

GUIA DE PROTEÇÃO DE DADOS PESSOAIS

AGENTES DE TRATAMENTO

CC.04.001.2024

OUTUBRO, 2024

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: AGENTES DE TRATAMENTO

VERSÃO 1 – OUTUBRO, 2024.

Diretoria de Controles Internos – DCI

Maria Alice da Justa Lemos
Diretora de Controles Internos

Analista responsável por este Guia:

Laila Sá Ferreira

Jordan Vinícius de Oliveira

Encarregado de Proteção de Dados Pessoais

Equipe Extracontratual:

Laila Sá Ferreira

Taís Povill Rocha

Alessandra Rigueti Barcellos

Nadja Nara da Cruz Ferreira Ribeiro

FICHA TÉCNICA

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

AVISO LEGAL

Este Guia foi elaborado pela Equipe do Encarregado de Proteção de Dados Pessoais da Fundação Getulio Vargas – FGV e tem como objetivo o compartilhamento de conhecimento envolvendo a conformidade de atividades de tratamento de dados pessoais para o tema escolhido.

O presente documento possui intuito meramente informativo, não sendo utilizado para fins de exploração comercial e apresenta a devida referência na página 2. Do mesmo modo, este documento não deve ser considerado como aconselhamento jurídico e não substitui a avaliação de uma equipe profissional de proteção de dados para cada caso.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

SUMÁRIO

1. CONTEXTUALIZAÇÃO	5
2. AGENTES DE TRATAMENTO	6
2.1. AGENTE DE TRATAMENTO PESSOA JURÍDICA	11
2.2. AGENTES DE TRATAMENTO DE PEQUENO PORTE	13
3. IMPORTÂNCIA DA DEFINIÇÃO DOS AGENTES DE TRATAMENTO	16
3.1. BOAS PRÁTICAS E GOVERNANÇA	20
3.2. RESPONSABILIDADE CIVIL	22
3.3. ATENDIMENTO AOS TITULARES	23
3.4. COMUNICAÇÃO DE INCIDENTES	26
3.5. ELABORAÇÃO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS	28
3.6. CONTRATOS E O PAPEL DO AGENTE DE TRATAMENTO	30
4. CONCLUSÃO	32
APÊNDICE ÚNICO	34
CHECKLIST PARA DEFINIR QUAL O PAPEL ENQUANTO AGENTE DE TRATAMENTO	34

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

1. CONTEXTUALIZAÇÃO

O presente Guia é um dos frutos do projeto de adequação da Fundação Getulio Vargas – FGV em relação à Lei Geral de Proteção de Dados ("LGPD"), aprovada em agosto de 2018, e outras leis setoriais sobre o tema.

A LGPD é aplicável a qualquer operação de tratamento de dados pessoais, seja ela realizada por pessoa natural, pessoa jurídica de direito privado ou pessoa jurídica de direito público. Na condição de Instituição de Ensino Superior ("IES"), a FGV desenvolve, entre outras atividades, operações de caráter administrativo, acadêmico e educacional (como por exemplo, a necessidade de guarda permanente de históricos escolares, provas, realização de pesquisas, desenvolvimento de projetos etc.). Nesse sentido, na condição de Instituição Educacional, a FGV deverá observar as obrigações normativas específicas das entidades públicas reguladoras, como, por exemplo, o Ministério da Educação ("MEC") e a Autoridade Nacional de Proteção de Dados ("ANPD").

Assim, a FGV desenvolveu, em maio de 2019, um projeto para cumprir com os objetivos de sua conformidade regulatória perante as leis de proteção de dados, denominado **Projeto Presidência – Implantação do Programa de Conformidade: Leis de Proteção de Dados Pessoais ("Projeto")**. Esta iniciativa, entre outras atividades, buscou parametrizar ações de conformidade da FGV ao novo contexto regulatório de proteção de dados, bem como, a partir das lições aprendidas, fornecer subsídios e materiais de apoio ao setor educacional.

Após a conclusão do Projeto inicial, a FGV criou a **Equipe do Encarregado de Proteção de Dados Pessoais**, no âmbito de sua Diretoria de Controles Internos ("DCI"). Esta Equipe tem como finalidade principal manter a FGV em adequação às normas de proteção de dados aplicáveis às suas atividades, bem como funcionar na condição de interlocutora junto aos variados setores da Organização, à ANPD, aos titulares de dados pessoais e aos demais agentes de tratamento.

O objetivo geral deste Guia é fornecer algumas diretrizes para a definição dos Agentes de Tratamento, principalmente no âmbito das atividades realizadas por IES.

Como objetivos específicos, este Guia pretende:

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

- (a) Apresentar as definições jurídicas trazidas pela LGPD aos agentes de tratamento, como os diferentes papéis, responsabilidades e regras aplicáveis conforme a sua natureza jurídica (pessoa jurídica, pessoa física, agente de pequeno porte);
- (b) Pontuar questões relativas a contratos e os diferentes papéis de agentes de tratamento que uma instituição pode figurar dentro de um mesmo instrumento; e
- (c) Apresentar um *checklist* para auxiliar na definição do papel de agente de tratamento.

2. AGENTES DE TRATAMENTO

Nesta seção serão abordadas questões gerais sobre os conceitos de agentes de tratamento. Primeiro, abordar-se-á o conceito de controlador e operador. Em seguida, serão apresentados pontos centrais sobre as figuras do controlador conjunto e do suboperador. Um terceiro tópico trabalha com situações nas quais o controlador não trata dados pessoais diretamente, mas, ainda assim, determina as formas de seu tratamento. Ainda, será apresentado um tópico de critérios gerais para a definição do papel de agentes de tratamento.

O tratamento¹ de dados pessoais, conforme se depreende da leitura e interpretação dos dispositivos contidos na LGPD, poderá ser realizado por pessoa física ou por pessoa jurídica de direito público ou privado, as quais podem ser chamadas de agentes de tratamento.

A LGPD define em seu art. 5º, IX que os agentes de tratamento correspondem ao: (i) controlador, responsável por tomar as decisões relativas ao tratamento; e (ii) operador, a quem compete realizar o tratamento em nome do primeiro.

Em um contexto de um curso educacional de Ensino Superior, por exemplo, imagine que uma determinada instituição de ensino contratou uma empresa para digitalizar todo o seu acervo acadêmico para fins de cumprir com obrigações legais de armazenamento desses documentos.

Nesse exemplo, a instituição educacional é considerada a controladora dos dados pessoais de seus alunos e professores, sendo a empresa de digitalização, por sua vez, a operadora. A empresa

¹ Nos termos do art. 5º, X da LGPD: **tratamento** é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

contratada, assim, apenas deverá seguir as instruções e exigências da instituição educacional, não podendo tomar novas decisões sobre o que fazer com os dados pessoais.

A LGPD, ao prever as figuras do controlador e do operador, contudo, não trouxe definição expressa sobre o chamado controlador conjunto, aquele que toma decisões sobre o tratamento de forma compartilhada com outro controlador para benefício mútuo. A ausência de definição da figura da controladoria conjunta na lei brasileira (especialmente em seu art. 5º) poderia suscitar dúvidas acerca de sua legalidade, uma vez que o GDPR (Regulamento Geral sobre Proteção de Dados, Regulamento da União Europeia nº 2016/679), previu expressamente essa figura ao seu artigo 26².

Contudo, a referida questão foi abordada pela ANPD em seu Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado³, o qual determina que a referida autoridade entende que a LGPD permite a figura da controladoria conjunta, com fulcro no seu art. 42, §1º, II⁴.

Ainda no âmbito da **controladoria conjunta**, faz-se uma observação importante. Conforme pontuado pelo *European Data Protection Supervisor* (EDPS)⁵ na aplicação do *General Data Protection Regulation* (Regulation EU 2016/679 – “GDPR”), a **controladoria conjunta** poderá ocorrer por uma das seguintes formas: (i) decisões comuns, tomadas por duas ou mais Entidades que possuem um objetivo em comum e conjuntamente determinam a finalidade e as orientações sobre o tratamento de dados pessoais; e/ou (ii) decisões convergentes, entendidas como determinações distintas tomadas por mais de uma Entidade que são complementares entre si, de modo que o tratamento do dado pessoal não seria possível sem a participação conjunta das instituições.

Contudo, como já bem pontuado no Guia Orientativo para Definições dos Agentes de Tratamento

² Art. 26: 1. Quando dois ou mais controladores conjuntamente determinam os propósitos e formas de tratamento, eles serão considerados controladores conjuntos (UNIÃO EUROPEIA. *Regulação (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Jornal Oficial da União Europeia, Bruxelas, 04 maio 2016.

³ BRASIL. Autoridade Nacional de Proteção de Dados. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, p. 13. Abril de 2022. Disponível em <[link](#)>. Acesso em: 08 de jan. de 2024.

