O ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

EM INFOGRÁFICOS

Março 2022

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Quem somos?

Fundado em 1997, somos o escritório pioneiro em Direito Digital no país. Vimos nascer tendências, participamos delas e nos posicionamos sempre na vanguarda. Inovamos, perseguimos a excelência e ampliamos nossas frentes de atuação para atender, de forma ainda mais completa, nossos clientes.

Nossa atuação é reconhecida no Brasil e no exterior em rankings como Chambers & Partners, Who's Who Legal, The Legal 500, Best Lawyers, Leaders League, Análise Advocacia 500, entre outros.

DPO as a Service

Atuamos com a terceirização da função completa do **DPO** (*Data Protection Officer*) ou **Encarregado pelo Tratamento de Dados Pessoais**, na condição de pessoa jurídica, desenvolvendo atividades como:

- Monitoramento da conformidade;
- Manutenção do registro das atividades de tratamento de dados pessoais;
- Relatório de Impacto à Proteção de Dados Pessoais;
- Resposta às requisições dos titulares;
- Monitoramento de leis e normas;
- Gestão da evolução de maturidade do Programa de Privacidade;
- Apoio técnico-jurídico no desenvolvimento de novas iniciativas (*Privacy by Design*);
- Condução do Comitê de Privacidade;
- Treinamento de colaboradores;
- Simulação do plano de resposta a incidentes; e
- Relacionamento com a ANPD.

Também prestamos **assessoria para o exercício interno da função** nas empresas, apoiando tanto na definição e condução da estratégia do Programa de Privacidade, quanto na execução das atividades operacionais inerentes à função.

Índice

Introdução

A LGPD (Lei Geral de Proteção de Dados), vigente no Brasil desde setembro de 2020, criou a figura do Encarregado, com base no *Data Protection Officer* (DPO), previsto no Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês), que vigora na União Europeia. O Encarregado é mencionado sete vezes pela LGPD e conta com uma seção exclusiva. Nela, são definidas suas atribuições no tratamento de dados:

Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências

Orientar funcionários e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais

Receber comunicações da ANPD (Autoridade Nacional de Proteção de Dados) e adotar providências

Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares

Ainda, de acordo com o artigo 5º, inciso VIII, da LGPD, **o Encarregado é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre controlador, titulares de dados e ANPD".** Aqui cabe uma curiosidade: inicialmente, o texto da LGPD previa que o Encarregado seria somente "pessoa natural". No entanto, após edição da Medida Provisória nº 869/2018, posteriormente convertida na Lei nº 13.853/2019, a palavra "natural" foi suprimida, **abrindo a possibilidade de nomeação de pessoas jurídicas para a função.**

Como regra, todos os controladores de dados devem indicar um Encarregado, exceto aqueles que estejam enquadrados como agentes de tratamento de pequeno porte e que não realizem atividades de tratamento de alto risco, nos termos da Resolução nº 2/2022 da ANPD.

A ANPD publicou a Resolução CD/ANPD nº 2/2022, que regulamenta o tratamento jurídico diferenciado da LGPD para **agentes de tratamento de pequeno porte**, incluindo *startups*.

Algumas obrigações de adequação à LGPD, como a exigência de DPO ou Encarregado, são flexibilizadas ou dispensadas para:


Microempresas


Empresas de pequeno porte


Startups


Pessoas jurídicas de direito privado sem fins lucrativos


Pessoas naturais


Entes privados despersonalizados

Para isso, no entanto, há necessidade de uma avaliação criteriosa de enquadramento por parte desses agentes de tratamento para verificar se, de fato, atendem aos requisitos do texto legal. Leia **aqui** report sobre o tema.

Ainda de acordo com a Resolução, **"**a dispensa ou a flexibilização das obrigações **não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD**, inclusive das bases legais e dos princípios, de outras disposições legais, regulamentares e contratuais relativas à proteção de dados pessoais, bem como direitos dos titulares**"**.

A regulamentação cria, portanto, ambiente mais favorável ao cumprimento da legislação de proteção de dados, equilibrando a viabilidade operacional e de recursos das pequenas empresas com a efetivação dos direitos e das liberdades dos titulares.

