

Práticas de Compliance sob a Perspectiva de Privacidade e Proteção de Dados

Lefosse

Índice

1. **Introdução** ..... **pág. 4**

2. ***Background Check*** ..... **pág. 6**

No que consiste o *background check*? ..... **pág. 7**

Como o *background check* pode ser realizado? ..... **pág. 8**

A condução de *background check* é compatível com a LGPD? ..... **pág. 8**

Quais cuidados são recomendados na realização de *background check*? ..... **pág. 10**

Cuidados especiais em procedimentos *"Know Your Employee"* ..... **pág. 12**

Quais os principais cuidados que devem ser tomados na contratação de ferramentas automatizadas para rotinas de *background check*? ..... **pág. 14**

Quais os principais cuidados que devem ser tomados na condução de rotinas de *background check* diretamente por um colaborador ou departamento interno? ..... **pág. 14**

Com quem posso compartilhar as informações obtidas? ..... **pág. 14**

Por quanto tempo podem ser armazenados os resultados de pesquisas de *background check*? ..... **pág. 14**

3. **Canal de Denúncias** ..... **pág. 15**

O que é o canal de denúncias? ..... **pág. 16**

Quais cuidados devem ser tomados para mitigar riscos de proteção de dados? ..... **pág. 16**

Com quem posso compartilhar as informações obtidas? ..... **pág. 18**

Quais cuidados devo ter na contração de um canal de denúncias terceirizado? ..... **pág. 19**

Por quanto tempo podem ser armazenadas as informações obtidas? ..... **pág. 19**

4. Investigações Internas ..... pág. 20

O que é uma investigação interna? ..... **pág. 21**

O tratamento de dados pessoais em uma investigação interna pode ser amparado em qual(is) base(s) legal(is) previstas na LGPD? ..... **pág. 21**

Quais cuidados devem ser tomados para mitigar riscos de proteção de dados? . **pág. 22**

Posso acessar aparelhos pessoais de colaboradores e aplicativos de mensagens instantâneas? ..... **pág. 23**

Com quem posso compartilhar as informações obtidas? ..... **pág. 25**

Quais cuidados devo ter na contração de um canal de denúncias terceirizado? ..... **pág. 25**

Por quanto tempo podem ser armazenados dados de investigações internas? ..... **pág. 25**

5. Compartilhamento de dados pessoais ..... pág. 26

6. Contratação de fornecedores para execução e rotinas de Compliance ..... pág. 28

Quais cuidados devo ter na contratação de fornecedores? ..... **pág. 29**

7. Retenção e descarte de dados pessoais ..... pág. 31

8. Transferência internacional de dados pessoais ..... pág. 33

9. Governança Interna ..... pág. 35

Quais medidas são recomendáveis para a mitigação de riscos relacionados à cumulação de funções de DPO e CCO por um mesmo profissional? ..... **pág. 37**

10. Resumo das recomendações ..... pág. 38

11. Nosso time ..... pág. 41

Introdução

A Lei Geral de Proteção de Dados Pessoais (**LGPD**)[1], em vigor desde setembro de 2020, estabelece princípios, diretrizes e obrigações para o tratamento de dados pessoais,[2] tendo como objetivo a proteção dos direitos e liberdades dos indivíduos, como a privacidade e a autodeterminação informativa.

Na medida em que a privacidade e a proteção de dados pessoais são direitos fundamentais consagrados na Constituição Federal, e que LGPD é aplicável a toda e qualquer atividade de tratamento de dados pessoais,[3] é essencial que as práticas internas de uma empresa, incluindo as práticas de Compliance e Prevenção à Lavagem de Dinheiro ("**PLD**"), sejam revisitadas para identificação e correção de eventuais inconformidades com a LGPD.

Com o objetivo de orientar nossos clientes quanto às melhores práticas de **Compliance e Proteção de Dados Pessoais**, esta cartilha apresenta, de forma não exaustiva, conceitos importantes, pontos de atenção e recomendações práticas para a compatibilização das práticas mais comuns de Compliance às disposições da LGPD.

Para tanto, selecionamos temas corriqueiros que departamentos de Compliance normalmente enfrentam em suas rotinas, sob uma perspectiva de proteção de dados pessoais e privacidade, tais como a realização de *background check*, implementação de canal de denúncias, investigações internas, dentre outros.

1 Lei N. 13.709, de 14 de agosto de 2018. Esta lei é aplicável aos setores público e privado, independente do meio, país de localização dos dados ou da sede da organização, desde que a atividade (i) seja realizada no Brasil ou se destine a indivíduos localizados no Brasil, ou (ii) envolva dados coletados no Brasil.

2 Nos termos do artigo 5º, incisos I e X da LGPD, "dado pessoal" é "toda informação relacionada a uma pessoa natural identificada ou identificável", enquanto "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".

3 As exceções de aplicabilidade da LGPD estão previstas em seu artigo 4º: "Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. [...]".

Na medida em que essas atividades envolvem tratamento de dados pessoais, muitas vezes em volume considerável, é importante que os Departamentos de Compliance das empresas identifiquem os riscos pertinentes e adotem as cautelas necessárias para assegurar que tais atividades estejam em conformidade com a legislação de privacidade e proteção de dados, em especial a LGPD.



2. *Background Check*

No que consiste o *background check*?

É conhecido como *background check* o processo de pesquisas em bases de dados e mídias públicas para a obtenção de dados (pessoais ou não) que possam auxiliar organizações na **tomada de decisões informadas**, como a contratação de fornecedores e *onboarding* de clientes. Este processo costuma contemplar verificação de antecedentes, avaliação de conformidade com a legislação brasileira (especialmente a **Lei Anticorrupção**,[4] **Lei Antiterrorismo**[5] e a **Lei de Prevenção à Lavagem de Dinheiro**[6]), alinhamento com políticas internas e normas aplicáveis ao setor.

Trata-se de procedimento bastante comum na rotina de negócios, sendo uma etapa de diligência usualmente adotada para **avaliação de riscos e prevenção a fraudes** em situações diversas, como contratação e manutenção de relações contratuais com fornecedores, parceiros comerciais e clientes; realização de investimentos e operações societárias; contratação de colaboradores e condução de investigações internas, entre outros.

Nesse cenário, as principais rotinas de *background check* costumam ser divididas em processos:

"Know Your Customer"
("KYC" ou "Conheça seu Cliente"),

"Know your Supplier"
("KYS" ou "Conheça seu Fornecedor"),

"Know Your Partner"
("KYP" ou "Conheça seu Parceiro") e

"Know Your Employee"
("KYE" ou "Conheça Seu Colaborador"),
a depender do objeto e finalidade das pesquisas.

Vale lembrar que, mesmo quando o cliente, parceiro ou fornecedor objeto do *background check* for uma pessoa jurídica, a LGPD será aplicável sempre que houver acesso, coleta ou qualquer tipo de tratamento de dados pessoais de seus representantes legais, diretores e/ou colaboradores.