⁴ Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

(...) II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

⁵ UNIÃO EUROPEIA. o European Data Protection Board – EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, p. 9. Setembro de 2020. Disponível em <[link](#)>. Acesso em 15 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

de Dados Pessoais e do Encarregado⁶, é preciso cuidado ao estabelecer que instituições são **controladoras conjuntas**, pois o tratamento de um mesmo conjunto de dados por mais de uma Entidade não será considerado **controladoria conjunta** caso as finalidades/objetivos do tratamento sejam distintas. Vê-se a situação exemplo apresentada no Guia supramencionado da ANPD:

(...) diversos controladores podem tratar dados abertos do governo, cada um para suas finalidades específicas. **Se estas finalidades não forem comuns, convergentes ou complementares, ambos serão controladores singulares em relação ao tratamento de dados** e a controladoria conjunta não estará estabelecida, o que afastaria a incidência do art. 42, §1º, II, da LGPD. (grifos nossos)⁷

No mesmo sentido, outro ponto geral que necessita de importante esclarecimento é o da situação em que um operador contrata terceiro para lhe auxiliar no tratamento dos dados pessoais, em nome do controlador. Neste cenário, o terceiro contratado seria um suboperador. Seguindo a mesma lógica supramencionada, por não haver previsão legal do “suboperador” na LGPD, seria possível suscitar dúvidas acerca desta figura. AANPD, contudo, no mesmo Guia mencionado anteriormente, também encerrou o referido debate ao determinar que:

(...) **a falta do conceito de suboperador na LGPD não impossibilita ou torna ilegal que ele exista ou que tenha funções, competências e responsabilidade no ambiente de proteção de dados pessoais brasileiro**, principalmente porque pode desempenhar a função de operador em subordinação a outro operador. Dito isso, importa saber que o suboperador é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador. (...)
(...) De maneira semelhante, **o RGPD também não traz uma definição para o suboperador**, limitando-se a definir o conceito de Operador (“Processor” em inglês/” Subcontratante” em português de Portugal) como consta no Artigo 4º do RGPD. Ainda assim, **a redação dos itens 2 e 4 do artigo 28 do RGPD prevê expressamente a possibilidade de um subcontratante contratar outro subcontratante**. (grifos nossos)⁸

Superado os supramencionados debates, e confirmando-se as figuras do controlador conjunto e do suboperador, têm-se que, ao tratar dados pessoais, uma instituição poderá ocupar uma das seguintes posições de agente, conforme definições extraídas do Guia elaborado pela ANPD⁹:

⁶ BRASIL. Autoridade Nacional de Proteção de Dados. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, p. 14. Abril de 2022. Disponível em <[link](#)>. Acesso em: 08 de jan. de 2024.
⁷ BRASIL. Autoridade Nacional de Proteção de Dados, op. cit., nota 6. p. 14.
⁸ BRASIL. Autoridade Nacional de Proteção de Dados, op. cit., nota 6. p. 19-20.
⁹ BRASIL. Autoridade Nacional de Proteção de Dados, op. cit., nota 6. p. 7-21.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	



PAPEL DO AGENTE DE TRATAMENTO

NO MOMENTO DO TRATAMENTO DOS DADOS PESSOAIS, AS INSTITUIÇÕES PODERÃO OCUPAR UMA DAS SEGUINTE POSIÇÕES

- **Controlador:** a quem compete as principais decisões referentes ao tratamento de dados pessoais e a sua finalidade, como por exemplo, mas não limitado, definição da base legal, os dados pessoais tratados, orientar os operadores etc.;
- **Controladoria Conjunta:** situação na qual duas ou mais instituições são responsáveis por determinar de forma conjunta, comum e/ou convergente a finalidade e demais nuances sobre uma ou mais operações de tratamento;
- **Operador:** responsável pela realização do tratamento segundo as orientações e determinações do controlador, tratando os dados em nome dele e conforme por ele definido; e
- **Suboperador:** contratado pelo operador, será responsável por realizar o tratamento de dados pessoais conjuntamente com ele. Sua relação, contudo, será diretamente com o operador que ficará responsável por repassar as orientações dadas pelo controlador; sendo que para efeitos da LGPD, no caso concreto, desempenhará a função de operador.

Vê-se que o **controlador** é o agente responsável por tomar as principais decisões que contribuirão para o cumprimento da finalidade que ensejou o tratamento de dados pessoais, como, por exemplo, quais dados pessoais serão tratados e sua natureza, o tempo de duração do tratamento e eventual eliminação, a finalidade, entre outras responsabilidades.

Nesse ínterim, pode-se dizer que o **controlador** é o principal interessado naquele tratamento para aquele objetivo específico. Todavia, isso não significa dizer que ele terá que tomar todas as decisões. Dentro de uma operação – especialmente aquelas em que se tem a atuação de um **operador** –, ainda que o **controlador** não seja responsável por definir alguns pontos e/ou especificidades técnicas, ele ocupará esse papel em decorrência do seu “poder de decisão”¹⁰ sobre os pontos essenciais à execução da finalidade, que são de seu interesse e responsabilidade. Faz-se menção, aqui, ao exposto pela ANPD em seu Guia sobre agentes de tratamento:

De acordo com o disposto na LGPD, o controlador é o responsável por tomar as ‘decisões referentes ao tratamento de dados pessoais’ (art. 5º, VI).
Extrai-se dessa disposição legal que **o tratamento não precisa ser realizado diretamente pelo controlador**. Muito embora o controlador também trate dados pessoais, **o elemento distintivo é o poder de decisão, admitindo-se que o controlador forneça instruções para que um terceiro (‘operador’) realize o tratamento em seu nome** (art. 5º, VII; art. 39). (grifos nossos)¹¹

¹⁰ BRASIL. Autoridade Nacional de Proteção de Dados. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, p. 11. Abril de 2022. Disponível em <[link](#)>. Acesso em: 08 de jan. de 2024.

¹¹ BRASIL. Autoridade Nacional de Proteção de Dados, op. cit., nota 10. p. 11.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

No que diz respeito à função do **operador**, tem-se que, conforme definido acima e previsto em lei, ele deve agir conforme “as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria”¹². Não tem, portanto, o poder de decisão acerca das principais nuances do tratamento para atingir uma finalidade, podendo apenas determinar alguns escopos técnicos sobre sua atuação, como, por exemplo, o software que será utilizado.

No âmbito do agente **suboperador**, tendo-se em vista o papel central do **controlador** e em consonância com as orientações da ANPD¹³, recomenda-se que a questão, sempre que possível, seja avaliada por contrato, especialmente onde houver maior risco.

Abaixo, seguem exemplos sobre a definição dos agentes de tratamento:

Tipos de Agentes	Exemplo
Controlador	<ul style="list-style-type: none"> Um curso de idiomas envia e-mail para os alunos matriculados e para ex-alunos sobre oportunidade de intercâmbio com desconto em instituições estrangeiras parceiras. O curso, pessoa jurídica, é controlador dos dados pessoais de contato. Um fotógrafo, profissional liberal, armazena em ambiente de nuvem formulários cadastrais de pessoas naturais com interesse em contratá-lo, bem como mantém pastas com as fotos de todos os seus clientes. O fotógrafo, pessoa física, é controlador.
Controlador Conjunto	<ul style="list-style-type: none"> A Instituição W desenvolveu um projeto de pesquisa em parceria com a Faculdade B e que contará com o tratamento de dados pessoais. Ambas as instituições têm interesse no produto oriundo do projeto, bem como tomam todas as decisões referentes a ele, como, por exemplo, o tema, a finalidade, a metodologia, o cronograma, entre outras especificidades necessárias ao seu desenvolvimento. Portanto, ambas são consideradas controladoras conjuntas dos dados pessoais tratados no âmbito da pesquisa.
Operador	<ul style="list-style-type: none"> Instituição XY é contratada para organizar o processo seletivo de vestibular de uma Faculdade, devendo seguir as regras estipuladas no Edital e observar outros pontos que são exigidos à Faculdade nesse processo seletivo pelo Ministério da Educação. A Faculdade é a controladora dos dados pessoais, enquanto a Instituição XY é a operadora que tratará os dados dos inscritos para desenvolver o processo seletivo em nome da Faculdade.
Suboperador	<ul style="list-style-type: none"> Empresa de ônibus contrata empresa de software para gerenciar seu sistema de passagens. Esta segunda empresa, por sua vez, tem contratada uma solução de armazenamento em nuvem com uma terceira empresa, onde ficarão todos os registros da empresa de ônibus. Neste caso, a empresa de armazenamento em nuvem é suboperadora da empresa de software, sendo a empresa de ônibus a controladora.

¹² BRASIL. Art. 39 da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

¹³ BRASIL. Autoridade Nacional de Proteção de Dados. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, p. 20. Abril de 2022. Disponível em <[link](#)>. Acesso em: 08 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

A definição do papel dos agentes de tratamento deverá sempre levar em consideração a situação fática e jurídica na qual a instituição está inserida¹⁴. Assim, de forma a encerrar o presente item, faz-se as seguintes orientações:



DICA

SOBRE CRITÉRIOS GERAIS DISTINTIVOS

- A definição do papel dos agentes durante operações deve levar em consideração o papel da Entidade dentro de tratamento específico. Para auxílio na definição do papel da instituição enquanto agente de tratamento consulte o **checklist disponível no Apêndice Único deste Guia**;
- Havendo mais de um agente de tratamento na operação, recomenda-se elaborar instrumento (ex.: contrato) de forma a determinar o papel das Entidades envolvidas (se controlador, operador, controlador conjunto) e delimitar as obrigações de cada parte;
- Em caso de dúvidas ou dificuldades na definição, ou para elaboração de instrumento, é recomendado consultar a equipe do encarregado de proteção de dados da instituição ou a área que auxilia no tema de proteção de dados pessoais.

2.1. AGENTE DE TRATAMENTO PESSOA JURÍDICA

Ainda dentro do escopo geral de agentes de tratamento, merece destaque o agente de tratamento pessoa jurídica. O presente subcapítulo visa elucidar o papel desse tipo de agente de tratamento e a posição dos seus funcionários/colaboradores.

A pessoa jurídica, seja ela de direito público ou privado, ao tratar dados pessoais, será considerada agente de tratamento, sendo que o papel de controlador/controlador conjunto ou de operador/suboperador recairá sobre a Entidade como um todo. Assim, os funcionários, colaboradores e/ou qualquer outro profissional subordinado, vinculado ou membro da pessoa jurídica não serão considerados pessoalmente como agentes de tratamento e não poderão ocupar o papel de controlador ou operador.

Nesse sentido, o encarregado de proteção de dados pessoais, por sua vez, ao ser indicado para ocupar esse cargo por pessoa jurídica, não será considerado pessoalmente o agente de tratamento – controlador ou operador. A ele caberá apenas a função de ser o representante da pessoa jurídica competente para assuntos relacionados ao tema de proteção de dados pessoais e a LGPD.

¹⁴ UNIÃO EUROPEIA. o European Data Protection Board – EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, p. 9. Setembro de 2020. Disponível em <[link](#)>. Acesso em 15 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Conforme definido no art. 5º, VIII da LGPD, o encarregado é a “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)”¹⁵. Portanto, não será considerado pessoalmente como agente de tratamento de uma operação, papel que será direcionado à Entidade que representa.

A ANPD discorreu, inclusive, sobre a impossibilidade do papel de agente (controlador ou operador) pessoa jurídica ser atribuído diretamente a uma pessoa vinculada a ela, conforme descrito abaixo:

(...) não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos. É o caso de empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta. Nesse sentido, a definição legal de controlador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades. De forma diversa, trata-se de comando legal que atribui obrigações específicas à pessoa jurídica, de modo que esta assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD.¹⁶

Assim, o Presidente de uma Fundação ou de um Órgão Público, o sócio administrador de uma Empresa ou o encarregado de proteção de dados indicado por uma Entidade não serão considerados controladores ou operadores de acordo com a LGPD, pois esta posição de agente de tratamento, no contexto citado, caberá de forma exclusiva à pessoa jurídica (à Fundação/Órgão Público, Empresa, Entidade). A título exemplificativo, se uma Instituição Educacional figura como agente de tratamento, podendo ocupar a posição de controladora ou operadora em determinada operação em que trate dados pessoais, o(a) seu(sua) Diretor(a), Reitor(a), Presidente figurará como representante legal e não se confundirá com a própria entidade agente de tratamento, sendo o seu Encarregado o responsável por representar e intermediar a relação entre essa instituição, os titulares e as Autoridades no âmbito da LGPD.



ATENÇÃO!

A indicação como agente de tratamento (controlador ou operador) de pessoas físicas que exerçam funções de liderança em Pessoa Jurídica (presidentes, diretoras, chefes de departamento, encarregadas de proteção de dados e assemelhadas), ou que a ela esteja vinculado como funcionário, colaborador, entre outros, **não está correta de acordo com a LGPD!**

¹⁵ BRASIL. Art. 5º, VIII da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

¹⁶ BRASIL. Autoridade Nacional de Proteção de Dados. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, p. 9. Abril de 2022. Disponível em <[link](#)>. Acesso em: 08 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

2.2. AGENTES DE TRATAMENTO DE PEQUENO PORTE

Um outro ponto de importância no que diz respeito ao capítulo 2 são os agentes de tratamento de pequeno porte, que poderão figurar em qualquer dos papéis descritos anteriormente. Assim, o presente subcapítulo tem por objetivo elucidar quais instituições poderão ser consideradas como agentes de pequeno porte e outros pontos de relevância que foram objeto de regulamentação pela ANPD.

Em 27 de janeiro de 2022, a ANPD publicou a Resolução CD/ANPD nº 2, que tem por objetivo regular a aplicação da LGPD a empresas, instituições e/ou organizações às quais se refere como agentes de tratamento de pequeno porte. Nos termos do art. 2º da referida Resolução, serão considerados como de pequeno porte:

- (i) Microempresas ou empresas de pequeno porte, assim definidas as sociedades empresárias, simples e limitada unipessoal, conforme art. 41 da Lei nº 14.195/2021¹⁷. Ainda, inclui-se, para fins do referido regulamento, o empresário como previsto no art. 966 do Código Civil¹⁸, e microempreendedor individual registrado no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas que preencham os requisitos dos artigos 3º e 18-A, §1º da Lei Complementar nº 123/2006¹⁹;
- (ii) Startups, consideradas as organizações empresariais ou societárias, novas ou em atuação recente, “cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no Capítulo II da Lei Complementar nº 182, de 1º de junho de 2021”²⁰;

¹⁷ Conforme art. 41. da Lei nº 14.195/2021 “As empresas individuais de responsabilidade limitada existentes na data da entrada em vigor desta Lei serão transformadas em sociedades limitadas unipessoais independentemente de qualquer alteração em seu ato constitutivo”. Disponível em <link>, acesso em 23 de jan. 2024.

¹⁸ Conforme art. 966 da Lei 10.406/2002 – Código Civil “Considera-se empresário quem exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços”. Disponível em <link>, acesso em 23 de jan. 2024.

¹⁹ Conforme art. 3º da Lei Complementar nº 123/2006 “Para os efeitos desta Lei Complementar, consideram-se microempresas ou empresas de pequeno porte, a sociedade empresária, a sociedade simples, a empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei no 10.406, de 10 de janeiro de 2002 (Código Civil), devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, conforme o caso, desde que: I - no caso da microempresa, aufera, em cada ano-calendário, receita bruta igual ou inferior a R\$ 360.000,00 (trezentos e sessenta mil reais); e II - no caso de empresa de pequeno porte, aufera, em cada ano-calendário, receita bruta superior a R\$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R\$ 4.800.000,00 (quatro milhões e oitocentos mil reais)”. Disponível em <link>, acesso em 23 de jan. 2024.

²⁰ BRASIL. Autoridade Nacional de Proteção de Dados. Art. 2º, III da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022. Disponível em <link>, acesso em 23 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

- (iii) Pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente; e
- (iv) Pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais e assumam obrigações típicas de controlador ou operador.

A partir da leitura da referida norma, a sua finalidade é a flexibilização de algumas obrigações e orientações estabelecidas pela LGPD a esses agentes de tratamento de pequeno porte, de modo que a adequação e proteção dos dados não se torne um empecilho a suas atividades ou tenha custo extremamente alto. Contudo, conforme consta no art. 3º da Resolução supramencionada, o tratamento jurídico diferenciado **não se estende caso os agentes de pequeno porte:**

I - realizem tratamento de alto risco para os titulares, ressalvada a hipótese prevista no art. 8º;

II - auferirem receita bruta superior ao limite estabelecido no art. 3º, II, da Lei Complementar nº 123, de 2006 ou, no caso de startups, no art. 4º, § 1º, I, da Lei Complementar nº 182, de 2021; ou

III - pertençam a grupo econômico de fato ou de direito, cuja receita global ultrapasse os limites referidos no inciso II, conforme o caso. (grifos nossos)²¹

No que diz respeito aos incisos II e III acima mencionados, não há dúvidas sobre eventual auferimento de receita superior a limite estabelecido, havendo, inclusive, menção à legislação específica. Contudo, a definição de alto risco pode gerar dúvidas. Assim, para fins de auxílio e clareza ao agente de pequeno porte do que seria um tratamento de alto risco, a ANPD determinou, no caput do art. 4º da Resolução ora em análise, que se configurará tratamento de alto risco quando preenchido cumulativamente pelo menos um critério geral, estabelecidos no inciso I do artigo, e um critério específico, elencados no inciso II:

Critérios Gerais	- Tratamento de dados pessoais em larga escala;
	- Tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares.
Critérios específicos	- Uso de tecnologias emergentes ou inovadoras;
	- Vigilância ou controle de zonas acessíveis ao público;
	- Decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular;
	- Utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

²¹ BRASIL. Autoridade Nacional de Proteção de Dados. *Art. 3º da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022*. Disponível em <[link](#)>, acesso em 23 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Ainda, os §§ 1º e 2º do dispositivo supramencionado orientam os agentes de pequeno porte sobre quais características deverão ser observadas para configurar “larga escala” e/ou “afetar significativamente interesses e direitos fundamentais”, auxiliando de forma mais precisa os agentes de pequeno porte na avaliação do tratamento de alto risco:

§ 1º O tratamento de dados pessoais em larga escala será caracterizado quando abranger **número significativo de titulares**, considerando-se, ainda, **o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado**.

