

TMT
4 de novembro de 2024

OBRIGAÇÕES DOS RESPONSÁVEIS PELO TRATAMENTO NA CONTRATAÇÃO DE SUBCONTRATANTES E SUB-SUBCONTRATANTES

O Parecer 22/2024 do EDPB

No dia 7 de Outubro de 2024, o Comité Europeu para a Proteção de Dados (EDPB) adoptou o Parecer 22/2024 (o “Parecer”) a pedido da Autoridade Dinamarquesa para a Proteção de Dados. O Parecer vem esclarecer as obrigações dos responsáveis pelo tratamento (entidades que determinam as finalidades e meios de tratamento de dados pessoais) ao delegarem operações de tratamento a subcontratantes e sub-subcontratantes, clarificando o cumprimento dos requisitos do Artigo 28 do RGPD (relativo a contratos e condições de contratação de subcontratantes), e assegurar uma aplicação harmonizada destas obrigações nos Estados-Membros da UE. Nesta Briefing, abordamos os pontos principais do Parecer.

› Responsabilidade dos Responsáveis pelo Tratamento: supervisão e verificação de Subcontratantes e Sub-subcontratantes

Identificação completa da cadeia de Sub-subcontratantes

No Parecer é sublinhado que o Responsável pelo Tratamento deve, a todo o momento, ter acesso às informações detalhadas sobre todos os Sub-subcontratantes ao longo da cadeia de tratamento de dados – incluindo nome, morada e pessoa de contacto. Esta exigência visa permitir que os Responsáveis pelo Tratamento exerçam o seu dever de supervisão e possam atuar rapidamente em caso de falhas ou pedidos de informação dos titulares dos dados.

Mesmo em atividades de tratamento de baixo risco,

esta exigência mantém-se. O Subcontratante inicial deve, de forma proativa, informar o Responsável pelo Tratamento sobre qualquer alteração nos Sub-subcontratantes envolvidos, mantendo atualizadas as informações e facilitando o acesso do Responsável pelo Tratamento a esses dados em qualquer momento.

Garantias de conformidade técnica e organizativa

Os Responsáveis pelo Tratamento têm o dever de verificar que os Subcontratantes e Sub-subcontratantes oferecem garantias suficientes para implementar medidas técnicas e organizativas adequadas. Essas garantias são essenciais para assegurar que o tratamento cumpre o Regulamento Geral sobre a Proteção de Dados (“RGPD”) e protege os direitos dos titulares dos dados.

TMT 4 de novembro de 2024

A verificação das garantias dos subcontratantes deve ser contínua. O Parecer destaca que esta obrigação não se limita a uma verificação inicial, mas exige revisões periódicas, com o nível de monitorização ajustado ao risco específico associado ao tratamento dos dados. Por exemplo, atividades de tratamento de dados que envolvam categorias especiais de dados pessoais ou operações de grande escala podem exigir verificações mais rigorosas.

O Responsável pelo Tratamento deve, portanto, avaliar regularmente a suficiência das garantias de cada Subcontratante e Sub-subcontratante, conforme o risco inerente ao tipo de tratamento realizado. Medidas práticas incluem a exigência de políticas de privacidade robustas, auditorias conduzidas por terceiros e certificações de segurança, como ISO 27001, para demonstrar a conformidade.

Documentação de conformidade e responsabilidade

Para cumprir o princípio de responsabilidade (*accountability*), o Responsável pelo Tratamento deve documentar todas as ações e medidas de conformidade adotadas na escolha e supervisão dos seus Subcontratantes e Sub-subcontratantes. Esta documentação é essencial para demonstrar conformidade perante as autoridades de supervisão e permite comprovar as ações de diligência adequadas em caso de uma auditoria ou inspeção.

Métodos de documentação recomendados incluem questionários de conformidade, relatórios de auditorias, certificações e inspeções *in loco*.

› **Requisitos contratuais entre Responsáveis pelo Tratamento e Subcontratantes**

O Artigo 28(3) do RGPD estabelece que o contrato entre o Responsável pelo Tratamento e o Subcontratante deve incluir uma cláusula especificando que o tratamento de dados deve ser realizado exclusivamente segundo as instruções documentadas do Responsável pelo Tratamento, salvo quando uma obrigação legal do Subcontratante imponha o contrário. O Parecer recomenda a inclusão da formulação “*salvo se for exigido por lei da União ou do Estado-Membro a que o subcontratante está sujeito*”, para maior clareza. No entanto, tal formulação é uma recomendação e não uma exigência obrigatória.

Imposição de obrigações ao longo da cadeia

O Parecer sublinha que o contrato entre o Responsável pelo Tratamento e o Subcontratante deve assegurar que as obrigações de proteção de dados se estendam a todos os Sub-subcontratantes. O Artigo 28(4) do RGPD exige que o Subcontratante passe adiante, ao longo da cadeia, as mesmas obrigações contratuais de proteção de dados. Assim, todos os níveis de subcontratação devem adotar medidas consistentes de proteção de dados,

TMT 4 de novembro de 2024

refletindo as condições iniciais estabelecidas pelo Responsável pelo Tratamento.