4 Lei N. 12.846, de 1º de agosto de 2013, bem como seu Decreto regulamentador, nº 11.129, de 11 de julho de 2022.
5 Lei N. 13.260, de 16 de março de 2016.
6 Lei N. 9.613, de 3 de março de 1998.

Como o *background check* pode ser realizado?

Existem várias ferramentas no mercado que viabilizam a condução de *background check* de forma automatizada, centralizando as buscas em um canal único. Estas ferramentas compilam dados de diversas fontes públicas, como bases de dados do Poder Judiciário, Ministério Público, entidades da administração pública, cartórios e listas administrativas de sanções. Ainda, podem compilar informações tornadas públicas pelo próprio titular em redes sociais e *websites* diversos.

Alternativamente, há organizações que optam por conduzir as pesquisas de *background check* manualmente, ou seja, consultando as mídias e bases de dados públicas diretamente, sem ferramentas intermediárias.

A condução de *background check* é compatível com a LGPD?

Em linhas gerais, para uma atividade envolvendo tratamento de dados pessoais ser considerada lícita nos termos da LGPD, esta deverá:

> ***(i)*** atender aos princípios da LGPD, com destaque ao princípio da finalidade, que pressupõe que a atividade de tratamento deve possuir uma **finalidade** legítima;
> ***(ii)*** ser amparada em alguma das hipóteses autorizativas previstas na lei, comumente referidas como **bases legais**.

Assim, no contexto dos processos de *background check*, primeiramente deve-se identificar a **finalidade** que se pretende alcançar, para então definir a **base legal**.

Em algumas situações, por exemplo, o *background check* será necessário para atender a uma obrigação legal, como os procedimentos de ***Know Your Customer*** por ***gatekeepers***[7], na medida em que a Lei de Lavagem de Dinheiro estabelece que estes devem:

> ***(i)*** implementar uma política de prevenção à lavagem de dinheiro e financiamento do terrorismo;
> ***(ii)*** identificar e manter cadastro atualizado de seus clientes, assim como de todos os intervenientes nas transações;
> ***(iii)*** registrar as transações;
> ***(iv)*** comunicar ao COAF as transações ou propostas de transações suspeitas;
> ***(v)*** comunicar ao órgão regulador a inocorrência de operações suspeitas.

7 São denominadas gatekeepers as pessoas jurídicas arroladas pela Lei de Lavagem de Dinheiro que, por desempenharem atividades sensíveis, estão sujeitas aos mecanismos de prevenção e comunicação de operações suspeitas, auxiliando o Poder Público na detecção de indícios de lavagem de dinheiro.

Nestes casos, a base legal será, justamente, o **cumprimento de obrigação legal ou regulatória pelo controlador**.[8]

Para outras modalidades de *background check*, contudo, a finalidade não será relacionada ao cumprimento de uma obrigação legal específica, e sim a interesses da organização ou empresa, como prevenção de fraudes. Nestes casos, a base legal mais adequada será o **legítimo interesse do controlador ou de terceiros**.[9]

Não obstante o possível enquadramento em bases legais previstas pela LGPD, o *background check* deve observar alguns cuidados para ser considerado compatível com referida lei, especialmente quanto à observação dos princípios de proteção de dados nela previstos, como o já mencionado princípio da finalidade e os princípios da **necessidade**[10], da **não discriminação**[11], da **qualidade dos dados**[12], da **transparência**[13], da **segurança**[14], e da **responsabilidade** e **prestação de contas**[15].

Além disso, nas hipóteses em que o *background check* for realizado com base no legítimo interesse, deve-se também considerar os requisitos previstos na LGPD para aplicação desta base legal, devendo estar alinhado, dentre outros fatores, às legítimas expectativas do titular de ter seus dados pessoais tratados para esta finalidade.

8 Art. 7º, II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

9 Art. 7º, IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

10 De acordo com o princípio da necessidade, o tratamento de dados pessoais devem ser limitado ao mínimo possível para atingir a sua finalidade.

11 Pelo princípio da não-discriminação, é vedado o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos.

12 Do princípio da qualidade decorre que o responsável pelo tratamento de dados deve garantir a exatidão, clareza, relevância e atualização dos dados tratados.

13 Pelo princípio da transparência, devem ser fornecidas informações claras, precisas e facilmente acessíveis aos titulares de dados pessoais sobre o tratamento de dados realizado.

14 De acordo com o princípio da segurança, devem ser adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

15 A prestação de contas corresponde à demonstração, pelo responsável pelo tratamento de dados, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Quais cuidados são recomendados na realização de *background check*?



Atentar-se aos dados pessoais sensíveis[16]

O legítimo interesse não pode ser utilizado como base legal de tratamento de dados pessoais sensíveis. Isto significa que os processos de verificação de antecedentes deverão ser estruturados de modo a sequer darem acesso a dados pessoais sensíveis, quando forem amparados no legítimo interesse.

Ademais, por conta da proteção especial conferida a estes dados pela LGPD, mesmo quando a base legal utilizada for o cumprimento de obrigação legal ou regulatória, o tratamento dos dados pessoais sensíveis deve ser evitado e reduzido ao mínimo necessário para atingir a finalidade do *background check*.



Tratar apenas os dados pessoais estritamente necessários para atingir a finalidade do *background check*

É importante que os responsáveis pela condução das pesquisas sejam devidamente orientados quanto à finalidade de cada *background check*, para que tenham clareza sobre os dados que têm a coleta justificável nos casos concretos. Ou seja, de acordo com o princípio da necessidade previsto pela LGPD, deve-se tratar apenas os dados pessoais estritamente necessários para atingir a finalidade do *background check*, sendo a coleta excessiva de dados uma violação às disposições da lei.



Ter em mente que dados de acesso público e dados tornados manifestamente públicos pelo titular também são sujeitos à LGPD

É comum o raciocínio de que dados pessoais de alguma forma disponíveis publicamente poderiam ser utilizados para quaisquer finalidades. Contudo, a LGPD também aborda essas situações, estabelecendo um regime específico para o tratamento de dados publicamente acessíveis e para os dados manifestamente tornados públicos pelo titular.[17] Desse modo, atividades de tra-

16 De acordo com o art. 5º, II, da LGPD, dado pessoal sensível corresponde ao 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.

17 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...]

tamento envolvendo esses dados não estão excluídas da aplicação geral dos princípios da LGPD e da necessidade e atribuição de uma base legal válida, conforme destacado abaixo:

> O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização;
>
> O tratamento dos dados pessoais tornados públicos pelo titular também deve assegurar os direitos e princípios previstos na LGPD, incluindo a necessidade de identificação de base legal aplicável ao tratamento destes dados.



Garantir transparência do tratamento dos dados pessoais

É direito dos titulares ter acesso a informações claras sobre como os seus dados pessoais são tratados. Para isso, é importante que as políticas de privacidade da organização – sejam as políticas internas, direcionadas aos colaboradores, sejam as políticas externas, direcionadas aos demais titulares com os quais a organização se relaciona – contemplem as rotinas de *background check* realizadas.