§ 2º O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que **a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade**. (grifos nossos)²²



EXEMPLO STARTUP

Imagine que uma Startup de direito privado desenvolva uma solução de segurança que faça cruzamentos de fotos e vídeos de procurados com imagens publicadas em perfis em redes sociais, de modo a comercializar a solução com entidades de segurança pública e privada:

- A análise dos perfis públicos é feita por meio de uma ferramenta totalmente automatizada que consulta os respectivos perfis e tenta traçar pontos em comum da face nas fotos.

Na situação hipotética ora apresentada, vê-se que a Startup não poderá se valer das benesses da Resolução CD/ANPD nº 2 de 2022, uma vez que diversos requisitos listados ao inciso II do artigo 4º estão presentes, como tratamentos em larga escala e que afetem direitos e interesses dos titulares, tecnologia emergente, tratamento automatizado e de dados biométricos.

Importante destacar que esta Resolução não isenta os agentes de tratamento de pequeno porte de cumprir e observar a LGPD²³, ela apenas flexibiliza algumas obrigações estipuladas pela Lei. Assim, os agentes de tratamento de pequeno porte deverão observar os princípios, a base legal aplicável, entre outras obrigações/determinações estipuladas pela LGPD e não flexibilizadas na norma.

²² BRASIL. Autoridade Nacional de Proteção de Dados. *Art. 4º da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022*. Disponível em <[link](#)>, acesso em 23 de jan. de 2024.

²³ BRASIL. Autoridade Nacional de Proteção de Dados. *Art. 6º da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022*. Disponível em <[link](#)>, acesso em 23 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Por fim, conforme determina o §3º do art. 4º da referida Resolução, caberá ao agente de tratamento, quando solicitado pela ANPD, comprovar que se enquadra como de pequeno porte e que não configura uma das hipóteses previstas no art. 3º deste mesmo diploma legal, podendo, portanto, se valer das regras especiais estipuladas. Ainda, a ANPD poderá determinar que o agente de tratamento de pequeno porte cumpra todas as obrigações dispensadas e/ou flexibilizadas pela Resolução, a depender das circunstâncias do tratamento²⁴.

As flexibilizações das obrigações estabelecidas na Resolução em análise serão abordadas mais detalhadamente no próximo capítulo, o qual versará sobre a importância da definição dos papéis de agentes de tratamento.



ATENÇÃO!

- **A Resolução CD/ANPD nº 2/2022 não afasta a aplicabilidade da LGPD.** A referida norma tem por objetivo flexibilizar e/ou prever orientações diferenciadas aos agentes de pequeno porte, em razão do seu tamanho e do custo envolvido na adequação à LGPD, de modo que o cumprimento à lei seja viável e adequado a eles;
- As normas e obrigações estabelecidas pela LGPD e não flexibilizadas pela referida Resolução deverão ser integralmente observadas e cumpridas pelos agentes de pequeno porte.

3. IMPORTÂNCIA DA DEFINIÇÃO DOS AGENTES DE TRATAMENTO

Feitas as considerações sobre agentes de tratamento e a definição dos respectivos papéis que uma pessoa física ou jurídica poderá ocupar, passa-se à análise da importância dessa determinação.

Neste capítulo, abordar-se-ão as principais responsabilidades previstas em lei de acordo com o papel de agente de tratamento, incluindo-se, ainda, as obrigações flexibilizadas aplicáveis aos agentes de tratamento de pequeno porte mencionados anteriormente. Ressalta-se que no decorrer da lei poderá haver outras obrigações, as quais **não** serão mencionadas no presente Guia, tendo-se em vista que o objetivo é trazer, de forma geral, o tema agentes de tratamento, sem, contudo, tratá-lo de forma exaustiva.

²⁴ BRASIL. Autoridade Nacional de Proteção de Dados. *Art. 16 da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022*. Disponível em <[link](#)>, acesso em 23 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Conforme mencionado anteriormente, o controlador e o operador possuirão diferentes atribuições ao longo do tratamento dos dados pessoais, evidente, pois, que as responsabilidades e obrigações previstas na LGPD serão diferentes para cada tipo de agente de tratamento, tornando-se imprescindível a definição dos papéis para o correto cumprimento da lei, evitando-se, inclusive, que uma Entidade assumira obrigações não compatíveis com os seus deveres legais.

Portanto, cabe iniciar este tópico abordando uma obrigação mais geral e orientativa e que é primordial para a definição do papel de agente: a tomada de decisão dos principais elementos do tratamento de dados pessoais para uma finalidade determinada/específica.

Conforme já descrito, cabe ao controlador tomar as principais decisões que impactarão direto no tratamento, visando o alcance de sua finalidade. Isto significa dizer que a ele compete definir, por exemplo, mas não limitado: (i) a finalidade/objetivo do tratamento, a razão para qual os dados pessoais serão necessários; (ii) quais dados pessoais precisarão ser tratados para atingir essa finalidade, se sensíveis²⁵ ou não²⁶; (iii) as bases legais aplicáveis para autorizar o tratamento; e (iv) as regras para armazenamento e segurança dos dados pessoais.

Ressalta-se, novamente, que os itens acima são meramente exemplificativos, sendo certo que dentro de uma operação de tratamento poderão existir elementos ou pontos de decisão considerados necessários e essenciais ao cumprimento da finalidade, os quais serão, via de regra, obrigatoriamente de responsabilidade do controlador (salvo se houver previsão contratual em sentido contrário estipulada entre controlador e operador em um determinado caso concreto e essa previsão não implicar isenção/transferência de responsabilidade legal).

No que diz respeito ao operador, este agente de tratamento deverá seguir as instruções e determinações feitas pelo controlador, conforme define o art. 39 da LGPD: “Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria”.²⁷

²⁵ Segundo a LGPD, dado sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural – art. 5º, II da LGPD.

²⁶ Segundo a LGPD, dado pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável – art. 5º, I da LGPD.

²⁷ BRASIL. Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Tal previsão legal não impede que o operador possa tomar decisões técnicas relevantes para o tratamento de dados pessoais. Salvo se houver impedimento em contrato com um controlador, as decisões sobre especificidades técnicas ou que não afetem diretamente no objeto/finalidade do tratamento **poderão** ser tomadas pelo próprio operador, observadas as disposições da LGPD, como por exemplo a definição da utilização de um software ou determinado ambiente para armazenar os dados pessoais e questões de ordem técnica sobre o uso seguro dos dados.

Ainda, as considerações acima, sobre definição do papel do agente de tratamento, são aplicáveis aos agentes de tratamento de pequeno porte, não havendo nenhuma flexibilização e/ou diferenciação ao controlador/operador que se encaixar nessa categoria.

Dando continuidade às orientações mais gerais sobre as obrigações dos agentes de tratamento, é necessário mencionar a nomeação da figura do Encarregado de Proteção de Dados, definido no art. 5º, VIII da LGPD como “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)”²⁸.

O art. 41 da referida norma determina que o controlador deverá indicar o encarregado pelo tratamento de dados pessoais e, conforme estabelecido pela Resolução CD/ANPD nº 18 de 16 de julho de 2024 (norma que aprovou o regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais), esta nomeação deverá ser realizada por ato formal²⁹ do agente de tratamento controlador³⁰. Ainda, a divulgação da identidade do encarregado pelo agente de tratamento deverá observar o disposto no art. 9º da referida Resolução, *in verbis*:

Art. 9º A identidade e as informações de contato do encarregado deverão ser **divulgadas publicamente**, de forma clara e objetiva, **em local de destaque e de fácil acesso**, no sítio eletrônico do agente de tratamento, ressalvada a hipótese do § 3º deste artigo.

§ 1º A divulgação da identidade do encarregado abrangerá, no mínimo:

I - **o nome completo, se for pessoa natural**; ou

II - o nome empresarial ou o título do estabelecimento, bem **como o nome completo da pessoa natural responsável, se pessoa jurídica**.

§ 2º A divulgação das informações de contato do encarregado abrangerá, no mínimo, os **dados referentes aos meios de comunicação que viabilizem o**

²⁸ BRASIL. Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

²⁹ Entende-se por ato formal “o documento escrito, datado e assinado, que, de maneira clara e inequívoca, demonstre a intenção do agente de tratamento em designar como encarregado uma pessoa natural ou uma pessoa jurídica.”, nos termos do §1º da Resolução CD/ANPD nº 18 de 16 de julho de 2024.

³⁰ BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 18 de 16 de julho de 2024*. Disponível em <[link](#)>, acesso em 23 de jul. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

exercício dos direitos dos titulares junto ao controlador e possibilitem o recebimento de comunicações da ANPD.

§ 3º O agente de tratamento que **não possuir sítio eletrônico** poderá realizar a **divulgação da identidade e das informações de contato do encarregado por quaisquer outros meios de comunicação disponíveis**, especialmente aqueles usualmente utilizados para contato com os titulares. (grifos nossos)³¹

Importante destacar, ainda, que a Resolução supramencionada determina em seu art. 6º que o agente de tratamento que figurar na posição de operador não está obrigado a indicar formalmente um encarregado sendo que, se o fizer na forma acima, o ato poderá ser considerado como boa prática³².