A Terceirização do Encarregado (*DPO as a Service*)

A LGPD autoriza que o Encarregado não seja um colaborador da própria empresa. Permite, portanto, que essa figura seja terceirizada a uma pessoa jurídica. As razões de escolha do *DPO as a Service* (ou DPOaaS) são várias, porém a mais valiosa é seu nível de entendimento especializado sobre a LGPD.

Os Encarregados terceirizados podem dispor de uma equipe multidisciplinar, com conhecimento em regulações setoriais, gestão de incidentes, legislações internacionais, segurança da informação, entre outros assuntos.

De acordo com o § 2º, art. 41, da LGPD, o Encarregado deve interagir, orientar, executar, assessorar, monitorar, cooperar, recomendar e decidir. Sua função é multifacetada, devendo considerar um incidente de segurança pela ótica de todos os *stakeholders* (ANPD, titulares dos dados e empresa controladora dos dados). A externalidade do *DPO as a Service* permite atuação objetiva em relação ao incidente de segurança, assim como sua especialidade oferece resposta rápida, informada e de fácil acesso à ANPD.

As formas de terceirização do Encarregado não se limitam ao *DPO as a Service*. O Encarregado externo poderá também ser contratado para:

Dar apoio na estruturação e na contratação de DPO interno

Dar apoio ao DPO interno

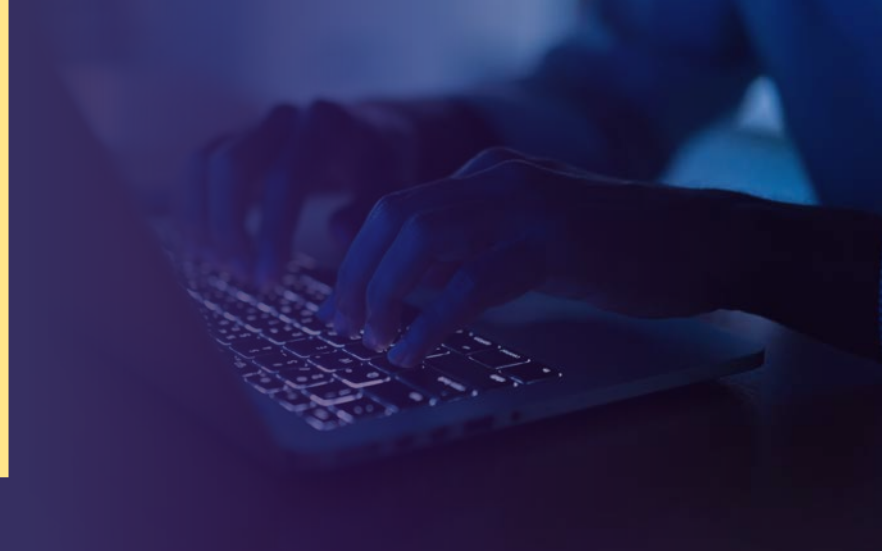
Ser conselheiro do Comitê de Privacidade

Responsabilidade

De acordo com a LGPD, o Encarregado não é responsável pelo tratamento irregular dos dados. As responsabilidades civil e administrativa estão restritas aos agentes de tratamento. Isso quer dizer que a responsabilidade do Encarregado está limitada ao exercício adequado de suas funções.

A partir de agora, confira uma série de infográficos reunindo as informações mais importantes sobre o Encarregado. Boa leitura!

DPO E OS DIREITOS DOS TITULARES DE DADOS



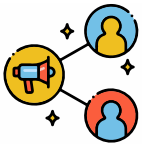
Nos programas de privacidade das organizações, devem existir estruturas de governança e ferramentas internas. O bom funcionamento desse programa se deve à atividade do DPO (*Data Protection Officer*), o Encarregado pelo Tratamento de Dados Pessoais nomeado pela empresa, que garantirá a equalização entre políticas internas e riscos à organização.

