28 DE JANEIRO

DIA INTERNACIONAL DA PROTEÇÃO DE DADOS

E-book

Melhores práticas de Governança e Conformidade com a LGPD

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

WWW.OPICEBLUM.COM.BR

Índice

1. Dia Internacional da Proteção de Dados

No dia 28 de janeiro, celebra-se o Dia Internacional da Proteção de Dados. A data – oficializada em ao menos 50 países – faz referência à Convenção 108, que foi aberta para assinatura em 28 de janeiro de 1981.

A Convenção 108 é o primeiro e, até então, o único documento internacional vinculante. Apesar de sua origem europeia, pode ser ratificado por Estados fora do Conselho Europeu – como é o caso da Argentina.

Assim como a Convenção 108, o Dia Internacional da Proteção de Dados – primeiramente, instituído na Europa – hoje tem relevo global. E, a exemplo de outros marcos comemorativos, apresenta-se como um convite à reflexão.

No período entre 2009 e 2019, bilhões de registros de empresas ao redor do mundo foram sujeitos a incidentes de segurança. Nesse cenário, cabe a nós enquanto titulares dessas informações ponderar sobre como e quais dados pessoais disponibilizar. Em um mundo crescentemente digitalizado, a preocupação com a Privacidade e com os dados pessoais não pode ser ignorada.

De forma prática, diversas aplicações que utilizamos no dia a dia nos permitem modular nossas configurações de Privacidade – sejam aplicações de compras online, comunicação, lazer, esporte e deslocamento ou navegadores, mídias sociais e redes de caráter profissional. Em todas elas, a utilização de senhas com variação de tipos de caracteres é essencial. Qualquer coisa que não se pareça com H0i5ef@2ç merece alguns minutos de reflexão.

Olhando para trás, o Dia Internacional da Proteção de Dados tem ampliado progressivamente sua envergadura. De 2018 para 2019, a data dobrou seu alcance. A cobertura midiática, por sua vez, teve crescimento ainda mais expressivo. Temas ligados à Privacidade e Proteção de Dados são cada vez mais debatidos tanto em reportagens quanto em eventos.

Visando nos juntar a esse movimento, o Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados preparou este e-book, com artigos sobre diferentes aspectos da Proteção de Dados e Privacidade. Boa leitura!

2. Conformidade com a LGPD e o Dia Internacional da Proteção de Dados

2. Conformidade com a LGPD e o Dia Internacional da Proteção de Dados

O Dia Internacional da Proteção de Dados é comemorado em 28 de janeiro por uma decisão do Conselho Europeu, em referência ao dia em que o primeiro instrumento transnacional, com força vinculante, a tratar da Proteção de Dados como objeto de tutela foi assinado (Convenção 108, de 1981).

Assim, em uma data tão simbólica, trazemos luz às discussões relevantes sobre o tema, especialmente no ano em que a norma brasileira - a Lei Geral de Proteção de Dados (Lei 13.709/2018 ou LGPD) - entrará em vigor, previsto para acontecer em 16 de agosto.

Na medida em que a vigência da lei se aproxima, muitas organizações ainda se perguntam: como adequar o meu negócio à Lei Geral de Proteção de Dados? Em outras palavras, o que fazer para garantir que minha organização seja capaz de respeitar todos os princípios, cumprir todas as obrigações e atender a todos os direitos previstos na LGPD?

O objetivo deste texto é justamente compartilhar nossa visão e metodologia, de forma condensada, bem como o caminho que entendemos mais eficiente rumo a essa tão alardeada e relevante adequação.

Para nós, escritório fundado em 1997 já especializado em Direito Digital, era natural o entendimento da relevância do tema, de forma que há anos auxiliamos empresas na mitigação de riscos relacionados à Privacidade e Proteção de Dados, muito baseado na experiência do exterior, principalmente Europa, continente berço das discussões e normativas sobre o tema (não é por acaso que o Dia Internacional de Proteção de Dados criado pelo Conselho Europeu é comemorada no mundo todo).

Foi nesse contexto, apoiando organizações a se adequarem à regulamentação europeia de Proteção de Dados (*General Data Protection Regulation*) e já sabendo que a nossa futura Lei Geral de Proteção de Dados (LGPD) seria inspirada nela, pois inclusive contribuímos legislativamente desde o início da sua construção, que nos inspiramos nas melhores práticas já utilizadas para a adequação ao GDPR, visando aplicar uma abordagem condizente com a realidade das organizações brasileiras em sua busca pela conformidade.