Assim, tendo-se em vista que a posição da instituição poderá variar a depender da situação concreta (em poucas situações o agente de tratamento será exclusivamente operador), é recomendável que a indicação de Encarregado de Proteção de Dados seja feita conforme orientações da Resolução CD/ANPD nº 18/2024.

No que diz respeito aos agentes de pequeno porte, tem-se que a Resolução CD/ANPD nº 2/2022, em seu art. 11, flexibilizou a regra contida no art. 41 da LGPD, não sendo necessário que essa categoria de agente indique um encarregado pelo tratamento de dados pessoais, conforme também determinado no §3º do art. 3º da Resolução CD/ANPD nº 18/2024. Caso o agente indique o encarregado, tal medida será considerada uma boa prática, nos termos do §2º, do art. 11 da Resolução CD/ANPD nº 2/2022.

Contudo, caso opte por não indicar um encarregado, o agente de pequeno porte deverá obrigatoriamente disponibilizar um canal de comunicação para o titular, de modo a atender reclamações e comunicações desse último, bem como adotar providências e prestar esclarecimentos às Autoridades quando necessário³³.

Delimitadas as obrigações gerais impostas aos agentes de tratamento, dar-se-á continuidade a este capítulo abordando as orientações/obrigações no âmbito do tratamento de dados pessoais mais

³¹ BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 18 de 16 de julho de 2024*. Disponível em <link>, acesso em 23 de jul. de 2024.

³² O Art. 6º da Resolução CD/ANPD nº 18 de 16 de julho de 2024 assim determina: “A indicação de encarregado por operadores é facultativa e será considerada política de boas práticas de governança para fins do disposto no art. 52, § 1º, inciso IX, da Lei nº 13.709, de 14 de agosto de 2018, e no art. 13, inciso II, do anexo da Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, desde que observadas as normas deste Regulamento.”

³³ BRASIL. Autoridade Nacional de Proteção de Dados. *Art. 11, §1º da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022*. Disponível em <link>, acesso em 23 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

específicas, além do atendimento a direitos dos titulares, aspectos sobre responsabilidade civil, gestão de incidentes e elaboração de relatório de impacto.



DICA

NOMEAÇÃO ENCARREGADO DE PROTEÇÃO DE DADOS

- Tendo-se em vista que as instituições poderão figurar ora como controladores, ora como operadores a depender da situação concreta, **recomenda-se a nomeação do encarregado pelo tratamento de dados pessoais** nos termos do art. 41 da LGPD e observadas as orientações constantes da Resolução CD/ANPD nº 18/2024;
- **Aos agentes de tratamento de pequeno porte também se recomenda a nomeação do encarregado** nos termos do art. 41 da LGPD, ainda que a Resolução CD/ANPD nº 2/2022 tenha flexibilizado, tendo-se em vista que tal indicação será vista como boa prática.

3.1. BOAS PRÁTICAS E GOVERNANÇA

Este primeiro subcapítulo abordará uma obrigação que deverá ser observada por ambos os agentes de tratamento, controlador e operador, quais sejam adoção de boas práticas e governança para garantir o cumprimento das legislações de proteção de dados e a segurança da informação, prevenindo a ocorrência de incidentes.

O art. 50 da LGPD assim determina:

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.³⁴

Portanto, caberá a ambos os agentes de tratamento analisar, a partir do seu contexto operacional e do nível de risco das atividades por eles conduzidas, as medidas técnicas e organizacionais mais apropriadas. O nível de sofisticação dos padrões técnicos exigidos de uma instituição financeira, por exemplo, será relativamente maior do que os exigidos de um pequeno *e-commerce* que funciona em uma rede social.

³⁴ BRASIL. Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Ao adotar as medidas apropriadas para sua instituição, o agente de tratamento deverá levar em consideração, para a definição, a natureza dos dados, o escopo do tratamento, a finalidade para qual ele se dirige, a probabilidade de ocorrer eventos adversos que possam causar incidente, a gravidade dos riscos e quais os benefícios aos titulares³⁵, podendo implementar programas de governança em privacidade que, no mínimo³⁶:

- **Demonstrem o comprometimento do controlador na adoção de políticas internas que assegurem o cumprimento das normas de boas práticas à proteção de dados pessoais;**
- **Se aplique a todo o conjunto de dados pessoais tratados pela instituição e que estão sob seu controle;**
- **Se adapte à estrutura, escala e ao volume das operações e da sensibilidade dos dados;**
- **Estabeleça políticas e salvaguardas apropriadas, tendo-se em vista o processo de avaliação sistemática de impactos e riscos à privacidade;**
- **Estabeleça uma relação de confiança com o titular, atuando de forma transparente e com mecanismos que assegurem a participação dos titulares;**
- **Esteja integrado com a estrutura geral de governança da instituição, aplicando mecanismos de supervisão interna e externamente;**
- **Possua planos de respostas a incidentes e remediação;**
- **Seja atualizado constantemente.**

Aos agentes de pequeno porte, por sua vez, também será necessária a adoção de boas práticas de modo a garantir o tratamento adequado à LGPD. Contudo, a Resolução CD/ANPD nº 2/2022, trouxe em seus artigos 12 e 13, orientações simplificadas de como aderir a boas práticas, conforme a transcritos a seguir:

Art. 12. Os agentes de tratamento de pequeno **porte devem adotar medidas administrativas e técnicas essenciais e necessárias, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais**, considerando, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento.

(...)

Art. 13. Os agentes de tratamento de pequeno porte **podem estabelecer política simplificada de segurança da informação**, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda,

³⁵ BRASIL. Art. 50, §1º da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

³⁶ BRASIL. Art. 50, §2º da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (grifos nossos).³⁷

Ainda que a adoção de boas práticas em um formato simplificado seja obrigatória, é facultado ao agente de pequeno porte elaborar política de segurança da informação, em formato simplificado, que será considerada como boas práticas e governança na eventualidade de ser aplicada alguma sanção/penalidade, nos termos do art. 52, §1º, VIII e X da LGPD³⁸.

Ainda, a ANPD já publicou Guia Orientativo Segurança da Informação para Agentes de Tratamento de Pequeno Porte, disponível neste [link](#), que é um guia de boas práticas à segurança da informação endereçados a esses agentes, levando-se em consideração seu tamanho e as possíveis limitações existentes, o qual se recomenda fortemente a leitura, caso a instituição se enquadre como de pequeno porte.

Não há dúvidas, pois, que a adoção de boas práticas pelas instituições é mandatória e devem ser observadas tanto pelo controlador quanto pelo operador quando do regular tratamento de dados pessoais.



DICA

ADOÇÃO DE BOAS PRÁTICAS

- Recomenda-se que as instituições analisem o mercado para avaliar como outros agentes de tratamento estão se adequando à LGPD e quais os mecanismos técnicos/administrativos disponíveis, permitindo a compreensão do ambiente externo ao qual está inserido e assim auxiliar nas decisões necessárias à elaboração e condução de um programa de governança.

3.2. RESPONSABILIDADE CIVIL

ALGPD estabelece que ambos os agentes de tratamento são responsáveis pelos danos que vierem a causar a outrem, em razão de violação à legislação de proteção de dados pessoais, seja de ordem patrimonial, moral, individual ou coletivo³⁹.

³⁷ BRASIL. Autoridade Nacional de Proteção de Dados. *Arts. 12 e 13 da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022*. Disponível em <[link](#)>, acesso em 23 de jan. de 2024.

³⁸ BRASIL. Autoridade Nacional de Proteção de Dados. *Arts. 12, §1º e 13, §2º da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022*. Disponível em <[link](#)>, acesso em 23 de jan. de 2024.

³⁹ BRASIL. Art. 42 da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Dessa maneira, não se tratando de uma das hipóteses previstas no art. 43 desse mesmo diploma legal⁴⁰ – em que a responsabilização poderá ser afastada –, caberá ao agente de tratamento reparar o dano causado ao titular e/ou qualquer outra pessoa física/jurídica afetada por ele.

Contudo, pela leitura do art. 42, §1º, vê-se que tal responsabilidade é do controlador, sendo que o operador poderá responder de forma solidária somente nos casos⁴¹ abaixo descritos, situações nas quais será equiparado a figura do controlador:

- (a) Agir em desconformidade com as obrigações e determinações estipuladas pela LGPD; e
- (b) Não seguir as instruções lícitas do controlador.

Isto significa dizer que: violada a LGPD ou qualquer outra norma/regulamento relativo à proteção de dados pessoais, o controlador deverá reparar o dano causado ao titular e/ou terceiros, cabendo ao operador a responsabilidade solidária se sua conduta se encaixar em uma das duas hipóteses descritas acima.

Em situação de controladoria conjunta, a responsabilidade dos controladores observará o seu envolvimento concreto no tratamento de dados que ocasionou eventual dano ao titular, conforme determina o art. 42, §1º, II da LGPD, *in verbis*:

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.⁴²

Por fim, no que diz respeito à responsabilidade de agentes de tratamento de pequeno porte, não há nenhum tipo de flexibilização ou orientação diversa, sendo estes responsáveis por eventual descumprimento de legislação de proteção de dados pessoais nos termos descritos anteriormente.