Especialmente quando justificado no legítimo interesse do controlador, o responsável pelas pesquisas deverá se certificar de que:

(i) A finalidade pretendida não infringe qualquer outra norma do ordenamento jurídico vigente. Para isso, recomenda-se que a área ou colaborador que pretende realizar o *background check* dentro da organização consulte o departamento jurídico interno ou escritório parceiro antes da implementação do processo, para garantir a sua compatibilidade com todas as leis vigentes aplicáveis à relação da organização com o titular;

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
[...]
§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

(ii) Há equilíbrio entre os interesses do controlador e dos indivíduos afetados pelo *background check*. Para isto, é recomendável, como boa prática,[18] a realização da Avaliação de Legítimo Interesse ("**LIA**", do inglês *Legitimate Interest Assessment)*, que tem como objetivo a ponderação entre os interesses legítimos pretendidos pelo controlador e os direitos e expectativas razoáveis dos titulares. Por meio do LIA, o controlador pode verificar a viabilidade do legítimo interesse como base legal do *background check*, com base nos requisitos previstos na lei para a aplicação desta base legal, além de documentar esta verificação, para fins de registros adequados e *accountability*.

Relatório de Impacto à Proteção de Dados Pessoais ("RIPD")[19]

Nas hipóteses de *background check* amparadas no legítimo interesse, também é recomendável a elaboração do RIPD, documento previsto na LGPD, de responsabilidade do controlador, destinado a atividades de tratamento de dados que possam resultar em riscos aos direitos fundamentais dos titulares. No RIPD, o controlador deverá descrever as etapas do *background check*, os riscos identificados e os mecanismos e salvaguardas visando à mitigação desses riscos. Vale destacar, ainda, que a ANPD poderá solicitar ao controlador o RIPD nestes casos.[20]

Cuidados especiais em procedimentos "*Know Your Employee*"

Os processos de "*Know Your Employee*" são mais restritos do que as outras modalidades de *background check*. A jurisprudência do Tribunal Superior do Trabalho ("**TST**") se baseia no entendimento de que a consulta ampla e irrestrita de antecedentes de colaboradores e candidatos em processos seletivos extrapola os limites do poder diretivo do empregador.

18 Embora o LIA não esteja expressamente previsto na LGPD e não tenha sido objeto de regulamentação ou guia orientativo por parte da ANPD até o momento, esta é uma boa prática embasada em orientações do General Data Protection Regulation ("GDPR"), que vem sendo difundida entre os agentes de tratamento de dados pessoais sujeitos à LGPD enquanto pendente, no ordenamento jurídico brasileiro, definições legais ou jurisprudenciais sobre como deve se dar a avaliação da aplicabilidade da base legal do legítimo interesse.

19 O relatório de impacto (ou *Data Protection Impact Assessmet* - DPIA) é um documento desenvolvido pelo controlador da atividade de tratamento de dados pessoais, que contém a descrição dos processos de tratamento de dados que podem gerar riscos às liberdades civis e aos direitos fundamentais do titular, descrevendo também medidas, salvaguardas e mecanismos de mitigação dos riscos identificados.

20 Nos termos do § 3º do artigo 10 da LGPD: A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Assim, sob a ótica trabalhista, a consulta de antecedentes ou exigência de apresentação de documentos poderá ser realizada apenas em situações amparadas em expressa previsão legal. Por exemplo: empresas que atuam em determinados setores possuem obrigações legais e regulatórias específicas quanto à prevenção à lavagem de dinheiro e ao financiamento do terrorismo, de modo que o KYE pode ser uma prática alinhada ao cumprimento destas obrigações.

Ainda, a jurisprudência trabalhista entende que práticas de KYE, como a consulta de antecedentes criminais, são aceitáveis quando justificadas pela natureza do ofício ou do grau especial de fidúcia exigido no cargo. No entanto, os tribunais restringem o tipo de informação que pode ser considerado para práticas desta natureza. Por exemplo, o TST proferiu decisão pela não utilização de dados de cadastros de crédito para a contratação de empregados, entendendo, dentre outros fundamentos, que esta atividade viola princípios da LGPD para o tratamento de dados pessoais.[21]

Portanto, é importante que o empregador analise, caso a caso, a real necessidade das pesquisas "*Know Your Employee",* bem como a pertinência dos dados tratados para esta finalidade, tendo em mente que o KYE injustificado poderá sujeitar o empregador a riscos de:

> ***(i)*** reclamações embasadas em exposição de dados, violação da intimidade, discriminação e danos morais; e
>
> ***(ii)*** aplicação de multas decorrentes de fiscalizações administrativas dos órgãos competentes, o que representa riscos para os indivíduos e empresas que adotam esta prática.

Por fim, a transparência exigida pela LGPD, neste caso, pode ser reforçada pela ampla divulgação interna das políticas e procedimentos de Compliance e PLD da organização em que estejam inseridas as rotinas "*Know Your Employee*", de modo a permitir que os colaboradores tenham pleno conhecimento das finalidades almejadas.

Quais os principais cuidados que devem ser tomados na contratação de ferramentas automatizadas para rotinas de *background check*?

Para recomendações sobre a contratação de fornecedores para execução de atividades decorrentes de *background check* e outras rotinas de Compliance, consulte a **seção 6** desta cartilha.

21 TST E-RR-933-49.2012.5.10.0001. Subseção I Especializada em Dissídios Individuais. Relatora Ministra Maria Helena Mallman. Julgado em 16.12.2021. Publicado em 25.02.2022.

Quais os principais cuidados que devem ser tomados na condução de rotinas de *background check* diretamente por um colaborador ou departamento interno?

Quando as pesquisas de verificação de antecedentes são realizadas diretamente por algum colaborador da organização, é recomendável:

Estruturar políticas e procedimentos internos que amparem a execução das pesquisas, documentando, por exemplo, as finalidades pretendidas, as bases de dados que podem ser consultadas, os cuidados que devem ser adotados no manuseio dos dados pessoais, a vedação ao tratamento de dados pessoais sensíveis quando a base legal da pesquisa for o legítimo interesse do controlador, os princípios de proteção de dados a serem observados, entre outros.

Restringir a atividade a um número limitado de colaboradores, que sejam treinados sobre as políticas e procedimentos estabelecidos pela organização.

Firmar acordo de confidencialidade com os colaboradores responsáveis pela realização das pesquisas, bem como por aqueles que necessitem acesso aos resultados das pesquisas para execução de suas atividades.

Com quem posso compartilhar as informações obtidas?

Para recomendações sobre o compartilhamento de informações decorrentes de *background check* e outras rotinas de Compliance, consulte a **seção 5** desta cartilha.

Por quanto tempo podem ser armazenados os resultados de pesquisas de *background check*?

Para recomendações sobre retenção e descarte de informações decorrentes de pesquisas de *background check* e outras rotinas de Compliance, consulte a **seção 7** desta cartilha.



3. Canal de Denúncias

O que é o canal de denúncias?