Nesse sentido, a primeira constatação foi a de que a organização precisaria conhecer suas atividades de tratamento de dados pessoais e o papel delas dentro de cada modelo de negócio. Primeiro, porque o artigo 37 da LGPD traz essa obrigação, e depois, porque a lógica de fato sugere que para tratar dados de forma lícita, é preciso saber quais são esses dados, onde eles estão e para o que eles servem.

Assim, a tendência inicial foi identificar e analisar todos os processos que envolviam dados pessoais para, então, apontar quais seriam suas inconsistências perante à LGPD, isto é, o que precisaria ser mudado para que aquele processo que envolvia um dado pessoal estivesse adequado à referida lei.

Essa lógica não está errada, muito pelo contrário. Contudo, o denominado data mapping deve ser utilizado de forma estratégica ao longo da adequação. Isso porque os processos mudam o tempo todo, ou seja, uma inconsistência identificada hoje pode não existir mais amanhã.

Por exemplo, se forem identificadas três inconsistências para cada processo em uma organização que tenha 300 atividades de tratamento de dados (uma média razoável quando se olha para os processos macro), deverão ser corrigidas 900 inconsistências ao todo.

Na prática, não é razoável criar 900 planos de ação que precisarão ser endereçados no curto espaço de tempo que temos até agosto de 2020. Além disso, essa abordagem não é sustentável a longo prazo, posto que sempre seria necessário buscar essas inconsistências a cada mudança ou criação de um novo processo.

Assim, analisamos profundamente as boas práticas de Governança implantadas internacionalmente, incorporando-as em nossa jornada de adequação, e passamos a utilizar uma abordagem voltada ao panorama macro: a criação de um programa de *Compliance* em Proteção de Dados.

Um programa de *Compliance* é fundado em: engajamento da liderança (*tone at the top*); mecanismos de resposta e investigação a inconsistências legais; uma função ou equipe de *Compliance* para gerir e monitorar o programa; responsabilização e prestação de contas (*accountability*); entre outros pontos que, inclusive, encontram respaldo na própria LGPD, quando esta encoraja a implantação de boas práticas de Governança (art. 50, §2º).

Sobre a base de *Compliance*, seria necessário inserir as especificidades previstas na LGPD. Assim, inspirados também nos principais frameworks de Privacidade empregados mundo afora, criamos um *framework* especialmente customizado para atender aos requisitos da LGPD.

Dessa forma, as regras de Privacidade da organização são criadas em conexão com a própria Governança corporativa, irradiando orgânica e construtivamente nas atividades de tratamento de dados pessoais, posto que as regras devem ser seguidas por todos os colaboradores, que são a 1ª linha de defesa de uma organização.

Este *framework* é composto por 11 pilares e cada um deles visa atender a uma necessidade prevista, direta ou indiretamente, pela LGPD. São eles:

1. Gestão e Governança: avalia-se a existência de uma estrutura que garanta o *accountability* do Programa de Privacidade, bem como o posicionamento do Encarregado e engajamento da liderança.
2. Coleta, Uso e Armazenamento: o mais abrangente dos pilares, contempla os controles que a organização possui (políticas, processos, procedimentos etc.) para que os principais pontos do ciclo de vida do dado sejam executados dentro das regras previstas em Lei. Por exemplo, é nesse pilar que identificamos se as atividades de tratamento de dados possuem uma base legal adequada e se é atribuída (e observada) uma finalidade para o uso destes dados.
3. Transparência: os titulares de dados precisam saber o que é feito com seus dados pessoais.

Neste pilar, avalia-se a existência de mecanismos internos para identificar se a organização é suficientemente transparente com o titular do dado. Entra aqui também entender se os Avisos de Privacidade preenchem todos os requisitos legais.

4. Consentimento: caso a organização utilize consentimento para tratar dados pessoais, deve-se garantir que todos os requisitos dessa base legal da LGPD sejam cumpridos (ser livre, informado e inequívoco). Além disso, a organização deve garantir controles para gerenciar a opção dos titulares – concessão ou revogação do consentimento.

5. Exercícios de Direitos do Titular: a organização deve possuir processos internos para garantir que os titulares sejam atendidos corretamente suas requisições, como possibilidade de revogação de consentimento, e de forma a não expor dados de terceiros nem segredos de negócio.

6. Compartilhamento: Avalia-se a existências de políticas e procedimentos que garantam que, ao compartilhar dados com terceiros (dentro ou fora do Brasil), estes sejam validados previamente e que salvaguardas técnicas e contratuais sejam impostas para evitar tratamento indevido destes dados.