3.3. ATENDIMENTO AOS TITULARES

⁴⁰ A saber, conforme o art. 43 da LGPD, os agentes de tratamento não poderão ser responsabilizados caso consigam provar que: (i) não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou (iii) o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

⁴¹ BRASIL. Art. 42, §1º, I da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

⁴² BRASIL. Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Outra obrigação atribuída em lei exclusivamente ao controlador são os atendimentos de solicitações de titulares. Conforme previsto no Capítulo III da LGPD, o controlador deverá receber e analisar, de forma gratuita e simplificada, todas as requisições de direito que sejam feitas por titulares de dados.

Os direitos que podem ser solicitados pelos titulares ao controlador, e constam no Capítulo III da referida lei, são: (i) confirmação de tratamento, (ii) acesso aos dados pessoais tratados, (iii) correção dos dados pessoais, (iv) eliminação/exclusão dos dados pessoais, (v) direito de interrupção (anonimização, bloqueio ou eliminação), (vi) direito de oposição, (vii) direito à portabilidade, e (viii) direito à revogação do consentimento. O direito de petição à ANPD deverá ser exercido diretamente à Autoridade, não tendo o controlador competência e/ou responsabilidade em seu recebimento, condução e/ou atendimento.

Ressalta-se que, para além de requisições de direitos, o titular poderá, eventualmente, entrar em contato com o controlador para esclarecer dúvidas pontuais sobre o tratamento dos seus dados, sendo de responsabilidade deste agente auxiliá-lo no que tange à LGPD e a dados pessoais.

É importante destacar que o controlador tem o dever de receber e analisar a requisição encaminhada por titular, o que não significa dizer que ele precisará, necessariamente, acatar ou deferir o direito solicitado. Existem direitos, como por exemplo o de exclusão, que não são absolutos e dependem de uma análise fática, jurídica e técnica sobre sua viabilidade. Assim sendo, ao receber e analisar um direito, caso o controlador entenda que não será possível atendê-lo, ele deverá responder ao titular justificando os motivos que ensejaram a negativa da solicitação.

É importante destacar que não há na LGPD, ou qualquer regulamentação por parte da ANPD⁴³, a forma e modo como devem ser encaminhadas e recebidas as solicitações feitas por titulares. Caberá, portanto, ao controlador definir um meio próprio para recebimento dessas requisições (por exemplo: e-mail ou sistema específico) e divulgá-lo para que o titular fique ciente do canal que poderá entrar em contato com o controlador.

O operador, por sua vez, não tem a obrigatoriedade de atender a direitos dos titulares conforme se depreende da leitura da LGPD. Observada a liberdade contratual, não há na lei disposição que impeça o controlador e operador de negociarem que o último se torne responsável por atender os direitos dos titulares de dados pessoais. Contudo, ressalta-se apenas que tal obrigação não poderá

⁴³ Até a data de publicação deste Guia não houve manifestação da ANPD sobre como deve ocorrer o atendimento a direitos dos titulares.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

violar a LGPD e nem servir de subterfúgio para eximir a responsabilidade do controlador perante os direitos que este deve garantir junto aos titulares.

Assim, via de regra, ao operador caberá auxiliar o controlador caso o atendimento ou a resposta à demanda encaminhada dependa de elementos que estão sob o domínio do primeiro em razão de sua atuação como operador. Caso seja necessário auxílio do operador, o controlador deverá solicitá-la diretamente a ele, que deverá responder dentro dos seus limites e responsabilidades.

No âmbito dos agentes de pequeno porte, tem-se que, enquanto figurarem como controladores, também estarão obrigados a receber e analisar solicitações de direitos dos titulares, conforme determinam os artigos 6º e 7º da Resolução CD/ANPD nº 2/2022. Com intuito de auxiliar esses agentes controladores, a Resolução os facultou a possibilidade de se organizarem “por meio de entidades de representação da atividade empresarial, por pessoas jurídicas ou por pessoas naturais para fins de negociação, mediação e conciliação de reclamações apresentadas por titulares de dados”⁴⁴, de modo que possa ser operacional e financeiramente facilitado.

Ainda, a referida Resolução, em seu art. 14, estabeleceu que os prazos para os agentes de pequeno porte serão em dobro daqueles estabelecidos na LGPD e/ou posteriormente por meio de regulamento da ANPD, prevendo especificamente em seus incisos I e III, respectivamente, que o atendimento a solicitações de titulares conforme art. 18, §§3º e 5º e o prazo estabelecido no art. 19, II, ambos da LGPD, serão contabilizados em dobro. Portanto, o prazo para atendimento do direito de acesso ou confirmação de tratamento no formato de declaração, deverá ser respondido pelo agente de pequeno porte controlador no prazo de 30 dias (o prazo para os demais agentes é de 15 dias).



RESUMO

ATENDIMENTO A DIREITOS DOS TITULARES

- O controlador será responsável por receber, analisar e responder solicitações referentes a direitos dos titulares, cabendo ao operador auxiliar quando solicitado e dentro dos limites de suas atribuições;
- O agente de tratamento de pequeno porte também deverá atender a requisições de titulares, lhe sendo concedido prazo em dobro nos termos do art. 14 da Resolução CD/ANPD nº 2/2022.

⁴⁴ BRASIL. Autoridade Nacional de Proteção de Dados. *Art. 8º da Resolução CD/ANPD n.º 2, de 27 de janeiro de 2022*. Disponível em <[link](#)>, acesso em 23 de jan. de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

3.4. COMUNICAÇÃO DE INCIDENTES

Mais uma obrigação importante e que merece destaque no presente Guia é a responsabilidade pela comunicação de incidentes de segurança da informação que envolvam dados pessoais. Antes de determinar a quem cabe a responsabilidade de comunicar, importante elucidar, de forma breve, o que é um incidente de segurança da informação e quando ele deve ser comunicado à ANPD.

Um incidente de segurança da informação, de forma simples, pode ser definido como um evento adverso que comprometa a (i) confidencialidade, (ii) integridade ou a (iii) disponibilidade⁴⁵ de determinadas informações/dados. É verificada violação à: (i) confidencialidade, quando a informação/dado é disponibilizada a quem não deveria ter acesso; (ii) integridade, quando a informação contida em determinado ambiente é corrompida, adulterada ou de qualquer forma afetada e não condiz mais com a informação anteriormente registrada; e (iii) disponibilidade, quando a informação/dado e/ou o sistema não estão mais disponíveis para o acesso das pessoas que necessitam o ter.

Dito isto, confirmada a ocorrência do incidente de segurança da informação, tem-se que somente deverá ser comunicado à ANPD e aos titulares se, concomitantemente, (a) envolver dados pessoais de titulares, e (b) acarretar risco ou dano relevante ao titular, conforme determina o art. 48 da LGPD e a Resolução CD/ANPD nº 15/2024, que trata do tema <link>.

Sobre o conceito de “dano ou risco relevante ao titular”, a referida Resolução estipula ao seu artigo 5º dois requisitos precisam ser preenchidos concomitantemente:

- (a) Possibilidade de que sejam afetados significativamente interesses e direitos fundamentais do titular, como as que o impeçam de exercer direitos garantidos por lei, utilizar serviços, ou que lhe causem danos patrimoniais ou extrapatrimoniais; e
- (b) Envolvam dados de uma entre as seis categorias a seguir – (i) dados pessoais sensíveis, (ii) dados de crianças, adolescentes ou idosos, (iii) dados financeiros, (iv) dados de autenticação em sistemas, (v) dados protegidos por sigilo legal, judicial ou profissional, ou (vi) dados em larga escala.

⁴⁵ BRASIL. Autoridade Nacional de Proteção de Dados. *Comunicação de incidente de segurança*. Disponível em <link>, acesso em 05 de maio de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Feita uma breve introdução ao tema de incidentes, retoma-se ao tema central desse Guia: qual agente de tratamento é responsável por comunicar a ANPD e aos titulares sobre a ocorrência de um incidente que envolve dados pessoais e pode acarretar risco/dano relevante?

A resposta para essa pergunta consta no art. 48 da LGPD e no artigo 4º da Resolução CD/ANPD nº 15/2024, qual seja o controlador. Portanto, verificada suspeita de incidente envolvendo dados pessoais, é responsabilidade do controlador avaliar a situação, a gravidade do caso e a necessidade de comunicar à ANPD e aos titulares envolvidos na operação. O prazo estabelecido pela ANPD para essa comunicação é de até 3 (três) dias úteis da ciência do evento e, ainda que o controlador não possua todas as informações sobre o fato, deverá observar o referido prazo procedendo com uma comunicação preliminar⁴⁶.

Ao operador caberá adotar as melhores práticas para prevenir incidentes e, verificada a ocorrência de um evento adverso que configure incidente, deverá comunicar o controlador o quanto antes, sem demoras injustificadas⁴⁷. A comunicação ao controlador deverá considerar o prazo estabelecido pela ANPD, supramencionado, bem como deverá conter todas as informações necessárias à comunicação do incidente à ANPD e aos titulares. Como já pontuado no parágrafo acima, ainda que não seja possível passar inicialmente todas as informações necessárias à comunicação à ANPD, sugere-se que o operador conceda o máximo de informações possíveis sobre o incidente, de modo que o controlador possa fazer uma comunicação preliminar à referida Autoridade dentro do prazo regulamentar.

