Boletim Informativo

LGPD E PROTEÇÃO DE DADOS

COMO REALIZAR A GESTÃO DE TERCEIROS E FORNECEDORES EM PROGRAMAS DE ADEQUAÇÃO A LGPD.

EDIÇÃO

JUNHO | 2022

LUCHESI ADVOGADOS

INTRODUÇÃO

Um dos temas de bastante relevância nos programas de adequação a LGPD é a gestão de fornecedores e terceiros e as diretrizes que as empresas deverão aplicar para mitigar riscos relacionados a proteção de dados. Isso porque, no âmbito da LGPD, a responsabilidade pelos danos causados ao titular de dados pode ser atribuída tanto ao Controlador quanto ao Operador, sem prejuízo da responsabilidade solidária destes dois agentes.

Nesse sentido, a gestão de fornecedores e terceiros que tratam dados pessoais em nome do Controlador se torna assunto imprescindível uma vez que, ao garantir que o terceiro tem praticas adequadas de proteção de dados e a contratação está de acordo com as finalidades estabelecidas pelas partes no momento da contratação, há uma mitigação de riscos e de responsabilidades das partes em caso de eventual incidente de segurança, isso sem contar na melhora da reputação e da imagem da empresa perante os titulares de dados que se sentirão mais seguros em confiar os seus dados pessoais a empresas adequadas a LGPD.

Sem esgotar o tema, neste boletim trataremos especificamente de um caminho, dentre vários, que pode ser percorrido pelas empresas na gestão da contratação de fornecedores e terceiros especialmente quanto aos requisitos que garantam a adequação a Lei Geral de Proteção de Dados.

1 DEFINIÇÕES IMPORTANTES – CONTROLADOR E OPERADOR. COMO IDENTIFICAR CADA UM?

Importante que se tenha de forma clara a distinção entre Controlador e Operador, para que seja possível estabelecer as obrigações e responsabilidades de cada um, dentro da relação contratada.

A ANPD recentemente publicou um Guia Orientativo de definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, que busca esclarecer dúvidas e oferecer diretrizes aos Controladores e Operadores sobre suas responsabilidades e obrigações.

Em linhas gerais, o Controlador é o agente de tratamento responsável por tomar as principais decisões referente ao tratamento dos dados pessoais e por definir a finalidade e os meios deste tratamento, tem o poder de decisão e o seu papel pode decorrer expressamente de obrigações estipuladas em leis, regulamentos ou em contratos firmado entre as partes.

Já o Operador é o agente de tratamento que irá tratar os dados pessoais para as finalidades previamente estabelecidas pelo Controlador, só agindo nos limites das finalidades determinadas pelo Controlador.

É obrigação tanto do Controlador quanto do Operador, dentro dos limites de sua atuação, adequar-se a LGPD tratando os dados pessoais com os cuidados e a proteções exigida pela lei.

2 PASSO A PASSO SOBRE OS PRINCIPAIS CUIDADOS NA CONTRATAÇÃO DE TERCEIROS E FORNECEDORES

Há alguns cuidados mínimos que os Controladores e Operadores devem observar para que se estabeleça a necessária governança dos dados pessoais a luz do que prevê a LGPD, a saber:

- Determinar em contrato as responsabilidades de cada parte, de forma expressa e de acordo com a função que cada um exerce dentro da operação, de modo a garantir que não haverá tratamento contrário ao estabelecido pela LGPD;

- Garantir que o tratamento de dados seja realizado para as finalidades especificadas no contrato e que, em havendo qualquer incidente de segurança, o Controlador seja imediatamente comunicado;

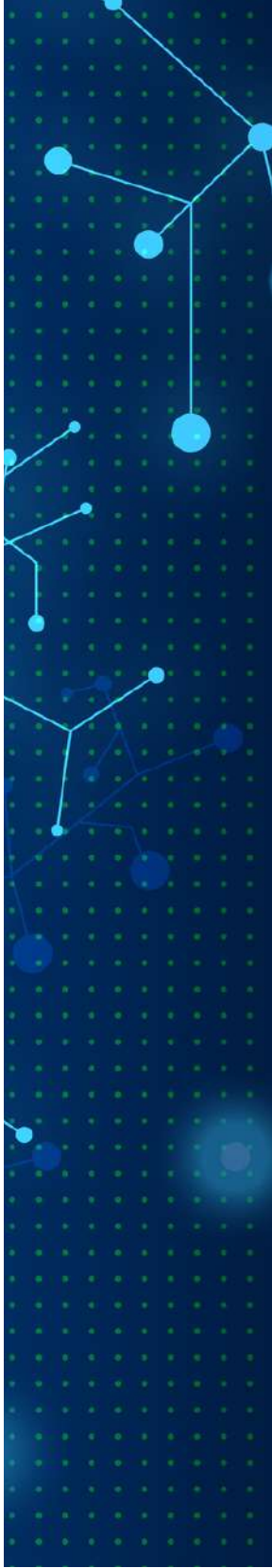
- Verificar previamente qual o risco que esse terceiro ou fornecedor traz ao Controlador, buscando analisar as questões relacionadas ao volume de dados que serão tratados, tipo de dados (se sensíveis ou não) e, com base nos resultados obtidos e evidencias recebidas, refletir sobre qual o grau de segurança e de governança que se deve exigir do terceiro/fornecedor.