Além disso, o DPO funciona como ponto de contato entre os mais diversos atores das relações de privacidade:

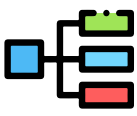
EMPRESA (controlador e operador)

TITULAR DE DADOS

ANPD

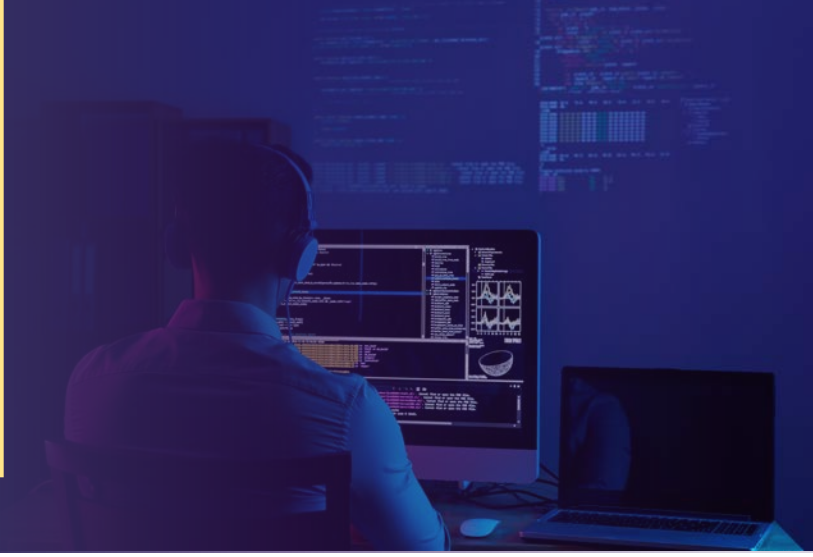


Caberá ao Encarregado organizar os fluxos de resposta às requisições dos titulares. Essa sistemática garantirá respostas adequadas e em tempo hábil.



Sobre os canais de comunicação com os titulares de dados, esses devem ser gratuitos e sob supervisão do DPO e da equipe de privacidade.

SIMULAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO



O número de ataques à segurança cibernética das empresas tem crescido exponencialmente nos últimos anos. Uma das recomendações de prevenção é que as organizações realizem simulações periódicas como forma de compreender seu grau de maturidade para lidar, de maneira efetiva, com eventuais incidentes e seus respectivos desdobramentos.

Já ouviu falar de *Bug Bounty Programs*? São autorizações dadas pelas empresas para que *hackers* realizem avaliações de segurança em seus ativos em troca de recompensa no caso de identificação de vulnerabilidades.

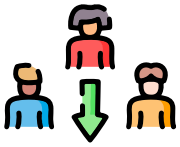
Em geral, apenas o primeiro relato de vulnerabilidade válida, isto é, reproduzível e corrigível, é recompensado. Os demais são considerados duplicados. Empresas como Facebook, Microsoft, Google, Intel e United Airlines têm programas próprios de identificação de *bugs*, enquanto Airbnb, IBM, AT&T e outras fazem uso de programas oferecidos por plataformas especializadas.

No Brasil, a primeira plataforma de *bug bounty* foi lançada em 2020 e já conta com a participação de mais de 1,5 mil especialistas em segurança da informação, além de oferecer recompensas que somam até R$ 8 mil por falha identificada. Entre os clientes estão as empresas OLX e BitcoinTrade. Saiba mais **aqui**.

De acordo com o comitê de crise estabelecido por cada organização, devem participar das simulações:

Profissionais de níveis estratégico e tático

Encarregado (DPO)



Membros dos departamentos Jurídico, Segurança da Informação, Compliance, TI, RH e Relações Públicas

Dessa forma, as simulações devem ser periódicas e acompanhar a evolução dos tipos de incidentes, de vulnerabilidades e de ataques cibernéticos existentes, como:

Simulação de acesso não autorizado;

Exfiltração de dados ou informações (pessoais ou corporativas);

Perda/roubo de equipamentos;

Extorsão (como *ransomware*); e

Interrupção de serviços.

Caso a empresa tenha um Plano de Resposta a Incidentes, o documento também fará parte das ações de simulação desempenhadas.

Após a realização das simulações, as organizações devem ser capazes de:

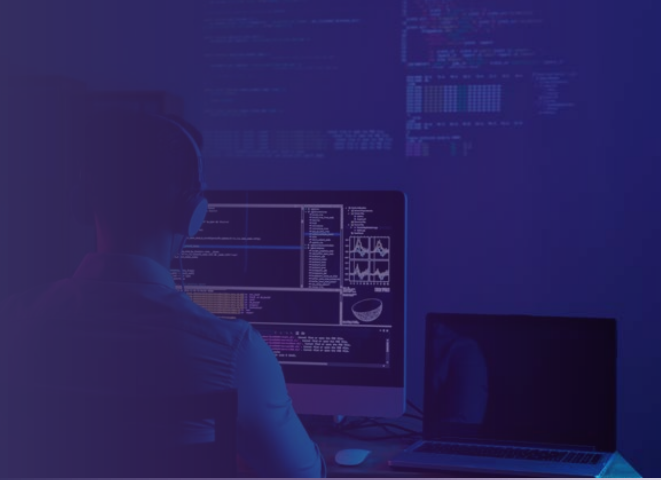
Classificar e diferenciar ameaças

Criar estratégias de mitigação de riscos

Adotar medidas de preservação de evidências

Identificar o tipo de violação de dados e as medidas jurídicas correspondentes a serem adotadas

GESTÃO DE RISCOS E PROTEÇÃO DE DADOS



Uma das atribuições mais importantes do *Data Protection Officer* ou Encarregado pelo Tratamento de Dados Pessoais é o monitoramento dos riscos sob a perspectiva de governança e de tratamento de dados pessoais.

Avaliação e gestão de risco de um programa de privacidade podem ser divididas em dois grandes blocos:

- Riscos de governança, avaliados sob a perspectiva do agente de tratamento, caso ele não proteja o titular de dados de forma adequada e eficaz;
- Riscos decorrentes das atividades de tratamento, nas quais o risco ao titular está em primeiro plano.

Dessa forma, sob o aspecto de governança, a busca é por entender quais são as obrigações institucionais do agente de tratamento, ou seja, quais estruturas e regras devem estar funcionando para garantir o cumprimento dos objetivos da LGPD.

Nos riscos de governança, as medidas de mitigação são de estruturação institucional, a exemplo da definição de:

- Comitê de privacidade
- Encarregado
- Políticas e procedimentos, com efeitos mediatos

Já nos riscos decorrentes da atividade de tratamento, as medidas de conformidade devem focar nos riscos aos titulares de dados e podem alterar a forma como a atividade é desenvolvida.

Portanto, o que se mede nos riscos de governança é a maturidade dos agentes de tratamento, enquanto nos riscos do tratamento em si, o que se observa é a efetividade da proteção em um contexto específico.

Dessa forma, caberá ao DPO atuar, ao lado dos agentes de tratamento, na mitigação dos riscos por meio dessas abordagens, metodologias e métricas específicas, garantindo, assim, total conformidade da organização com a LGPD.

REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS

O registro das operações de tratamento de dados pessoais consiste em uma das principais medidas de estruturação do programa de privacidade. É fundamental para guiar o Encarregado em suas atividades e deve indicar:

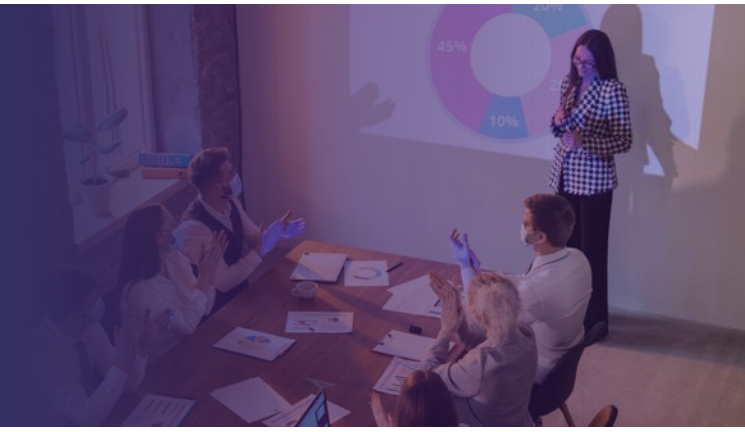
Tipos de dados tratados e categorias de titulares impactados

Bases legais para o tratamento de dados com maior chance de questionamento pelas autoridades

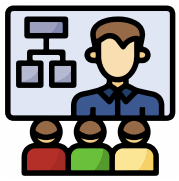
Compartilhamento de dados com terceiros

Também é tarefa do Encarregado incluir em seu planejamento de longo prazo a revisão contínua do registro das operações de tratamento de dados pessoais, assegurando uma gestão eficiente, orientada a riscos, do programa de privacidade.

PLANO DE TREINAMENTO E COMUNICAÇÃO



O Encarregado também terá como atribuição determinar conteúdo, formato, público-alvo e demais detalhes do Plano de Treinamento e Comunicação em Proteção de Dados, segundo as necessidades e os riscos do negócio.