Direito de auditoria e solicitação de cópia de contratos de Sub-subcontratantes

O Responsável pelo Tratamento tem o direito de auditar os seus Subcontratantes e Sub-subcontratantes para verificar o cumprimento das obrigações contratuais e do RGPD.

Caso o Responsável pelo Tratamento considere necessário, pode solicitar uma cópia dos contratos de sub-subcontratação para verificar se as obrigações de proteção de dados foram efetivamente passadas ao longo da cadeia de tratamento. No entanto, o Parecer esclarece que o Responsável pelo Tratamento não é obrigado a solicitar essas cópias de forma sistemática. Esta solicitação deve ser feita com base numa análise de risco, podendo ser realizada em casos específicos, como a suspeita de não conformidade.

Processo de verificação proporcional ao risco

O nível de verificação deve ser ajustado conforme o risco associado ao tratamento dos dados. Para atividades de tratamento de dados de alto risco, o Responsável pelo Tratamento deve exigir garantias mais rigorosas dos seus Subcontratantes e Sub-subcontratantes, incluindo auditorias adicionais ou avaliações de conformidade aprofundadas. No

Parecer é sugerida uma abordagem proporcional, em que a intensidade das verificações depende do nível de risco identificado, sendo recomendado que o Responsável pelo Tratamento adote um sistema de monitorização ajustável, que contemple revisões periódicas e auditorias quando necessário.

› Transferências internacionais de dados: obrigações dos Responsáveis pelo Tratamento e Subcontratantes

O Parecer reforça que, mesmo quando a transferência de dados para fora do Espaço Económico Europeu (EEE) é efetuada por um Subcontratante ou Sub-subcontratante, o Responsável pelo Tratamento mantém a responsabilidade sobre o tratamento e transferência de dados pessoais. Assim, o Responsável pelo Tratamento deve assegurar que qualquer Sub-subcontratante opera de acordo com as exigências do Capítulo V do RGPD (relativo às transferências internacionais de dados).

Uso de Cláusulas Contratuais-Tipo (SCCs)

Quando aplicável, o Responsável pelo Tratamento deve garantir que o Subcontratante utiliza as Cláusulas Contratuais-Tipo (SCCs) ou outros mecanismos aprovados para assegurar que o nível de proteção previsto no RGPD é respeitado durante e após a transferência. Estes mecanismos devem ser devidamente documentados, e o Responsável pelo

TMT 4 de novembro de 2024

Tratamento pode exigir que o Subcontratante disponibilize a documentação relevante para verificação de conformidade.

Responsabilidade mútua em transferências internacionais

Tanto o Responsável pelo Tratamento como o Subcontratante são responsáveis pelo cumprimento do RGPD, especialmente em caso de transferência para países terceiros que possam ter legislação incompatível com o RGPD. Se o Subcontratante realizar uma transferência não autorizada ou fora das instruções do Responsável pelo Tratamento, ambos podem ser considerados responsáveis. Em caso de incumprimento, o Responsável pelo Tratamento pode ser responsabilizado se a transferência não cumprir os requisitos legais.

› Conclusões e recomendações práticas

O Parecer reforça a responsabilidade contínua dos Responsáveis pelo Tratamento na seleção e monitorização de Subcontratantes e Sub-subcontratantes. Os Responsáveis pelo Tratamento devem demonstrar conformidade com o RGPD através de medidas proporcionais ao nível de risco e de uma documentação rigorosa, assegurando que as obrigações são devidamente transmitidas ao longo da cadeia de tratamento.

Com base no Parecer, é recomendável que um Responsável pelo Tratamento:

- ✓ Mantenha um registo atualizado de todos os Subcontratantes e Sub-subcontratantes envolvidos em cada tratamento de dados;
- ✓ Avalie e verifique as garantias de conformidade dos Subcontratantes, conforme o risco associado ao tratamento de dados;
- ✓ Documente todas as ações de supervisão e conformidade para demonstrar a responsabilidade;
- ✓ Inclua nos contratos (os denominados acordos de tratamento de dados ou *data processing agreements* – DPAs) as cláusulas obrigatórias para proteção de dados, conforme o Artigo 28 do RGPD, no mínimo; e
- ✓ Exerça o direito de auditoria periodicamente, especialmente em casos de atividades de tratamento de alto risco ou dúvidas quanto à conformidade dos Subcontratantes e Sub-subcontratantes.

Este documento contém informação genérica e não configura a prestação de assessoria jurídica que deve ser obtida para a resolução de casos concretos e não pode ser divulgado, copiado ou distribuído sem autorização prévia da [Vasconcelos Advogados](#).

Para informação adicional, por favor contacte:

João Peixe: joao.peixe@va.pt