- Realizar o Privacy by Design junto aos terceiros e fornecedores, em especial, nas contratações que envolvam o desenvolvimento ou utilização de algum software, sistema, plataforma ou aplicativo. Falamos sobre o tema no nosso último Boletim. Para ter acesso basta clicar aqui.

- Realizar auditoria específica no terceiro e/ou fornecedor a respeito da sua adequação a Lei Geral de Proteção de Dados.

Os cuidados apresentados acima não são taxativos, e a depender de variantes ao caso concreto, as empresas deverão aplicar além destas, outras medidas que garantam o grau de proteção desejável, e que não coloque em risco toda a sua operação.

Por isso, a importância da revisão periódica dos procedimentos internos, para garantir que os cuidados sejam observados de forma contínua, tanto para contratos existentes e já firmados, quanto para as negociações futuras ou em andamento.



3 COMO AVALIAR O RISCO E VERIFICAR A ADEQUAÇÃO DO TERCEIRO A LGPD?

Para avaliar se o terceiro/fornecedor está em conformidade com a LGPD, é necessário que, no processo indicado no item 2 acima as empresas busquem coletar as evidências necessárias que comprovem essa adequação.

Essas evidências podem ser coletadas por intermédio de uma auditoria específica (Due diligence) que avalie tanto questões relativas à segurança da informação na rede digital ou física, quanto questões relativas à governança, por exemplo, análise e implementação de políticas, regulamentos, dentre outros.

É essencial que o procedimento de Due diligence, além de levantar informações especificas sobre o tipo de contrato também avalie, sempre por meio de evidências, a implementação dos controles de segurança e proteção de dados pessoais, a partir dos seguintes passos que são sugeridos abaixo:

- Resposta a um questionário contendo controles de segurança e proteção de dados pessoais, sob o aspecto de governança, processos, cultura e tecnologia;
- Avaliação do questionário e identificação dos riscos apresentados e fatores que possam mitigá-los;
- Análise do Plano de Ação do terceiro/fornecedor, se necessário;
- Monitoramento e implementação do Plano de Ação do terceiro/fornecedor.

Esse processo é essencial para que as empresas tenham conhecimento sobre as vulnerabilidades do terceiro/fornecedor, o que consequentemente possibilita uma análise mais detalhada do risco da contratação. Caso se decida por exemplo, seguir com a contratação, mesmo que o terceiro não esteja em conformidade com a legislação, a empresa fica ciente de que assumirá os riscos da operação.

A necessidade de identificar, avaliar e gerenciar os riscos relativos à privacidade e proteção de dados é parte integrante da responsabilidade da empresa como Controladora e tema crucial para desenvolvimento de uma estrutura de gerenciamento de privacidade. Afinal, avaliar questões relativas como por exemplo, compartilhamento de uma base de dados pessoais com um fornecedor que não implementa controle mínimos de segurança da informação e não atende aos direitos dos titulares de dados pessoais, pode ser crucial para a própria manutenção da contratação.

CONCLUSÃO

Em um passado não tão distante, as empresas se preocupavam em contratar com fornecedores que tinham o melhor preço e esse era, quase sempre, o ponto de partida, para se fechar uma negociação e assinar um contrato. Nos dias atuais, nem sempre o melhor preço, garante a melhor qualidade no serviço, tampouco tem relação com a as melhores práticas de mercado em relação a governança e segurança no tratamento de dados pessoais.

Isso porque, conforme já abordado acima, a responsabilidade pelos danos causados ao titular de dados é solidária, entre Controlador e Operador. Por essa razão é tão importante, definir em contrato as obrigações e responsabilidades das partes, pois mesmo que não tenha uma determinação expressa sobre a necessidade de um instrumento contratual para tratar os dados pessoais, essa medida é vista como boa prática, já que serão estabelecidos os limites de atuação dos agentes de tratamento, serão fixados parâmetros objetivos para a alocação de responsabilidades o que poderá reduzir os riscos e as incertezas decorrentes da operação.

Atualmente o maior desafio para as empresas tem sido avaliar de modo contínuo os procedimentos realizados junto aos terceiros/fornecedores contratados e assegurar que eles estejam adequados e se utilizando de medidas de segurança que garantam a proteção dos dados pessoais tratados.

Os cuidados e providências apresentados neste Boletim, não afastam a responsabilidade dos agentes de tratamento, mas podem ajudar a mitigar os riscos em caso de um dano ocasionado em decorrência de um eventual incidente de segurança.

Desse modo, atender os requisitos da legislação de proteção de dados pessoais e exigir que os seus fornecedores e parceiros comerciais também atendam a legislação é medida essencial para a proteção do negócio e para a reputação da empresa perante seus clientes, colaboradores e mercado.

Este material foi produzido pela equipe de Privacidade e Proteção de Dados do escritório Luchesi Advogados e não tem a pretensão de esgotar o tema, mas convidar todos ao debate e à troca de experiências sobre o assunto.

Caroline Fornarolli da Cruz
caroline.fornarolli@luchesiadv.com.br

Ellen Carolina da Silva
ellen.carolina@luchesiadv.com.br

Luciana Cavalcanti Bucharelli
luciana.bucharelli@luchesiadv.com.br

Thamiris do Carmo de Souza
thamiris.souza@luchesiadv.com.br

LUCHESI
ADVOGADOS

SÃO PAULO
Avenida Francisco Matarazzo, 1500
16º andar - Torre New York
CEP: 05001-100

(11) 3662-4333 / (11) 3664-3464
luchesiadv@luchesiadv.com.br luchesiadv.com.br