O documento orienta o treinamento dos colaboradores e as iniciativas de comunicação interna, incluindo campanhas e ações educativas, medidas fundamentais para a prestação de contas (*accountability*) eficaz junto à ANPD (Autoridade Nacional de Proteção de Dados).

Um treinamento geral para colaboradores inclui alguns itens essenciais, entre os quais se destacam:

- Explicação sobre objetivos da LGPD;
- Descrição dos seus princípios básicos e como se aplicam à realidade da empresa;

Explicação abrangente sobre a Política de Privacidade da empresa e outros documentos aplicáveis; e

Informações sobre canais de comunicação para dúvidas e/ou reporte de incidentes.

É necessário destacar que o Encarregado pelo Tratamento de Dados Pessoais (DPO) possui função estratégica na criação de uma cultura de privacidade na organização, sendo o responsável por estruturar iniciativas de conscientização sobre o tema, fornecendo treinamento adequado às equipes de acordo com os riscos verificados dentro de cada área e/ou posição específica.

Por fim, o DPO deve ter em mente que o Plano de Treinamento e Comunicação deve ser revisto periodicamente, incluindo novas iniciativas de conscientização interna e renovação dos treinamentos já ministrados.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Em seu artigo 38, a LGPD prevê várias situações em que a Autoridade Nacional de Proteção de Dados poderá determinar a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

O RIPD deve obedecer a alguns requisitos previstos na LGPD:

- Responsabilidade de elaboração é do controlador;
- Conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados; e
- Como boa prática, o DPO pode ser acionado para apoiar as áreas de negócio na elaboração do RIPD.

Dessa forma, o RIPD representa documentação útil, necessária e, ainda, estratégica, para que os controladores possam realizar avaliação e gestão de riscos de privacidade em suas organizações, contribuindo positivamente para a conformidade com a LGPD e o sucesso do Programa de Governança em Privacidade.

Saiba **aqui** como identificar, com base na LGPD, se você é controlador ou operador.

PRIVACY BY DESIGN

O *Privacy by Design* é um *framework* de privacidade essencial para garantir a proteção de dados pessoais e mitigar os riscos aos titulares de dados desde a concepção de novas atividades de tratamento. Atualmente, o conceito está previsto no artigo 25 do GDPR e ao longo dos princípios previstos na Lei Geral de Proteção de Dados (LGPD), bem como de forma expressa em seu artigo 46, §2.

Além de uma prática consagrada internacionalmente, o *Privacy by Design* representa reforço importante para os Encarregados ou DPOs (*Data Protection Officers*) na busca pela implementação do valor da privacidade nas ferramentas de *compliance*, de modo a efetivamente contribuir para o atendimento:

Dos requisitos da lei

Dos direitos dos titulares

Da garantia da proteção dos dados pessoais

COMUNICAÇÃO DE CONTRATOS

Os agentes de tratamento devem seguir regras e procedimentos para que os contratos nas organizações estejam em conformidade com a LGPD, como os seguintes:

- Análise dos tipos de contratos e dos dados tratados;
- Definição das cláusulas contratuais;
- Análise de especificidades (questões particulares que podem ser relevantes);
- Validação interna; e
- Envio à contraparte.

Há, portanto, caminhos que devem ser percorridos para que a organização controle adequadamente seus contratos à luz da LGPD, mitigando riscos e se protegendo da melhor forma possível. Como uma boa prática, o DPO da companhia deve ser devidamente comunicado sobre cada novo produto ou serviço que venha a ser contratado ou oferecido envolvendo tratamento de dados pessoais.

Saiba mais **aqui** sobre como adequar os contratos à LGPD.

Créditos

Sócios

José Roberto Opice Blum
Renato Opice Blum
Marcos Gomes da Silva Bruno
Rony Vainzof
Camilla Jimene
Caio César Carvalho Lima
Danielle Serafino
Juliano Maranhão
Ricardo Campos
Henrique Fabretti Moraes

Conteúdo jurídico

Giovana Figueiredo Peluso Lopes
Bruno Toranzo
Yasmin Brandão

Revisão

Henrique Fabretti Moraes
Bruno Toranzo
Yasmin Brandão

Arte e diagramação

Paola Cosentino

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF