necessidade de proteger a independência funcional do DPO, destacando que um DPO que acumula funções de gestão em áreas operacionais não pode executar suas responsabilidades de forma imparcial (TJUE, 2023).

6. Consequências e Sanções por Não Conformidade

A análise dos precedentes internacionais reforça a necessidade de uma governança sólida e independente em proteção de dados, evidenciando que o descumprimento das diretrizes de independência do DPO pode acarretar penalidades severas e comprometer a conformidade da organização. No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD), respaldada pela Resolução CD/ANPD nº 18 e pela Lei Geral de Proteção de Dados (LGPD), dispõe de uma ampla gama de sanções administrativas para aplicar às organizações que desrespeitam as normas de proteção de dados. Entre as sanções previstas estão:

- **Advertência**, com indicação de prazo para a adoção de medidas corretivas.
- **Multa simples**, de até 2% do faturamento da empresa no Brasil, limitada a R$ 50 milhões por infração.
- **Multa diária**, sujeita ao mesmo limite máximo de R$ 50 milhões.
- **Publicização da infração**, após confirmada a sua ocorrência, com o objetivo de alertar o público e reforçar a transparência.
- **Bloqueio dos dados pessoais** a que se refere a infração até a sua regularização.
- **Eliminação dos dados pessoais** relacionados à infração, quando não regularizados em conformidade com as exigências legais.
- **Suspensão parcial do funcionamento do banco de dados** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador.
- **Suspensão do exercício da atividade de tratamento dos dados pessoais** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período.

- **Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados pessoais**, afetando a continuidade de operações de tratamento em casos de não conformidade grave.

Essas sanções, aplicáveis pela ANPD, não apenas refletem a gravidade com que a autoridade brasileira trata as práticas de não conformidade, mas também servem como um alerta para que as organizações priorizem a conformidade com a LGPD, assegurando a independência do DPO e implementando políticas robustas de proteção de dados.

Além das sanções financeiras e operacionais, a falta de conformidade traz sérios danos à reputação da empresa e compromete a confiança dos titulares de dados, prejudicando sua credibilidade no mercado. Esse desgaste reputacional pode ser tão prejudicial quanto as sanções diretas, afetando parcerias comerciais e a fidelidade dos clientes.

Também é importante considerar os riscos de ações judiciais por parte dos titulares de dados. A LGPD, alinhada ao GDPR, prevê a responsabilidade civil das empresas por danos morais e materiais decorrentes do tratamento inadequado de dados pessoais. Isso significa que, além das sanções administrativas impostas pela ANPD, as organizações podem enfrentar processos judiciais que resultem em indenizações substanciais, especialmente em casos de danos recorrentes ou de grande escala.

Portanto, é essencial que as empresas adotem uma política interna rigorosa de proteção de dados, garantindo a independência do DPO e promovendo boas práticas de segurança da informação. Esse compromisso não só minimiza os riscos e evita sanções, mas também fortalece a confiança do mercado e a integridade da organização perante os titulares de dados, estabelecendo uma base sólida para a conformidade contínua com a LGPD e com os padrões internacionais de proteção de dados.

7. Quando um Diretor ou Gerente pode ou não atuar como DPO.

A função do DPO (Encarregado de Proteção de Dados) é regida pela necessidade de independência e imparcialidade em relação ao tratamento de dados pessoais, conforme estabelecido pela Resolução CD/ANPD nº 18 e pelo artigo 38 do GDPR. Portanto, a nomeação de um diretor ou gerente para essa função deve ser cuidadosamente avaliada para evitar conflitos de interesses, sendo o risco de conflito de interesses muito alto quando falamos de diretores ou gerentes.

O Guia da ANPD estabelece que o encarregado deve atuar com autonomia, evitando acumular funções que definam meios e objetivos do tratamento que o encarregado deve exercer suas funções

com plena autonomia, não devendo acumular cargos que determinem meios e objetivos do tratamento de dados pessoais. Em uma mesma organização, há risco de conflito quando o encarregado ocupa posições de **chefia, gerência ou direção** em áreas estratégicas, como **Recursos Humanos, Tecnologia da Informação, Finanças ou Saúde**, já que o exercício cumulativo dessas funções pode comprometer a objetividade e a autonomia técnica necessárias ao desempenho de suas atribuições. Por essa razão, é indispensável uma análise criteriosa do caso concreto, levando em conta o contexto e as circunstâncias específicas de cada situação. Como boa prática, recomenda-se manter a função do encarregado **separada das demais áreas do negócio**, de modo a assegurar maior independência e reforçar sua capacidade de atuação técnica e imparcial.