É um canal que permite, ao público interno e/ou externo, a comunicação de eventuais desvios de conduta e a elucidação de dúvidas acerca das regras internas da organização ou empresa. Um canal de denúncias eficaz deve estar alinhado a um sistema adequado de gestão e tratamento das comunicações recebidas e é um dos elementos fundamentais na construção e manutenção da integridade dentro das organizações.

A forma como o canal de denúncias será estruturado deve ser compatível com as características e os riscos de cada modelo de negócios. De modo geral, é recomendável que o canal de denúncias:

> ***(i)*** seja independente e imparcial, de modo que os responsáveis por receber e processar as denúncias não tenham conflitos de interesse com as questões analisadas;
>
> ***(ii)*** permita o registro de comunicações de maneira anônima**;**
>
> ***(iii)*** contemple procedimentos seguros nas fases de recepção e triagem das denúncias – que podem ser conduzidas por empresas terceirizadas.

Independentemente da estrutura, é natural que o processo envolva tratamento de dados pessoais. Com relação ao próprio denunciante, por vezes a coleta de seus dados somente ocorrerá quando este, de forma espontânea, decidir pela sua identificação. Porém, ainda que opte pelo anonimato, o teor da denúncia poderá conter dados pessoais e dados pessoais sensíveis de terceiros que o denunciante entenda necessários para a compreensão e apuração dos fatos alegados.

Por isso, é indispensável que a empresa adote medidas específicas para que o seu canal de denúncias esteja em conformidade com a LGPD, especialmente no que diz respeito ao tratamento dos dados recebidos por meio dele ou coletados em razão das investigações subsequentes.

Quais cuidados devem ser tomados para mitigar riscos de proteção de dados?

É importante que os princípios de proteção de dados sejam observados em todas as etapas de tratamento de dados pessoais por meio do canal de denúncias, ou seja, desde a **coleta**, **categorização**, **análise para definição de eventuais providências**, **processamento** e **armazenamento**. A seguir, apresentamos algumas medidas que podem ser adotadas como ponto de partida para a adequação do canal à LGPD:

Definição da base legal: na medida em que um canal de denúncias pode envolver temáticas diversas, é improvável que uma organização consiga prever, de forma exaustiva, todas as finalidades e todas as categorias de dados pessoais que podem ser recebidas por meio de um canal de denúncias. Em razão disso, tampouco é provável que a organização possa embasar todas as atividades de tratamento de dados pessoais decorrentes do canal de denúncias em uma única base legal prevista na LGPD. Assim, em cada caso, deve o controlador analisar qual a base legal mais adequada para o tratamento dos dados acessados para esta finalidade (por exemplo, o exercício regular de direitos, o cumprimento de obrigação legal ou regulatória e, até mesmo, o legítimo interesse do controlador ou de terceiros, a depender da natureza dos dados obtidos).

Segurança e confidencialidade: não é novidade que as informações recebidas por meio de um canal de denúncias devem ser processadas e armazenadas de modo a garantir a segurança e confidencialidade dos dados. Nesse sentido, é importante se certificar de que sejam implementadas medidas de segurança da informação compatíveis com a sensibilidade dos processos, tais como registros de *logs* de acesso, múltiplos fatores de autenticação, pseudonimização, criptografia, dentre outros.

Transparência: tanto do ponto de vista de Compliance como de Proteção de Dados, é importante que as pessoas que queiram utilizar o canal de denúncias tenham informações claras e de fácil acesso, dentre outras, quanto a ***(i)*** finalidades para as quais o canal pode ser utilizado; ***(ii)*** como os dados pessoais do denunciante e os dados revelados por meio da denúncia serão tratados; ***(iii)*** como se dará o processo de investigação pós denúncia; e ***(iv)*** com quais terceiros as informações podem ser compartilhadas. Para tanto, a organização deve garantir que as suas políticas de privacidade (destinadas a colaboradores e ao público externo) cubram as atividades de tratamento relacionadas ao canal de denúncias. É recomendável, ainda, a elaboração de uma política específica referente ao canal de denúncias.

Limitação de acesso: é fundamental se certificar de que as denúncias recebidas sejam acessadas apenas pelos colaboradores que realmente necessitam ter acesso àquelas informações por participarem do processamento da denúncia e apuração dos fatos. É importante que as informações do canal sejam armazenadas com controle de acesso das pessoas autorizadas, sendo registrados e armazenados dados sobre quem acessou determinada informação.

Capacitação: além de limitar o acesso às pessoas autorizadas, é essencial que essas pessoas sejam devidamente instruídas quanto à aplicação

da LGPD às suas atividades. Os colaboradores que atuem com o canal de denúncias devem, por exemplo, saber diferenciar dados pessoais de dados pessoais sensíveis, compreendendo as diferenças de tratamento entre eles. Ademais, devem ser treinados quanto aos princípios da necessidade, adequação e finalidade, de modo que sejam capazes de analisar, caso a caso, quais dados pessoais podem ser tratados em relação com a denúncia.

Revisão de processos: é recomendável revisitar os processos relacionados ao canal de denúncias periodicamente, para garantir que a proteção dos dados seja observada em todas as fases. Isso pode incluir:

Adequação do formulário utilizado para recebimento da denúncia, para que seja viabilizado o envio de denúncia anônima ou para redução da quantidade de informações solicitadas no momento do cadastro da denúncia ao mínimo necessário;

Adequação dos meios utilizados para apurar e investigar a denúncia, conforme será aprofundado na seção desta cartilha destinada à condução de investigações internas;

Revisão dos prazos de retenção dos dados recebidos pelo canal de denúncias, diferenciando os prazos das denúncias que resultam em investigações daquelas que são arquivadas por falta de provas;

Revisão do programa de integridade e do código de ética e conduta da organização, de modo que informem, de forma clara, quais condutas são consideradas irregulares pela organização e como funciona o canal de denúncias, alinhado às disposições da LGPD.

***Accountability*:** além das medidas indicadas acima, é recomendável elaborar um **RIPD** específico para o tratamento de dados em conexão com o canal de denúncias, para fins de documentar a análise de risco atrelada à atividade. Na mesma linha, nas situações em que a base legal utilizada seja o legítimo interesse do controlador ou de terceiros, é igualmente recomendável a elaboração do **LIA**, visando a ponderação dos interesses da organização e os direitos e liberdades fundamentais dos titulares de dados.

Com quem posso compartilhar as informações obtidas?

Para recomendações sobre o compartilhamento de informações decorrentes de canais de denúncias e outras rotinas de Compliance, consulte a **seção 5** desta cartilha.

Quais cuidados devo ter na contração de um canal de denúncias terceirizado?

Para recomendações sobre a contratação de fornecedores para execução de canais de denúncias e outras rotinas de Compliance, consulte a **seção 6** desta cartilha.

Por quanto tempo podem ser armazenadas as informações obtidas?

Para recomendações sobre retenção e descarte de informações decorrentes de canais de denúncias e outras rotinas de Compliance, consulte a **seção 7** desta cartilha.



4. Investigações Internas

O que é uma investigação interna?