7. Segurança: Os dados devem ser tratados de forma segura, portanto, a organização deve possuir um programa de segurança da informação que garante a aplicação das medidas de segurança necessárias, alinhadas aos riscos identificados e implementadas desde a concepção de novos produtos, serviços, processos etc.

8. Resposta a Incidentes: Não basta proteger o dado, deve-se estar preparado no caso de algum incidente (por exemplo, vazamento de dados). Aqui, é entendido o nível de prontidão da organização para a resposta de um incidente.

9. Monitoramento: Como todo bom programa de *Compliance*, é necessário monitorar se todas as regras, políticas, processos, procedimentos etc., estão sendo observados na prática. Além de identificar inconsistências – e poder agir para que estas não ocorram novamente – o monitoramento pode gerar indicadores que auxiliam na gestão do Programa de Privacidade.

10. Avaliação de Risco: é impossível olhar para todos os pontos ao mesmo tempo, principalmente, sabendo que recursos são limitados e devemos utilizá-lo com inteligência. Por isso, neste ponto identifica-se a existência de uma prática periódica de avaliação de riscos de Privacidade e se essa avaliação é utilizada para direcionar as prioridades do Programa de Privacidade.

11. Treinamento e Comunicação: a criação de uma cultura de Privacidade é indispensável para que todos os colaboradores sejam agentes de Privacidade e ajudem a organização a estar em conformidade. Avalia-se aqui a existência de um plano de treinamento e comunicação que esteja alinhado à política corporativa de Privacidade e Proteção de Dados.

Para cada um deste pilares, são avaliados dezenas de critérios e para cada um deles é determinado o nível de maturidade com a LGPD, da seguinte forma:

- Inexistente
- Insuficiente
- Em construção
- Implementado
- Otimizado

Ao avaliarmos a maturidade da organização com base nestes pilares, conseguimos traçar tanto os planos de ação que precisarão ser endereçados para que se alcance um nível adequado de conformidade como identificar onde estão os principais riscos. Essa análise é feita utilizando-se também dos insumos do mapeamento.

Mediante a avaliação da organização e com base no *framework*, identificamos não só o que precisa ser feito para se adequar à LGPD, mas também o racional de priorização, concentrando esforços no que é importante e deixando para um segundo momento o que apresenta baixo risco, tanto para a organização, como, principalmente, para os titulares de dados.

Continuando a jornada de adequação, é estruturado o Programa de Privacidade e Proteção de Dados através da definição da estrutura de Governança (DPO, Comitê de Privacidade, alçadas de decisão etc.) e desenho das políticas e procedimentos internos. Nesta etapa, identificamos que o *Data Protection Officer* é fundamental para que o Programa de Privacidade seja, de fato, incorporado ao dia a dia da organização.

Considerando a falta de disponibilidade deste profissional no mercado e a dificuldade de capacitar um colaborador no prazo e com o nível de conhecimento necessários, uma possibilidade que tem sido cada vez mais empregada é a contratação do *DPO as a Service*, nada mais do que a terceirização desta função.

A etapa final desta jornada de adequação consiste em refazer o diagnóstico inicial, reavaliando a maturidade da organização com base em nosso framework, mapeando eventuais pontos ainda não endereçados.

O fim do projeto de adequação à LGPD significa apenas o início do trabalho de manter a consistência e a observância prática do Programa de Privacidade e Proteção de Dados, normalmente a principal atribuição do DPO, que pode contar com auxílio de softwares de gestão, além do apoio contínuo do time de segurança da informação.

Quanto ao mapeamento de dados entendemos que este continua sendo extremamente relevante, quando usado estrategicamente, ou seja, sendo considerado no contexto de um programa de *Compliance* e não apenas como instrumento para correção de inconsistências de processo.

Para ilustrar o raciocínio, apresentamos quatro exemplos de como usar o mapeamento de forma inteligente num projeto de adequação:

a) Para atribuição de riscos: o mapeamento fornece elementos quantitativos para uma atribuição de risco mais precisa, especialmente porque revela o volume de dados utilizados numa operação, a existência de dados sensíveis, de crianças etc;

b) Para garantir maior e melhor transparência: o conhecimento dos processos que envolvem dados pessoais possibilita à organização estruturar sua comunicação e avisos de Privacidade de forma mais completa e assertiva.

c) Para atendimento ao direito de confirmação de tratamento e direito de acesso: Saber quais são os dados pessoais, bem como eles são utilizados pela organização facilita o atendimento ao direito do titular de confirmar que suas informações são objeto de tratamento, bem como ao direito de acesso desse titular a essas informações; e

d) Para atribuição de uma base legal: só é possível realizar uma operação de tratamento de dados pessoais, se essa operação estiver justificada em uma das bases legais dos artigos 7º e 11º da LGPD.