Já a atuação em mais de uma organização é admitida, desde que o agente de tratamento avalie a capacidade de cumprimento das atribuições em cada entidade e a inexistência de conflito, considerando o setor econômico, o tipo de tratamento e a natureza das organizações, sob risco de decisões conflitantes ou troca de informações privilegiadas/estratégicas. A ausência de conflito é condição essencial de ética, integridade e conformidade com a LGPD; por isso, o encarregado (e o substituto) devem declarar situações potenciais e o agente de tratamento deve analisar conflitos internos e externos. Verificada a possibilidade de conflito, cabe não indicar, mitigar o risco ou substituir a pessoa. Como boa prática, recomenda-se unidade organizacional própria, separada das áreas que tomam decisões estratégicas, para fortalecer a independência do juízo técnico do encarregado.

Tabela comparativa — Conflito de interesse (Guia ANPD, dez/2024)

Eixo	Regras do Guia	Exemplos citados	Riscos/Impactos	Deveres e Providências	Boas práticas
Conflito na mesma organização	Encarregado deve atuar **autonomamente** e **não** acumular funções que **determinem meios e objetivos** do tratamento. **Não é conflito** a decisão **inerente** às atribuições do encarregado.	Cargos **de chefia, gerência ou direção**; áreas: **Recursos Humanos, TI, Finanças, Saúde**.	**Comprometimento da objetividade** e da **autonomia técnica**; interferências indevidas.	**Encarregado:** declarar potenciais conflitos. **Agente de tratamento**: analisar antes da indicação; se houver possibilidade de conflito: **(i)** não indicar; **(ii)**implementar medidas para	Separar a função do encarregado das áreas que tomam decisões estratégicas; estruturar unidade organizacional própria.

				afastar o risco; **(iii)** substituir.	
Atuação em mais de uma organização	É permitido acumular funções em mais de uma organização, desde que viável cumprir as atribuições em cada uma sem conflito.	Não foram citados exemplos. .	**Decisões conflitantes** entre clientes/entidades; **troca de informações privilegiadas ou estratégicas**.	**Agente**: realizar avaliação prévia de compatibilidade e riscos **internos e externos**; documentar análise. **Encarregado.**: garantir que a atuação paralela não compromete sua imparcialidade.	Cláusulas contratuais de **confidencialidade** e **barreiras de informação**; definição clara de **escopo** por organização.
Avaliação de possível conflito	A **ausência de conflito** é condição para práticas autônomas, éticas e íntegras, alinhadas à **LGPD** e à proteção da privacidade.	O Guia **não apresenta exemplos concretos,** mas **orienta** a avaliar fatores como setor econômico, tipo de tratamento e natureza das organizações, diante de riscos de decisões conflitantes ou troca de informações privilegiadas	Prejuízo à **conformidade**, à **imparcialidade** e ao **julgamento técnico** do encarregado.	**Encarregado e substituto**: **devem declarar** quaisquer situações que possam configurar conflito (**responsabilidade pela veracidade**). **Agente**: analisar conflitos **internos/externos** e, constatada a possibilidade, **não indicar**	

Situações em que um Diretor ou Gerente pode atuar como DPO.

Um diretor ou gerente pode ser designado como encarregado (DPO) desde que suas funções não interfiram nas decisões relativas ao tratamento de dados pessoais. Em conformidade com o Guia da ANPD, isso significa que a atuação executiva não deve abranger a definição dos meios ou das finalidades do tratamento, nem envolver deliberações estratégicas ou operacionais relacionadas à coleta, ao uso, ao armazenamento ou ao compartilhamento de informações pessoais. O objetivo é evitar que o mesmo indivíduo acumule atribuições que possam comprometer sua independência técnica e gerar conflito de interesses.