A investigação interna também é atrelada ao programa de integridade da organização e consiste na apuração de eventuais suspeitas de condutas irregulares ou ilícitas praticadas ou relacionadas a colaboradores, em qualquer nível hierárquico.

Uma investigação pode ser iniciada por conta de alguma denúncia recebida pelo canal de denúncias, para apurar suspeitas identificadas por outras rotinas de Compliance ou de outras áreas da organização, como Recursos Humanos e Segurança da Informação. É possível, também, que uma investigação interna seja iniciada a partir de fatores externos, como resultados de auditorias, processos administrativos ou judiciais, ou notícias veiculadas na mídia envolvendo a organização, seus administradores ou colaboradores.

De modo geral, a apuração envolverá a coleta e análise de dados (podendo incluir, dentre outros, conteúdos de e-mails corporativos e outros meios corporativos de comunicação), a condução de *backgrounds check*, a condução de entrevistas exploratórias e/ou confirmatórias e, ao final, a elaboração de um relatório.

Além da interrupção da conduta irregular e da aplicação das sanções cabíveis, as investigações internas são importantes para a adoção de medidas de remediação e prevenção de condutas similares no futuro.

Em alguns casos, o resultado da investigação poderá ser compartilhado com autoridades investigativas ou regulatórias e poderá, ainda, ser utilizado como prova para a tutela dos direitos e interesses da organização em processos judiciais, administrativos ou arbitrais.

O tratamento de dados pessoais em uma investigação interna pode ser amparado em qual(is) base(s) legal(is) previstas na LGPD?

As principais bases legais que podem amparar um processo interno de investigação, a depender do caso concreto, são:

O cumprimento de obrigação legal ou regulatória pelo controlador, por exemplo, se a investigação tiver como objeto a apuração de irregularidade que a organização tenha obrigação legal de reportar a autoridades. Esta base legal é aplicável ao tratamento de dados pessoais e de dados pessoais sensíveis.

O exercício regular de direitos em processo judicial, administrativo e arbitral, quando a investigação tiver como finalidade formar conjunto probatório e fundamentar processo contra os investigados ou organizações por eles representadas. Esta base legal também é aplicável ao tratamento de dados pessoais e de dados pessoais sensíveis.

O legítimo interesse do controlador ou de terceiros, na medida em que as in-

vestigações internas também podem ter como objeto a prevenção a fraudes, verificação do cumprimento das normas internas, código de conduta e ética da organização, entre outras situações. Esta base legal, contudo, é aplicável apenas ao tratamento de dados pessoais não sensíveis.

Quais cuidados devem ser tomados para mitigar riscos de proteção de dados?

A investigação interna por vezes engloba o monitoramento de atividades realizadas pelos colaboradores no âmbito corporativo, o que pode incluir o uso de ferramentas que fiscalizam a utilização da infraestrutura tecnológica da organização, como o controle de acesso a aplicações ou de arquivos enviados pelos colaboradores. Além disso, pode incluir o acesso a conteúdo de e-mails e comunicações trocadas via ferramentas corporativas.

Nesse sentido, vale lembrar que, para que uma atividade de tratamento de dados pessoais possa estar em conformidade com a LGPD, é um pressuposto que essa atividade não viole outras normas do ordenamento jurídico, na medida em que tal violação já corresponde ao descumprimento do princípio da finalidade da LGPD, que prevê que o tratamento de dados deve visar propósitos legítimos.

Assim, especialmente nos casos de investigações internas e monitoramento que tenham como alvo colaboradores da organização ou empresa, é importante esclarecer que o monitoramento é, entre outros argumentos, legitimado no poder diretivo do empregador previsto na Consolidação das Leis do Trabalho (CLT), bem como na propriedade do empregador sobre as ferramentas corporativas disponibilizadas para o exercício das atividades laborais. De todo modo, para que o monitoramento seja lícito, é necessário que:

O colaborador seja previamente informado acerca do possível monitoramento, de modo a relativizar sua expectativa de privacidade no ambiente profissional. Ou seja, políticas internas, como a política de privacidade destinada aos colaboradores, a política de segurança da informação e normas internas de Compliance devem assegurar transparência quanto à possibilidade de monitoramento das ferramentas corporativas.

O monitoramento não seja excessivo a ponto de violar a privacidade e intimidade dos indivíduos, tampouco tenha caráter vexatório.[22]

22 A título de exemplo, colaciona-se decisão do TST que reconheceu que o "exercício do poder fiscalizatório, realizado de modo impessoal, geral, sem contato físico ou exposição da intimidade, não submete o trabalhador a situação vexatória nem caracteriza humilhação, vez que decorre do poder diretivo do empregador, revelando-se lícita a prática desse ato" (TST-RR-169000-71.2009.5.02.0011, 5ª Turma. Relator Ministro Caputo Barros. Julgado em 04.05.2016).

O monitoramento seja restrito ao uso de dispositivos corporativos, como *notebooks*, celulares e tablets disponibilizados pela organização aos colaboradores. Nos casos de organizações que adotem a política de "*Bring Your Own Device*" (BYOD), a coleta de informações somente será possível se o empregador puder garantir a segregação entre as ferramentas corporativas e as ferramentas de uso pessoal do colaborador, de modo que o monitoramento e investigação não poderão ultrapassar os limites dos aplicativos e/ou softwares relacionados ao trabalho.

Ademais, todos os cuidados de segurança e confidencialidade das informações, limitação de acesso, capacitação dos responsáveis, revisão de processos e *accountability*, detalhadas na **seção 3.2 (canal de denúncias)**, também são aplicáveis à condução de investigações internas, inclusive quando a investigação envolver dados pessoais de titulares que não sejam colaboradores da organização ou empresa.

Posso acessar aparelhos pessoais de colaboradores e aplicativos de mensagens instantâneas?

Uma das principais discussões no contexto das investigações internas está relacionada à possibilidade de acessar mensagens trocadas entre os colaboradores em aplicativos de mensagens instantâneas, especialmente se não foram utilizados aparelhos corporativos, mas sim aparelhos pessoais desses colaboradores.[23] De um lado, há a preocupação das autoridades de que as organizações tenham políticas e procedimentos claros de retenção de documentos, a fim de viabilizar o acesso a evidências necessárias no contexto de uma investigação; de outro, os limites para que o acesso a essas informações não violem a privacidade desses colaboradores.

A dificuldade na retenção e acesso a esses dados apresenta-se ainda mais desafiadora diante dos aplicativos de mensagens instantâneas que, por sua natureza, são configurados para autodeleção, além de plataformas criptografadas disponíveis em nuvem cuja preservação e coleta torna-se, muitas vezes, inviável. Ainda, a adoção de algumas políticas de ***"Bring Your Own Device"*** pelas organizações pode significar dificuldades adicionais na preservação das informações.