Destaca-se, contudo, que a Resolução CD/ANPD nº 15/2024 apesar de determinar que seja o controlador a fazer a comunicação, não impede que este conceda poderes específicos para que o operador a faça. Deste modo, na eventualidade dos agentes acordarem entre si que a comunicação deverá ser feita pelo operador, recomenda-se ao controlador elaborar instrumento/documento concedendo poderes específicos para a realização da comunicação de incidente pelo operador à ANPD, bem como se sugere a ambos os agentes de tratamento, diante desta situação, que as comunicações feitas (preliminar e, eventualmente, complementar) sejam previamente aprovadas por aquele que figurar como controlador dos dados pessoais.

⁴⁶ BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD n.º 15, de 24 de abril de 2024*. Disponível em <[link](#)>, acesso em 03 de maio de 2024.

⁴⁷ BRASIL. Autoridade Nacional de Proteção de Dados, op. cit., nota 46.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

No que diz respeito aos agentes de pequeno porte controladores, caberá a comunicação do incidente dentro do prazo de 6 dias úteis, conforme orientado no art. 14, IV da Resolução CD/ANPD nº 2/2022, sendo essa, atualmente, a única flexibilização das normas de incidente aos agentes de pequeno porte. Todavia, conforme disposto no art. 10 da referida Resolução, a ANPD disporá de procedimentos simplificados ou flexibilizações sobre a comunicação de incidentes por esses agentes em regulamentação específica a esse tema.

Assim como mencionado no subcapítulo 3.1, o tema deste Guia é agente de tratamento, sendo que não serão abordadas aqui as obrigações e orientações detalhadas sobre incidente de segurança da informação, o qual poderá ser objeto de trabalhos futuros. Para mais detalhes sobre como comunicar e quais os requisitos mínimos à comunicação, sugere-se a leitura da página “Comunicação de incidentes de segurança” disponível no site oficial da ANPD no seguinte [link](#).



RESUMO COMUNICAÇÃO DE INCIDENTE

- A responsabilidade pela comunicação do incidente, via de regra, é do controlador. Na eventualidade das partes convencionarem que o operador deverá comunicar à ANPD, recomenda-se que o controlador elabore documento concedendo poderes específicos para o primeiro, bem como aprobe previamente o(s) documento(s) de comunicação a ANPD.

3.5. ELABORAÇÃO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

Passando-se ao próximo tópico, necessário trazer à baila a responsabilidade pela elaboração do Relatório de Impacto à Proteção de Dados (RIPD), definido no art. 5º, XVII como “**documentação do controlador** que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (grifos nossos)⁴⁸.

Conforme fica evidente já na própria definição de RIPD, a responsabilidade para elaboração deste documento é do agente de tratamento controlador, estando também previsto no art. 38 da LGPD. Assim, da leitura desses dispositivos, bem como das orientações sobre elaboração do RIPD

⁴⁸ BRASIL. Art. 5º, VII da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em <[link](#)>. Acesso em 15 de janeiro de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

emanadas da ANPD (disponível neste [link](#)), vê-se que o operador, via de regra, não tem a obrigação de elaborar esse documento.

Contudo, tanto o controlador quanto o operador deverão manter o registro das operações de tratamento que realizam⁴⁹, de forma que tais registros possam auxiliar, posteriormente e se necessário, na elaboração do RIPD, o qual poderá ser solicitado a qualquer momento pela ANPD⁵⁰.

Ante o exposto anteriormente, sugere-se que as instituições, dentro de suas atribuições e levando-se em consideração o seu papel de operador ou controlador nos cenários de tratamento de dados em que atuam, analisem a necessidade de elaboração do RIPD e, se preciso for, o façam de modo prévio – sem provação da ANPD – de modo que, caso solicitada, seja necessário somente alterar o relatório com as informações devidamente atualizadas.

No âmbito dos agentes de tratamento de pequeno porte, no art. 10 da Resolução mencionada no subcapítulo 2.2, tem-se a flexibilização do registro das atividades de tratamento de modo que seja feito no formato simplificado. Ou seja, ainda que os registros sejam obrigatórios, eles poderão ser de forma simplificada utilizando-se do modelo de registro disponibilizado pela ANPD neste [link](#).

Por fim, é importante salientar que a resolução não desobriga o agente de pequeno porte de elaborar e apresentar o RIPD caso solicitado pela ANPD nos termos do caput do art. 38 da LGPD, concedendo, apenas, o prazo em dobro, nos termos do art. 14, IV da referida Resolução aplicável.

DICA



RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

- Recomenda-se a leitura do guia específico elaborado pela FGV sobre o tema, disponível em sua página de [Proteção de Dados Pessoais](#), seção “Guia de Proteção de Dados Pessoais” – Relatório de Impacto à Proteção de Dados.

⁴⁹ BRASIL. Art. 37 da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em [link](#). Acesso em 15 de janeiro de 2024.

⁵⁰ BRASIL. Art. 38 da Lei 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais*. Brasília, DF: Diário Oficial da União, 2018. Disponível em [link](#). Acesso em 15 de janeiro de 2024.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

3.6. CONTRATOS E O PAPEL DO AGENTE DE TRATAMENTO

Para finalizar o presente capítulo, como visto anteriormente, a definição dos papéis de controlador/operador é muito importante para a atribuição das obrigações contidas nas legislações de proteção de dados pessoais. Dentro de uma relação entre instituições, principalmente quando há o tratamento de dados pessoais, é comum que exista um instrumento contratual visando regular as atividades que serão realizadas a partir daquele vínculo.

Dentro de uma relação contratual, em decorrência do seu objeto, é possível que as partes tenham diferentes obrigações, o que poderá impactar diretamente no papel de agente de tratamento que desempenharão. Há casos em que o escopo da própria contratação e o tipo de serviço prestado, por exemplo, fazem com que aquele contratante ou aquela contratada sempre figure como operador ou controlador.

Um exemplo em que, via de regra, as partes sempre atuarão no mesmo papel de controladora é o tratamento de dados pessoais de seus representantes e/ou funcionários. Nesta situação, em que há o tratamento de dados pessoais de pessoas naturais que possuam vínculo de representação e/ou empregatício/prestação de serviços, cada uma das instituições partes será a controladora dos dados pessoais daqueles que possuem relação direta com ela.

Contudo, a depender da situação concreta, poderá ocorrer que dentro de um mesmo contrato, as partes figurem em alguns momentos como operadora e em outros como controladora, ou até mesmo controladoras conjuntas ou suboperadoras, seja em razão do próprio objeto do contrato ou em razão da sua forma de execução, o que ensejará diferentes obrigações.

No mesmo sentido, adotando por premissa os contratos conexos e/ou coligados como instrumentos que regulamentam parcerias institucionais e doações de subsídios vinculados a outros arranjos jurídicos – uma vez que utilizados em decorrência de relação de dependência unilateral ou recíproca⁵¹ entre as partes – a definição do papel de agentes de tratamento não seguirá o padrão de controladora para a parte contratante e operador para a parte contratada, até porque a figura de contratante/contratado não será sequer aplicada nesse contexto.

⁵¹ MARINO, Francisco Paulo de Crescenzo, “*Contratos Coligados no Direito Brasileiro*”. São Paulo, 2009. “A coligação contratual traduz-se na existência de contratos que se encontram em uma relação de dependência unilateral ou recíproca, que pode ser decorrente de uma disposição legal, da natureza acessória de um dos contratos ou ainda do conteúdo contratual estabelecido pelas partes”.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

O que decerto definirá o papel das partes são justamente as atividades por elas realizadas que impliquem tratamento de dados pessoais, como por exemplo, o compartilhamento de uma base de dados entre as Instituições parceiras para análises/estudos (uma espécie de controladoria conjunta) ou a realização de coleta primária de dados pessoais por apenas uma Instituição (atuando como controlador singular), ou ainda, utilização de uma plataforma para aplicação de questionários no âmbito do acordo de parceria (um exemplo de operador), dentre outras situações.

Como pode ser observado, no contexto de contratos conexos e/ou coligados o papel dos agentes de tratamento poderá perpassar de forma harmônica entre controlador e operador, a depender das atividades de tratamento desenvolvidas individualmente, observadas as atribuições contratuais.

Portanto, estipular genericamente que a contratante é controladora e a contratada operadora, sem análise minuciosa das atividades que serão efetivamente realizadas individualmente pelas partes, das suas obrigações e da finalidade/objeto ao qual se destina, poderá ensejar na definição do papel de forma incorreta, atraindo para uma parte obrigações que não seriam, necessariamente, de sua responsabilidade. Além disso, vale ressaltar que a definição contratual não se sobrepõe ao papel concreto de tratamento de dados, embora seja sempre recomendada a correta disposição do papel das partes por escrito para que suas obrigações estejam estipuladas de forma clara.