Exemplo prático 1:

Um Diretor Financeiro responsável apenas pela elaboração do orçamento, pela gestão patrimonial e pelo controle contábil pode acumular a função de DPO, desde que não participe da definição de políticas de retenção, uso ou compartilhamento de dados pessoais, preservando a separação entre suas funções executivas e as atribuições de proteção de dados.

Exemplo prático 2:

Um Gerente de Logística que coordene exclusivamente o transporte e a distribuição de produtos pode ser designado como DPO, desde que não esteja envolvido em decisões relacionadas ao uso de dados de clientes ou empregados, garantindo que sua atuação no tratamento de dados pessoais seja imparcial e independente.

Nessas situações, o elemento central é que o DPO tenha autonomia técnica e independência funcional, com liberdade para supervisionar e orientar o tratamento de dados, garantir a conformidade com a LGPD e comunicar-se diretamente com a alta administração, sem sofrer pressões ou interferências de outras áreas da empresa.

Ademais, conforme estabelece o art. 7º da Resolução CD/ANPD nº 18/2024, cabe ao agente de tratamento definir as qualificações profissionais exigidas para o exercício da função de encarregado, levando em conta não apenas o conhecimento da legislação de proteção de dados, mas também o contexto, o volume e os riscos das operações de tratamento realizadas. Esse requisito revela-se

particularmente relevante quando se avalia a designação de diretores ou gerentes de áreas executivas, já que tais cargos, em regra, não incluem em sua descrição formal competências jurídicas e técnicas específicas em privacidade e proteção de dados. Assim, a indicação de um executivo para a função de DPO deve ser cuidadosamente analisada, considerando não apenas a ausência de conflito de interesse, mas também a efetiva capacitação técnica e jurídica necessária ao desempenho adequado de suas atribuições.

Situações em que um Diretor ou Gerente não poderia atuar como DPO

Se um diretor ou gerente estiver diretamente envolvido na definição dos meios e das finalidades do tratamento de dados pessoais, não poderá acumular a função de encarregado (DPO). Essa restrição decorre do risco de conflito de interesses, já que o profissional encarregado de fiscalizar e orientar a conformidade estaria, simultaneamente, participando de decisões estratégicas ou operacionais relacionadas ao tratamento. O resultado seria a perda da imparcialidade e da autonomia técnica indispensáveis para a função, comprometendo a efetividade da governança em proteção de dados pessoais.

Um Diretor de Tecnologia da Informação (TI), por exemplo, que tenha sob sua responsabilidade a implementação e a gestão dos sistemas que processam os dados pessoais de colaboradores e clientes, não pode exercer o papel de DPO. Isso porque sua função inclui a tomada de decisões diretamente relacionadas ao armazenamento, segurança e processamento de dados pessoais, o que o colocaria na posição de fiscalizar as próprias deliberações. A imparcialidade exigida para a atuação do DPO seria, nesse caso, claramente comprometida.

Situação semelhante ocorre com funções ligadas à Conformidade, Auditoria e Risco. Esses cargos frequentemente são incompatíveis com o papel de DPO, uma vez que exercem supervisão direta sobre os processos de tratamento de dados. Se o encarregado fosse, ao mesmo tempo, o responsável por auditar e revisar a conformidade regulatória em proteção de dados, haveria um duplo papel inconciliável: criar e fiscalizar as mesmas normas e controles. Isso geraria, inevitavelmente, comprometimento da objetividade técnica.

Exemplo prático:
Um Diretor de TI que supervisiona os sistemas de gestão, segurança e armazenamento de dados pessoais não pode acumular a função de DPO. Seu envolvimento direto em decisões sobre as tecnologias utilizadas e sobre a forma como os dados são processados impede a neutralidade necessária para avaliar a conformidade e supervisionar o cumprimento da legislação. O DPO não pode auditar ou fiscalizar as próprias escolhas tecnológicas da organização.

Além disso, cargos executivos de nível sênior, como CEO ou COO, também não devem ser indicados para a função de DPO. Esses executivos exercem influência decisiva sobre a estratégia da organização, incluindo a formulação de políticas de tratamento de dados pessoais. Como sua função abrange decisões amplas e estruturais, desde a definição de processos até a priorização de investimentos em dados, o conflito de interesses seria inevitável. Nessas circunstâncias, a independência necessária para o DPO não estaria assegurada, pois a supervisão seria contaminada por interesses corporativos mais amplos.