Nesse sentido, **nos Estados Unidos**, o Departamento de Justiça Americano[24] emitiu, recentemente, orientações para que as políticas corporativas de retenção de documen-

23 Vide, nesse sentido, o memorando do U.S. Department of Justice, "Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group", disponível em https://www.justice.gov/opa/speech/file/1535301/download. Nos termos deste documento, o DoJ espera que "all corporations with robust compliance programs [to] have effective policies governing the use of personal devices and third-party messaging platforms for corporate communications, (...) provide clear training to employees about such policies, and (...) enforce such policies when violations are identified".

24 Cf. nota acima.

tos contenham, no mínimo, ***(i)*** clara definição sobre qual seria o escopo das comunicações relacionadas aos negócios; ***(ii)*** descrição de quais aplicativos e dispositivos seriam permitidos e ou proibidos, fornecendo, ainda, orientações sobre seu uso apropriado; ***(iii)*** previsão sobre o direito da organização de acessar dados e mensagens nos dispositivos pessoais nas situações de investigação interna ou litígio; e, ainda, ***(iv)*** fornecer treinamentos periódicos a todos os colaboradores, incluindo diretoria e alta administração, acerca do uso desses dispositivos; e ***(v)*** estabelecer mecanismos de monitoramento, incluindo eventuais medidas disciplinares em caso de violação da política.

Na mesma esteira, a *U.S. Securities Exchange Commission* – SEC tem questionado as empresas sobre como elas monitoram, reveem e retêm essas informações, sobretudo em canais externos às corporações – e sancionado aquelas que não tiveram êxito nessa retenção.[25]

No Brasil, a discussão sobre o tema é pautada, essencialmente, pelo direito constitucional à privacidade e proteção de dados, pela legislação trabalhista, além das restrições trazidas pela LGPD ao tratamento de dados pessoais. Muito embora a jurisprudência trabalhista reconheça que o direito à privacidade no ambiente de trabalho é mitigado, não é possível afirmar que esta interpretação se aplica também a equipamentos de propriedade do próprio colaborador.

Ou seja, embora seja pacífica a possibilidade de acesso a informações armazenadas em dispositivos disponibilizados pelo empregador, desde que o empregado tenha prévia ciência de que este acesso é possível, o acesso a equipamentos pessoais do colaborador tem alto potencial de violar seu direito à privacidade, de modo que frequentemente só é aceito quando são adotadas ferramentas técnicas que separam os ambientes pessoais e profissionais em referidos equipamentos, sendo autorizado o acesso restrito ao ambiente profissional, como anteriormente mencionado.

Considerando as limitações e incertezas relacionadas ao tema, **é recomendável que empresas e organizações orientem seus colaboradores a concentrar as comunicações profissionais em equipamentos eletrônicos e softwares corporativos, disponibilizados pelo empregador, e que as políticas internas prevejam o uso de tais equipamentos para fins estritamente profissionais**, de modo a mitigar questionamentos relacionados à violação de privacidade de empregados.

Importante destacar, por fim, que o direito à privacidade do colaborador pode ser afastado por meio de ordem judicial que determine a apresentação de informações e documentos constantes de equipamentos pessoais utilizados para fins profissionais, para fins de produção de provas.

25 Para mais informações, veja-se https://corpgov.law.harvard.edu/2022/06/15/the-sec-and-messaging-apps/. Acesso em 30.05.2023.

Com quem posso compartilhar as informações obtidas?

Para recomendações sobre o compartilhamento de informações decorrentes de investigações internas e outras rotinas de Compliance, consulte a **seção 5** desta cartilha.

Quais cuidados devo ter na contração de um canal de denúncias terceirizado?

Para recomendações sobre a contratação de fornecedores para execução de investigações internas e outras rotinas de Compliance, consulte a **seção 6** desta cartilha.

Por quanto tempo podem ser armazenados dados de investigações internas?

Para recomendações sobre retenção e descarte de informações decorrentes de investigações internas e outras rotinas de Compliance, consulte a **seção 7** desta cartilha.



5. Compartilhamento de dados pessoais

Compartilhamento de dados pessoais

Naturalmente, as atividades descritas nesta cartilha poderão envolver o compartilhamento de dados pessoais com terceiros.

Os *gatekeepers*, por exemplo, ao tomarem conhecimento de transações suspeitas em suas rotinas de *"Know Your Costumer"*, precisam comunicar tais transações ao COAF, o que envolverá o compartilhamento de dados pessoais do cliente. O compartilhamento de dados também pode vir a ser necessário entre empresas de um mesmo grupo econômico, para fins de cumprimento das rotinas de Compliance, ou até mesmo a transferência internacional de dados, conforme descrita na **seção 8** desta cartilha.

Do ponto de vista de proteção de dados, a LGPD não veda o compartilhamento de dados pessoais, mas é necessário que o compartilhamento – assim como qualquer atividade de tratamento de dados pessoais – tenha uma finalidade legítima e seja adequado aos demais princípios da lei, bem como pautado em uma das bases legais previstas na LGPD. Desse modo, **é necessário analisar caso a caso a necessidade do compartilhamento e o fundamento legal que autoriza sua realização.**

Nesse ponto, destacamos que é um direito do titular ter informações acerca das entidades públicas e privadas com as quais o controlador compartilhe os seus dados. Portanto, para que este direito possa ser exercido, recomenda-se:



Revisitar procedimentos internos e mapear todos os terceiros com os quais são compartilhados dados, bem como as categorias de dados que são objeto de compartilhamento;



Incluir, em políticas de privacidade, informações claras sobre as hipóteses de compartilhamento e sobre o canal para o exercício de direitos previstos na LGPD por parte do titular de dados pessoais;



Revisar, conforme aplicável, os contratos que envolvam uso compartilhado de dados pessoais, prevendo mecanismos para atendimento a eventuais solicitações de exercício de direitos pelos titulares, além das recomendações apresentadas a seguir na **seção 6.1** desta cartilha.



6. Contratação de fornecedores para execução de rotinas de Compliance

Contratação de fornecedores para execução de rotinas de Compliance

As rotinas de *background check*, gerenciamento de canal de denúncias e condução de investigações internas podem ser terceirizadas pela empresa ou organização, especialmente quando o volume de pesquisas, denúncias e investigações for elevado.

Na medida em que estas contratações necessariamente envolvem o compartilhamento e tratamento de dados pessoais, destacamos a seguir algumas recomendações para mitigação dos riscos relacionados a proteção de dados neste contexto.

Quais cuidados devo ter na contratação de fornecedores?