À vista disso, dedicar uma subcláusula para a definição dos papéis de agentes de tratamento dentro das cláusulas gerais de proteção de dados pessoais no instrumento contratual, além de garantir adequação à LGPD, reverencia também os princípios da transparência, segurança e finalidade específica no tratamento dos dados pessoais para cada instituição envolvida e delimita as situações em que determinada parte poderá atuar como controladora ou operadora.

Em caso de dúvidas na definição dos papéis, sugere-se a utilização do *checklist* contido no [Apêndice Único](#) deste Guia para auxiliar.

Diante de todo o exposto durante o decorrer do capítulo 3, fica evidente a importância na definição dos papéis de agente de tratamento, tendo-se em vista as distribuições de competências e obrigações dispostas na LGPD. Fica claro, também, a necessidade de elaboração de instrumento contratual para definir de forma específica a relação, atribuições, obrigações e o papel de agente de tratamento.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	



DICA

- Recomenda-se que durante a interação entre 2 ou mais agentes de tratamento, seja elaborado **instrumento contratual** para definição das atribuições de cada uma das partes, com cláusula destinada especificamente ao tema de proteção de dados onde será definido o papel de agente de tratamento de cada, considerando-se as respectivas obrigações.

4. CONCLUSÃO

Este guia visou auxiliar na definição dos papéis dos agentes de tratamento e suas respectivas obrigações, considerando o cenário legal e regulatório atual do Brasil.

Para tanto, o primeiro capítulo visou contextualizar o presente Guia, acompanhado do segundo capítulo que introduziu o tema de agentes de tratamento, explicitando as definições de cada figura: controlador, operador, controladoria conjunta e suboperador. Ainda, este capítulo se dividiu em dois tópicos; o subitem 2.1 abordou a pessoa jurídica como agente de tratamento e o fato de caber a ela o papel de controladora ou operadora, sendo incorreta a indicação de seus funcionários, colaboradores, gerentes, diretores etc. como agente de tratamento. No segundo subitem, apresentou-se as nuances acerca dos agentes de tratamento de pequeno porte, conforme Resolução CD/ANPD nº 2/2022.

O terceiro capítulo aborda, de forma não exaustiva, a importância da definição do papel de controlador e operador, trazendo as principais diferenciações e obrigações de cada um dos papéis de agente. Ele foi dividido em tópicos e em sua introdução apontou-se que cabe ao controlador tomar as principais decisões, cabendo ao operador seguir as orientações do primeiro agente. Ainda, foi mencionada a eventual obrigatoriedade de indicação do encarregado pelo tratamento de dados.

O primeiro subcapítulo, 3.1, tratou de obrigações que se direcionam a ambos os agentes, apresentado a temática envolta das boas práticas e governança que as instituições e pessoas devem observar durante o tratamento de dados pessoais. Dando continuidade, o subcapítulo 3.2 trouxe a responsabilidade civil de cada um dos agentes, sendo que o controlador será responsável pelo tratamento, cabendo ao operador a responsabilidade solidária nos termos do art. 42, §1º da LGPD. O subcapítulo 3.3 apresentou a obrigação de atendimento de direitos dos titulares pelo controlador, cabendo ao operador auxiliá-lo quando necessário e na medida de suas atribuições.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

O subcapítulo 3.4 trouxe o tema de comunicação de incidentes e a responsabilidade do controlador em fazê-lo segundo as normas e regulamentos da ANPD, apresentando, ainda, as obrigações do operador em auxiliá-lo e comunicar ao agente controlador caso ocorra um incidente em relação a dados pessoais que estejam sob sua responsabilidade. O subcapítulo 3.5 apresentou a obrigação do controlador em elaborar o Relatório de Impacto à Proteção de Dados a depender da atividade de tratamento. O subcapítulo 3.6 abordou alguns os aspectos contratuais na definição dos agentes de tratamento e a importância de ter um instrumento que defina as obrigações e respectivos papéis decorrentes dela, apontando a possibilidade de em um mesmo contrato as partes figurarem por vezes como controladora e por outras como operadora.

Por fim, retoma-se que este Guia se destina a oferecer algumas diretrizes e boas práticas no tema de proteção de dados pessoais e a definição dos agentes de tratamento e está suscetível a constantes atualizações, incluindo aquelas decorrentes de futuros entendimentos consolidados e determinações de autoridades competentes, destinando-se a oferecer orientações, com base nas leis e regulamentos de proteção de dados aplicáveis.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

APÊNDICE ÚNICO

CHECKLIST PARA DEFINIR QUAL O PAPEL ENQUANTO AGENTE DE TRATAMENTO⁵²

SOU CONTROLADOR?	
1 <input type="checkbox"/>	Cabe a mim, ou à instituição de que faço parte, a decisão de tratar os dados pessoais.
2 <input type="checkbox"/>	Ainda que não tenha acesso direto aos dados pessoais, cabe a mim, ou à instituição de que faço parte, decidir tratar os dados pessoais, determinando/contratando um terceiro para tratar os dados em meu nome.
3 <input type="checkbox"/>	Cabe a mim, ou à instituição de que faço parte, determinar para quais finalidades o tratamento será realizado e os resultados decorrentes dele, bem como as bases legais que o amparem.
4 <input type="checkbox"/>	Cabe a mim, ou à instituição de que faço parte, a decisão de quais dados pessoais deverão ser tratados.
5 <input type="checkbox"/>	Cabe a mim, ou à instituição de que faço parte, a decisão de quais pessoas naturais terão seus dados pessoais tratados.
6 <input type="checkbox"/>	Eu, ou a instituição de que faço parte, tenho interesse e serei beneficiado, seja de forma comercial ou não, do resultado final daquele tratamento (salvo em casos em que houver a contratação de prestação de serviços para atuar em nome e conforme orientações de terceiro).
7 <input type="checkbox"/>	O tratamento dos dados pessoais decorre de uma relação contratual direta entre mim, ou a instituição da qual faço parte, e o titular ⁵³ de dados.
8 <input type="checkbox"/>	Os dados pessoais são de meus funcionários, colaboradores, estagiários, entre outras modalidades, ou da instituição de que faço parte.
9 <input type="checkbox"/>	Eu, ou a instituição de que faço parte, possuo autonomia (respeitadas as leis e regulamentos aplicáveis) no modo de tratamento dos dados pessoais.

ESTOU EM SITUAÇÃO DE CONTROLADORIA CONJUNTA?	
1 <input type="checkbox"/>	Eu, ou a instituição de que faço parte, tenho objetivos e interesses comuns com outra instituição/pessoa controladora no que diz respeito ao tratamento, como, por exemplo, a finalidade e o resultado.

⁵² Este *checklist* foi traduzido e adaptado a partir dos critérios e itens de autoria da *Information Commissioner's Office* – ICO, autoridade de proteção de dados pessoais britânica, disponível em “*A Guide to controllers and processors – Checklist*”, (tradução livre: Um Guia para controladores e operadores – Checklist), acessível clicando neste <[link](#)>. Nota, por se tratar de tradução e adaptação livre, alguns itens originais foram excluídos, editados ou embutidos em outros.

⁵³ Segundo a LGPD, o titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Vide art. 5º, V da LGPD.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

2 <input type="checkbox"/>	Eu, ou a instituição de que faço parte, trato a mesma base de dados que outro controlador para uma mesma finalidade determinada.
3 <input type="checkbox"/>	Eu, ou a instituição de que faço parte, desenvolvi o/as design/diretrizes do tratamento conjuntamente com outro controlador.
4 <input type="checkbox"/>	Eu, ou a instituição de que faço parte, tenho regras comuns de gerenciamento de informações com outro controlador.

SOU OPERADOR?

1 <input type="checkbox"/>	Cabe a mim, ou à instituição de que faço parte, seguir as instruções de um terceiro no âmbito do tratamento dos dados pessoais.
2 <input type="checkbox"/>	Os dados pessoais foram entregues a mim, ou à instituição que faço parte, por um cliente ou por terceiro, ou fui instruído sobre quais dados pessoais devem ser coletados/usados.
3 <input type="checkbox"/>	Não cabe a mim, ou à instituição de que faço parte, decidir por coletar e/ou tratar os dados pessoais de pessoas naturais por liberalidade própria.
4 <input type="checkbox"/>	Não cabe a mim, ou à instituição de que faço parte, decidir quais tipos de dados pessoais devem ser coletados e/ou tratados das pessoas naturais.
5 <input type="checkbox"/>	Não cabe a mim, ou à instituição de que faço parte, definir a base legal que amparará o tratamento.
6 <input type="checkbox"/>	Não cabe a mim, ou à instituição de que faço parte, definir para quais finalidades os dados pessoais serão utilizados.
7 <input type="checkbox"/>	Não cabe a mim, ou à instituição de que faço parte, decidir se ou dados pessoais poderão ou não ser divulgados e para quem.
8 <input type="checkbox"/>	Não é de meu interesse, ou da instituição da qual faço parte, o resultado final do tratamento dos dados pessoais.
9 <input type="checkbox"/>	Cabe a mim, ou à instituição de que faço parte, tomar apenas decisões pontuais e técnicas acerca do tratamento de dados pessoais, sendo que as principais decisões caberão exclusivamente a instituição terceira que me contratou/solicitou.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.001.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