Exemplo prático:
Um Chefe de Conformidade ou de Auditoria que realiza revisões e auditorias sobre processos relacionados ao tratamento de dados também não deve ser nomeado como DPO. Essas funções incluem avaliar o grau de aderência da organização às normas de proteção de dados e de segurança da informação. Se a mesma pessoa fosse DPO, ela estaria analisando a conformidade de atividades que ela própria executa, o que comprometeria a imparcialidade e a credibilidade da supervisão.

A nomeação de um diretor ou gerente como DPO deve sempre resultar de uma avaliação criteriosa do contexto organizacional. Quando suas atribuições envolvem decisões estratégicas ou operacionais sobre o tratamento de dados pessoais, ou quando há supervisão direta sobre áreas críticas (TI, Auditoria, Conformidade, Segurança da Informação), o risco de conflito de interesses é evidente e a indicação se torna inadequada.

No entanto, se a área de atuação executiva não tiver influência sobre políticas ou práticas de tratamento e houver separação clara de funções, a acumulação da função pode ser considerada. Em todos os casos, deve ser preservada a autonomia técnica e a imparcialidade do DPO, conforme determinado pela LGPD e pelo art. 7º da Resolução CD/ANPD nº 18/2024, que reforça a necessidade de qualificação técnica, conhecimento jurídico e compatibilidade com o risco e o volume das operações realizadas.

Critérios para Nomeação de Profissionais da Área Jurídica como DPO

A indicação de profissionais da área jurídica para exercer a função de encarregado (DPO) demanda uma análise criteriosa e reforçada, dada a possibilidade elevada de configuração de conflito de interesses. O papel do DPO, segundo a Resolução CD/ANPD nº 18/2024 e o GDPR, exige atuação independente, imparcial e autônoma, sem vinculação a pressões internas ou externas que possam comprometer sua capacidade de supervisão e fiscalização objetiva.

Quando um profissional jurídico assume a função de DPO, especialmente aquele que atua na representação da empresa em litígios ou processos administrativos envolvendo decisões de tratamento de dados pessoais, há um risco relevante de sobreposição de papéis. A defesa judicial ou administrativa das práticas da empresa implica, em regra, a adoção de uma postura parcial, voltada à proteção dos interesses corporativos. Essa posição contrasta diretamente com as atribuições de um DPO, cuja responsabilidade é questionar, monitorar e recomendar ajustes em tais práticas, inclusive quando falhas ou irregularidades forem constatadas.

Esse conflito se agrava em situações de auditorias, incidentes de segurança ou investigações regulatórias, nas quais o DPO deve ter liberdade para apontar deficiências e orientar correções. Caso acumule também a função de advogado interno, poderá enfrentar um dilema ético: proteger a organização em disputas ou cumprir seu dever de imparcialidade e fiscalização. Essa dualidade enfraquece a independência técnica, essencial para a credibilidade da função de encarregado.

Portanto, para preservar a integridade e a efetividade da atuação do DPO, recomenda-se que profissionais jurídicos que atuem diretamente na defesa ou representação da empresa não sejam acumulados nesta função. Cabe ao agente de tratamento assegurar que o DPO disponha de condições plenas para focar no monitoramento da conformidade, na prevenção de riscos e na tutela dos direitos dos titulares, sem interferências derivadas de responsabilidades de defesa jurídica da organização.

8. Como posso gerenciar estas situações contraditórias

A gestão de potenciais conflitos de interesses na função do encarregado (DPO) exige salvaguardas de governança e medida de suporte operacional que preservem autonomia técnica, objetiva e efetiva do papel.

8.1. Salvaguardas de independência do DPO

8.1.1. Do Mandado do Encarregado de Dados

Documento aprovado pela alta administração que define, no mínimo: missão e escopo; autonomia técnica, direito de acesso a informações, sistemas e pessoas; prazos de resposta das áreas (SLA´s) participação desde o "*privacy by design*"; poderes para recomendar medidas; e compromisso de não retaliação pelo exercício regular das atribuições.