Certificar-se de que os contratos com os fornecedores contenham, no mínimo:

Cláusulas de proteção de dados robustas, com alocação de responsabilidades e obrigações adequada à classificação das partes como agentes de tratamento de dados pessoais, bem como adequadas ao grau de segurança e confidencialidade que é esperado em rotinas de Compliance; e

Garantias quanto ao cumprimento da LGPD, boas práticas de Compliance e outras normas aplicáveis, acopladas a penalidades em caso de descumprimento;



Verificação dos mecanismos de segurança aplicados na condução das atividades, solicitando, sempre que possível, evidências destes mecanismos;



No caso de ferramentas terceirizadas, observar as políticas de privacidade e termos de uso das ferramentas antes da contratação, de modo a verificar se estas cumprem com a LGPD e com princípios de proteção de dados;



Especialmente no caso de ferramentas de background check, obter garantias, pelo fornecedor da ferramenta de pesquisa, de que sua base de dados é constituída de forma lícita. Inclusive, é recomendável obter do fornecedor, sempre que possível, garantia de que as bases públicas de dados utilizadas nas consultas (sites de órgãos públicos, portais de tribunais, entre outros), não possuem restrição à utilização de ferramentas de pesquisa utilizadas por tais fornecedores.[26]

26 Sobre esta temática, vale citar que, em outubro de 2021, o Serpro, empresa de tecnologia do Governo

6 *Contratação de fornecedores para execução de rotinas de Compliance*

É recomendável, por fim, o estabelecimento de um procedimento interno estruturado de auditoria/análise de fornecedores, com o intuito de apurar o atendimento do fornecedor às regras estabelecidas pela LGPD, bem como registrar internamente que essa análise foi realizada, para fins de *accountability*.

Federal (https://www.serpro.gov.br/) finalizou a contratação de solução de verificação de humanidade para todas as plataformas por ele gerenciadas (solução hCaptcha Enterprise), removendo o reCaptcha v2 e v3, com o objetivo de reforçar a privacidade e segurança de dados processados por órgãos do governo federal. Também relacionado ao tema, destacamos o Agravo em Recurso Extraordinário N. 1.307.386/RS, em trâmite no Supremo Tribunal Federal, no qual se discute a conformidade com a LGPD de portais que compilam dados de tribunais e disponibilizam, de forma irrestrita, informações relacionadas a processos criminais e trabalhistas. Para saber mais: https://www.mpf.mp.br/pgr/noticias-pgr/ferramentas-de-busca-que-permitem-acesso-a-acoes-criminais-e-trabalhistas-pela-consulta-de-dados-pessoais-fere-a-lgpd. Acesso em 18.04.2023.



7. Retenção e descarte de dados pessoais

Retenção e descarte de dados pessoais

A LGPD não determina um período específico pelo qual os dados pessoais devem ser guardados ou quando devem ser excluídos. Assim, cabe à organização verificar a finalidade e a necessidade do armazenamento para definir o prazo de retenção de dados adequado a cada atividade.

No caso das rotinas de Compliance abordadas nesta cartilha, o prazo de retenção poderá variar em função dos resultados que forem obtidos em cada processo e dos procedimentos que forem adotados em função desses resultados.

Por exemplo: em um *background check* prévio à contratação de um colaborador para um cargo cujo grau de fidúcia justifique a verificação de antecedentes, se as pesquisas não indicarem riscos e a contratação for efetivada, não há, em regra, necessidade e finalidade que justifiquem a manutenção destes dados pela organização ou empresa, sendo recomendável a exclusão após o encerramento do processo seletivo.

Por outro lado, dados resultantes dessas rotinas que possam ser necessários para formação de conjunto probatório em eventuais ações judiciais, administrativas ou arbitrais terão seu prazo de retenção atrelado aos prazos prescricionais aplicáveis.

Por fim, há situações em que o prazo de retenção será diretamente atrelado a alguma obrigação legal, como o prazo mínimo de 5 anos estabelecido pela Lei de Lavagem de Dinheiro, pelo qual os *gatekeepers* devem guardar os cadastros de seus clientes e o registro das transações.



8. Transferência internacional de dados pessoais

Transferência internacional de dados pessoais

No contexto de organizações e empresas multinacionais, assim como na apuração de prática de atos contra a administração pública nacional ou estrangeira (Lei Anticorrupção), poderá ser necessária a transferência de dados pessoais coletados no Brasil para país estrangeiro ou organismo internacional do qual o país seja membro.

Do ponto de vista de proteção de dados, a LGPD estabelece que a transferência internacional de dados pessoais somente é permitida mediante cumprimento de alguma das hipóteses autorizativas previstas nos artigos 33 e seguintes da lei.[27]

As hipóteses autorizativas da LGPD para a transferência internacional de dados incluem, dentre outras, o reconhecimento, pela ANPD, de que o país de destino dos dados proporciona grau de proteção a dados pessoais equivalente ao garantido pela LGPD. Na ausência de posicionamento deste sentido, outra opção é a adoção de salvaguardas que visem respaldar esta transferência, como, por exemplo, a adoção de cláusulas padrão contratuais, a serem sugeridas pela própria autoridade e implementadas pelas partes em contratos que envolvam a transferência de dados para outras jurisdições. Uma alternativa, também, é a adoção de normas corporativas globais, que estabelecem regras e padrões para o tratamento de dados pessoais dentro de um mesmo grupo econômico multinacional.

Contudo, até a data em que esta cartilha foi elaborada, a ANPD não regulamentou estas hipóteses, de modo que as regras previstas pela LGPD para transferência internacional de dados ainda não possuem eficácia. Para mitigar os riscos associados a este tema durante a pendência da regulamentação, **as empresas e organizações podem buscar garantias contratuais em contratos que envolvam a transferência internacional de dados pessoais, de modo a obter garantias de que o tratamento de dados realizado no exterior respeitará os termos estabelecidos pela LGPD.** Importante destacar que as situações envolvendo transferência internacional de dados costumam levar à aplicação de leis de jurisdições diversas, considerando as regras de extraterritorialidade de aplicação da LGPD.[28] Assim, é recomendável a **análise casuística das leis aplicáveis em todas as jurisdições envolvidas**, de modo a evitar riscos decorrentes de conflitos de legislação.

27 As hipóteses autorizativas podem ser resumidas da seguinte forma: (i) proferimento de decisão pela ANPD atestando a adequação do país ou organismo internacional destinatário dos dados às condições estabelecidas pela LGPD para tratamento de dados pessoais; (ii) adoção, pelas partes envolvidas na transferência, de mecanismos de salvaguarda previstos na LGPD, que permitirão a transferência internacional de dados para países não reconhecidos como adequados pela ANPD, como as cláusulas-padrão contratuais e as normas corporativas globais, dentre outros; (iii) outras situações específicas previstas na LGPD, como consentimento específico do titular, execução de contrato, execução de políticas públicas e cooperação jurídica internacional.

28 De acordo com o seu artigo 3º, a LGPD é aplicável em qualquer operação de tratamento realizada no Brasil ou cujos dados tratados tenham sido coletados no Brasil, ou que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil. Deste modo, mesmo que o tratamento de dados seja realizado em outra jurisdição, em ocorrendo uma destas hipóteses, será aplicável a lei brasileira.



9. Governança Interna

Governança Interna - Cumulação de Funções DPO e CCO

Desde a entrada em vigor da LGPD, tem sido comum que as empresas indiquem, como encarregado por proteção de dados – ou ***Data Protection Officer*** (DPO) –, profissional que já exercia a função de ***Chief Compliance Officer*** (CCO) da empresa – seguindo uma tendência que já se observava na Europa, desde a vigência do GDPR.