8.1.2. Linha de reporte e proteção organizacional

Reporte funcional do DPO ao nível mais alto de governança (conselho, diretoria ou comitê de privacidade), com registro em atas das interações periódicas. Estabelece critérios e rito formal para nomeação e substituição, vedando destituição por exemplo controle ou apontar não conformidades.

8.1.3. Segregação de funções e matriz RACI

Mapeie funções incompatíveis com a independência do DPO (em regra, cargos que definem meios e finalidades do tratamento): liderança de TI/Ciber (CIO/CISO), RH, Marketing, Finanças, Conformidade/Auditoria e jurídico contencioso sobre os mesmos tratamentos.

Aplique matriz RACI para cada macroprocesso de dados, assegurando que o DPO atue como **C** (consultado) e **I** (informado, nunca como **A/R (decisor /executor)** de atividades que determine meios/fins, aprove controles ou seja "proprietário" de bases / sistemas.

A seguir, um quadro síntese com exemplos de funções que tendem a configurar conflito e medidas mínimas de mitigação. A avaliação é sempre caso a caso.

Quadro 8.1-A — Funções tipicamente incompatíveis com a independência do DPO e mitigadores mínimos.

Função acumulada	Risco de conflito	Por quê	Medidas mínimas se inevitável
CIO/CISO / Head de TI	Alto	Define meios/finalidades e controla sistemas	DPO externo (PJ), recusa, segregação, reporte direto à alta gestão
Head de RH/Marketing/Finanças	Alto	Decide coleta/uso de dados pessoais	Mesmas medidas acima + matriz RACI e auditoria independente
Conformidade/Auditoria/Riscos	Alto	Supervisiona os mesmos controles que o DPO avalia	Separar funções; DPO sem poder de aprovação de controles
Jurídico contencioso	Médio-alto	Defesa de práticas sob escrutínio do DPO	Segregar contencioso; recusal; barreiras de informação
Jurídico consultivo (sem decisão)	Baixo-médio	Risco de influência	Charter limitando poderes; revisões cruzadas

Nota de rodapé da tabela: Base normativa: Res. CD/ANPD nº 18/2024 (arts. 18–21), GDPR art. 38(6) e WP243/EDPB. Exemplos ilustrativos.

8.1.4. Barrias de informação e recusa

Implemente barreiras quando o Encarregado ou seu substituto acumular outra função potencialmente conflitante: canais, pastas e agendas segregadas; registro formal de recusa por projeto / tratamento; rotação de revisores, revisão independente quando houver dúvida razoável de conflito.

8.1.5 Avaliação documentada de conflito

Conduza avaliação prévia (na nomeação) e periódica (anual ou a cada mudança relevante) com checklist de fatores: poder decisório, influência orçamentária, “proprietário” de processos/sistemas, metas e incentivos. Mantenha Registro de Conflitos com decisões e mitigadores adotados.

8.1.6 Recursos e acesso

Garanta recursos adequados (equipe, orçamento, ferramentas) e acesso tempestivo a evidências, relatórios e logs necessários. No caso do Encarregado de Dados ser uma pessoa jurídica (DPOaaS), inclua em contrato direitos de acesso, cláusulas de independência e dever de confidencialidade equivalentes aos do DPO interno.

8.1.7 Metas, KPIs e incentivos

Evite métricas que criem incentivos à subnotificação ou "maquiagem" de risco (ex.: "zerar incidentes"). Prefira indicadores de maturidade (tempo de resposta, cobertura de PIA/RIPD, eficácia de planos de ação) e metas qualitativas de governança.

8.1.8 Canal de integridade e proteção contra interferência

Disponibilize canal para reporte de tentativas de ingerência na atuação do Encarregado de Dados, com tratamento pelo nível superior ao reportado. Reforce política de não retaliação a quem coopera com a área de privacidade.

8.1.9 Transparência ao titular e autoridades

Divulgue contato do Encarregado de Dados e a estrutura de governança no aviso de privacidade e no site. No setor público, proceda também à publicação oficial da indicação; para agentes de pequeno porte, quando dispensado o Encarregado, mantenha canal de contato e responsabilidades equivalentes.

8.1.10 Substituto formal e continuidade

Designe substituto com salvaguardas idênticas de independência e recusa. Teste a continuidade (backups de agenda, dossiês de projetos, plano de férias/afastamentos).

- Checklist de evidências recomendadas (auditoria)
- Charter do DPO; organograma e linha de reporte;
- Matriz RACI e lista de funções incompatíveis;
- Registro de recusas e barreiras de informação;
- Avaliações periódicas de conflito;
- Atas de comitê/board com interlocução do DPO;
- Plano de recursos (equipe, orçamento, ferramentas) e KPIs de maturidade;
- Contrato de DPOaaS (se aplicável) com cláusulas de independência e acesso.

Modelo sintético – Declaração de (não) conflito

Eu, [nome], indicado(a) para exercer a função de Encarregado(a) de Proteção de Dados (DPO) da [organização], declaro que não exerço funções que determinem meios e finalidades do tratamento de dados pessoais na organização. Declaro, ainda, que informarei imediatamente qualquer situação potencial de conflito e me recusarei formalmente a atuar nos casos em que tal conflito seja identificado, conforme política interna e legislação aplicável.
[data/assinatura]

8.2 Medidas de suporte operacional

a) Auditorias independentes e PIA/RIPD

Realize auditorias internas/externas periódicas sobre o programa de privacidade e a efetividade das salvaguardas de independência. Garanta a participação do Encarregado de Dados (consultivo) e a execução de PIA/RIPD em projetos de risco, com rastreabilidade de pareceres e decisões.

b) Políticas e comunicação

Atualize e divulgue: Política de Proteção de Dados/Privacidade, Política de Segurança da Informação, Política de Gestão de Incidentes e Norma de Conflitos de Interesses do Encarregado de Dados (incluindo recusa, barreiras e escalonamento). Alinhe com o Código de Ética/Conduta.

c) Capacitação contínua

Programa anual de treinamento diferenciado por público (lideranças, TI, RH, Marketing, Jurídico, Produto), incorporando estudos de caso e lições aprendidas. Registre presença e eficácia (quiz, indicadores de retenção).

d) Integração a comitês e ciclo de decisões

Inclua o Encarregado de Dados no comitê de privacidade e nas instâncias de aprovação de projetos que envolvam dados pessoais (gateway/PMO), garantindo consulta prévia e prazos mínimos para revisão.

e) Gestão de mudanças e fornecedores

Avalie impactos de mudanças organizacionais (reorganizações, novos sistemas, M&As) sobre conflito de interesses. Em fornecedores e suboperadores, exija contrato com cláusulas de governança do Encarregado de Dados, cooperação e fluxo de informações.

f) Incidentes e interface com autoridades/titulares

Defina papéis e SLAs para notificação de incidentes, respostas a titulares e interação com a ANPD, assegurando que o Encarregado opine tecnicamente e tenha visibilidade integral do caso.

g) Monitoramento e melhoria contínua

Acompanhe KPIs de maturidade, ações corretivas e testes de eficácia, reportando resultados à alta administração e ao comitê.

8.3. Conclusão

Para mitigar, de forma efetiva os riscos de conflito de interesses, é indispensável verificar continuamente se as salvaguardas de independência (8.1) e as medidas de suporte operacional (8.2) estão funcionando na prática. Recomenda-se:

- Auditorias internas ou externas periódicas, avaliando a aderência à legislação aplicável e às melhores práticas, com evidências de correções implementadas.
- Transparência e comunicação: atualização e divulgação das políticas de Privacidade e de Segurança da Informação, com identificação clara do DPO e seus canais de contato para dúvidas dos titulares e de autoridades.
- Capacitação contínua das equipes envolvidas, reforçando papéis, responsabilidades e o rito de recusa/impedimento quando houver potencial conflito.
- DPO as a Service (DPOaaS) como alternativa válida, desde que o contrato assegure independência, ausência de conflito, direitos de acesso às informações, confidencialidade e mecanismos de recusa e de barreiras de informação.

Em síntese, a independência do Encarregado de Dados é um requisito de governança, não uma preferência organizacional. Consolidar essas práticas fortalece a autonomia técnica do encarregado, aumenta a confiança de titulares e reguladores e sustenta a maturidade do programa de privacidade.