A cumulação de funções de **DPO** e **CCO** por um mesmo profissional, a princípio, não é vedada pela LGPD, tampouco pelo GDPR. Contudo, existem discussões sobre a possibilidade e limites de cumulação de tais funções, considerando o **risco de conflitos de interesses**.

Este, inclusive, foi o entendimento de uma decisão proferida em 2020 pela Autoridade de Proteção de Dados da Bélgica,[29] que multou uma empresa por entender que tal cumulação de funções criava conflito de interesses e, assim, violava o GDPR.

Mais recentemente, a *Court of Justice of the European Union* (CJEU) analisou caso de cumulação de função de DPO que também ocupava o cargo de presidente do conselho de trabalhadores da empresa, apontando, em sua decisão, que o DPO não pode ser incumbindo de realizar tarefas ou obrigações que possam prejudicar a execução de funções desempenhadas em razão de sua atuação como DPO, de modo a preservar sua **independência funcional**. Disso decorre, de acordo com a decisão, que o DPO não poderia ser incumbido de tarefas ou obrigações que resultem na determinação de objetivos e métodos para o tratamento de dados pessoais.[30]

Tais decisões demonstram a importância de serem observados alguns cuidados pelas empresas que optam pela cumulação de funções de DPO e CCO.

Enquanto o GDPR prevê expressamente que o DPO pode realizar outras tarefas dentro da organização, desde que não haja conflito de interesses com as atividades relacionadas à proteção de dados, a LGPD é silente neste aspecto. Contudo, vale lembrar que a ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado,[31] que podem adotar critérios semelhantes aos do GDPR.

29 A Autoridade de Proteção de Dados da Bélgica multou uma empresa por entender que a cumulação de funções de *Data Protection Officer* e *Chief Compliance Officer* criava conflito de interesses e, assim, violava o GDPR. Disponível, em holandês, em https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/05/Beslissing_GK_18-2020_NL_-1.pdf. Acesso em 31.05.2023.

30 Decisão disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=270323&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=36320. Acesso em 18.04.2023.

31 LGPD, Art. 43, § 3º. A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Quais medidas são recomendáveis para a mitigação de riscos relacionados à cumulação de funções de DPO e CCO por um mesmo profissional?

Idealmente, o profissional que assume a posição de DPO em uma organização não deve ser responsável por determinar finalidades de atividades de tratamento de dados pessoais realizadas por outras áreas/departamentos da empresa. Por exemplo: as funções do DPO não devem ser exercidas pela mesma pessoa que estrutura processos de *background check* dentro da organização, pois haverá alto risco de conflito de interesses das áreas neste caso, impedindo que as funções do DPO sejam exercidas de forma independente.

A organização pode implementar uma política interna de prevenção de conflitos de interesses, estabelecendo procedimentos a serem observados casuisticamente pelo DPO e áreas relacionadas.

Criação de um comitê ou estrutura equivalente, envolvendo representantes de áreas diversas da organização, com o objetivo de apoiar o DPO na tomada de decisões.

Portanto, ainda que inexista lei no Brasil que impeça a cumulação de funções de DPO com funções de CCO – ou qualquer outro cargo executivo –, é necessário que as empresas adotem mecanismos internos eficientes para mitigação de conflitos de interesses e garantia da autonomia e liberdade decisória intrínsecas aos cargos de DPO e CCO.



10. Resumo das recomendações

Resumo das recomendações

Para garantir que uma prática de Compliance esteja de acordo com a LGPD, é necessário, em síntese, analisar se:



Esta atividade atende aos princípios estabelecidos pela LGPD para o tratamento de dados pessoais? Dentre outros, importante considerar:

Se a **finalidade** do tratamento de dados (ou seja, o objetivo que se pretende alcançar com o tratamento) é **lícita e legítima**, de acordo com o ordenamento jurídico brasileiro;

Se não são tratados dados excessivos, mas sim apenas os **necessários** para atingir a finalidade proposta;

Se há **transparência** ao titular de dados acerca da atividade (por exemplo, por meio de sua previsão em políticas da empresa);

Se são adotadas medidas de **segurança** compatíveis com o tratamento de dados realizado, incluindo restrição de acesso a tais dados apenas a quem de fato precise acessá-los.



Há base legal prevista na LGPD que ampare a realização da atividade pretendida? Dentre outras possibilidades, necessário considerar:

Se a atividade decorre de uma **obrigação legal ou regulatória** da empresa ou organização;

Se a atividade é necessária para o **exercício regular de direitos** da empresa ou organização, em possíveis processos judiciais, administrativos ou arbitrais;

Se a atividade atende aos **interesses legítimos** da empresa ou organização, considerando as limitações previstas na lei para o uso desta base legal.



Em caso de contratação de fornecedores para a execução da atividade, tais fornecedores são capazes de cumprir com as obrigações estabelecidas pela LGPD? Para tanto, é recomendável:

Analisar a **capacidade do fornecedor de atender às disposições estabelecidas pela LGPD** para o tratamento de dados pessoais, preferencialmente por meio de procedimento interno estruturado, registrando a conclusão desta análise;

Obter **garantias contratuais** do fornecedor acerca do seu cumprimento das disposições legais.



Os dados pessoais tratados em decorrência da atividade são armazenados por período adequado? Para tanto, importante considerar:

A existência de **finalidade** e **base legal** prevista na LGPD para continuidade do armazenamento dos dados;

A **necessidade** do armazenamento de dados, considerando, dentre outros aspectos, a obrigação de manutenção.

Importante: As medidas aqui descritas não são exaustivas, mas visam fornecer uma visão geral de critérios a serem considerados para apuração da adequação de práticas de Compliance ao quanto estabelecido pela LGPD.

Em caso de dúvidas, entre em contato como o nosso time:



Paulo Lilla
Sócio da prática de Tecnologia, Proteção de Dados e Propriedade Intelectual
paulo.lilla@lefosse.com



Juliana Daniel
Sócia da prática de Compliance, Investigações e Penal Empresarial
juliana.daniel@lefosse.com



Carla Segala
Advogada sênior de Tecnologia, Proteção de Dados e Propriedade Intelectual
carla.segala@lefosse.com



Ane Carvalho
Advogada de Compliance, Investigações e Penal Empresarial
ane.carvalho@lefosse.com



Blanca Albuquerque
Advogada de Tecnologia, Proteção de Dados e Propriedade Intelectual
blanca.albuquerque@lefosse.com



Mariana Sangoi
Advogada de Tecnologia, Proteção de Dados e Propriedade Intelectual
mariana.sangoi@lefosse.com

Lefosse

São Paulo

Rua Tabapuã, 1227 14º andar
04533-014 Itaim Bibi
São Paulo SP Brasil
+ 55 11 3024-6100

Rio de Janeiro

Av. Presidente Wilson, 231 Conjunto 2703
20030-905 Centro
Rio de Janeiro RJ Brasil
+ 55 21 3263-5480

lefosse.com

Siga-nos nas
redes sociais