9. Considerações Finais

A Resolução CD/ANPD nº 18, em consonância com o GDPR da União Europeia, consolida diretrizes rigorosas para a nomeação e a atuação do Encarregado de Proteção de Dados (DPO),

ressaltando a imprescindibilidade de sua independência e imparcialidade. Ao lado da regulamentação, a experiência internacional, em especial as decisões da Autoridade Belga de Proteção de Dados (DPA), bem como de autoridades na Alemanha e em Luxemburgo, evidencia que a ausência de separação clara entre as funções do DPO e outras responsabilidades organizacionais conduz a consequências severas. As multas aplicadas de €50.000 e €75.000, em razão de violações aos artigos 38(3) e 38(6) do GDPR, demonstram de forma inequívoca a gravidade das falhas relacionadas a conflitos de interesse no desempenho dessa função.

Esses precedentes internacionais devem ser compreendidos como alerta estratégico às organizações brasileiras. A Resolução nº 18 da ANPD adota premissas semelhantes, ao vedar que o DPO exerça cargos que possam comprometer sua imparcialidade ou sua autonomia, como funções ligadas à conformidade, à auditoria ou à gestão de riscos. No Brasil, a LGPD, em harmonia com a Resolução, estabelece que a integridade da função do DPO é essencial para assegurar uma supervisão confiável das atividades de tratamento de dados pessoais.

Portanto, torna-se imperativo que as organizações brasileiras instituam mecanismos de governança em proteção de dados robustos e transparentes, garantindo que o DPO disponha de autonomia técnica, recursos adequados e independência funcional para desempenhar suas atribuições de modo eficaz. A mitigação de riscos regulatórios e a proteção efetiva dos direitos dos titulares de dados não são apenas exigências legais, mas constituem pilares de confiança organizacional e de credibilidade institucional.

Em última análise, o panorama internacional confirma que a falta de imparcialidade na atuação do DPO não implica apenas em penalidades financeiras. Trata-se também de uma ameaça à reputação corporativa, à confiança dos titulares de dados pessoais e à sustentabilidade da governança organizacional em um cenário cada vez mais orientado pela ética digital e pelo respeito à privacidade. Para as empresas brasileiras, observar rigorosamente tais parâmetros não é apenas uma obrigação legal, mas um diferencial competitivo e reputacional indispensável na economia de dados contemporânea.

Referências Bibliográficas

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 18, de 16 de julho de 2024. Brasília, DF: ANPD, 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo: atuação do encarregado pelo tratamento de dados pessoais**. Brasília: ANPD, dez. 2024.

DPO Centre. Belgian DPA rules on DPO conflict of interest. Disponível em: https://www.dpocentre.com/news/dpo-conflict-of-interest/. Acesso em: 14 out. 2024.

NAUWELAERTS, Wim. Belgian Data Protection Authority fines bank for DPO's conflicting roles. Alston & Bird Privacy, Cyber & Data Strategy Blog, 31 jan. 2022. Disponível em: Belgian Data Protection Authority Fines Bank for DPO's Conflicting Roles | Alston & Bird Privacy, Cyber & Data Strategy Blog (alstonprivacy.com) .Acesso em: 14 out. 2024.

Hunton, Alston & Bird. Belgian DPA Sanctions Company for Non-Compliance with the GDPR's DPO Requirements. Hunton Privacy & Information Security Law Blog. Disponível em: https://www.huntonak.com/privacy-and-information-security-law/belgian-dpa-sanctions-company-for-non-compliance-with-the-gdprs-dpo-requirements. Acesso em: 14 out. 2024.

TJUE. **Acórdão do Tribunal de Justiça (Sexta Secção) de 9 de fevereiro de 2023**. Reenvio prejudicial- Proteção das pessoas singulares no tratamento de dados pessoais - Regulamento (UE) 2016/679 - Encarregado da proteção de dados - Proibição de destituição. **Processo C-453/21**, X-FAB Dresden GmbH & Co. KG v FC. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62021CA0453. Acesso em: 14 out. 2024.

Regulamento (UE) 2016/679, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR).

Grupo de Trabalho do Artigo 29 para a Proteção de Dados. Orientações sobre os Encarregados da Proteção de Dados (WP243), de 13 de dezembro de 2016, última redação revista e adotada em 5 de abril de 2017.

INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

/company/inpdados

/inpdados/

Este documento é classificado como “Público”.