De forma resumida, nossa metodologia implica:

I. Conhecer as principais atividades que envolvem tratamento dados pessoais de uma organização (data mapping);

II. Criar um sistema de *Compliance* (que chamamos de Programa de Privacidade e Proteção de Dados);

III. Ancorar as regras previstas pela LGPD em políticas, procedimentos e processos internos;

IV. Avaliar a maturidade da organização em relação ao Programa de Privacidade e Proteção de Dados que deve ser criado, para desenvolver planos de ação e identificar os pontos mais críticos;

V. Avaliar os riscos de Privacidade para priorizar os planos de ação e concentrar recursos onde é mais importante;

VI. Estruturar o Programa de Privacidade e Proteção de Dados;

VII. Iniciar a atuação do *Data Protection Officer*;

VIII. Conduzir uma revisão final do nível de maturidade da organização em relação ao framework proposto; e

IX. Dar continuidade ao Programa, garantindo sua aplicação prática e consistente, envolvendo ou não o uso de ferramentas de gestão.

Como mensagem final, relembramos que, em nosso entendimento, nenhum programa de *Compliance* é infalível e risco zero é impraticável. Devemos ter em mente que, se já não o era antes, com a regulação do uso de dados pessoais, qualquer atividade que envolva o tratamento deste tipo de informação passou a ser uma atividade de risco. Portanto, o objetivo de um Programa de Privacidade é reduzir este risco ao mínimo possível, não necessariamente eliminá-lo completamente.

** Autoria de Rony Vainzof, Caio Lima, Henrique Fabretti e Tiago Neves Furtado. Publicado em https://politica.estadao.com.br/blogs/fausto-macedo/conformidade-com-a-lgpd-e-o-dia-internacional-da-protecao-de-dados/.*

3. Cinco elementos necessários para a criação de um programa de Privacidade e Proteção de Dados

3. Cinco elementos necessários para a criação de um programa de Privacidade e Proteção de Dados

A Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) – trouxe várias regras, obrigações e direitos relacionados à Privacidade e Proteção de Dados pessoais que, caso sejam aplicados de forma estanque para cada operação de tratamento de dados pessoais, dão a impressão de extrema complexidade e dificuldade em atendê-los.

Porém, a própria LGPD trouxe a indicação de como solucionar este problema: a adoção de programas de Governança de dados pessoais. A vantagem dessa abordagem é a possibilidade de construir regras internas de conformidade com a LGPD, apoiada em pilares básicos de *Compliance*, que devem ser observados por seus colaboradores e refletidos nas atividades que envolvam tratamento de dados pessoais. Portanto, trata-se de transformar um programa de adequação à LGPD em uma jornada perene de transformação nas organizações sobre o tema.

Mas o que é Governança? Inspirados pelo conceito disponibilizado pelo Instituto Brasileiro de Governança Corporativa (IBGC), podemos definir Governança como um sistema de gestão e monitoramento que envolve todos os níveis de uma organização, através do qual seus princípios e valores básicos são convertidos em recomendações objetivas, de modo alinhar seu interesse com a finalidade de preservá-la e otimizar o seu valor econômico de longo prazo.

Trazendo este conceito para a esfera da Privacidade, o programa de Governança deve garantir que uma organização esteja em conformidade com a legislação (no caso, a LGPD), sob a orientação dos princípios e valores que dão sustentação ao propósito de existência da própria organização. Nesse contexto, ela deve considerar a necessidade de validar seus princípios e propósitos, bem como compreender o papel dos dados pessoais no seu modelo de negócio, protegendo-os de modo estratégico e garantindo sua adequada utilização.

Caso não haja esse alinhamento – isto é, entre o uso adequado dos dados e a cultura e os valores da organização –, um programa de Governança corre sério risco de se resumir a políticas e procedimentos escritos num papel, sem qualquer poder de engajamento das pessoas que fazem a organização e, consequentemente, distante do modelo de negócio vivido pela empresa.

Criar e gerir um programa de Privacidade eficiente e que traga um nível adequado de conformidade com a LGPD traz uma série de desafios. Listamos, a seguir, os cinco principais pontos de atenção para que o seu Programa de Privacidade traga bons resultados:

1. Diagnóstico prévio:

Um Programa de Governança eficiente necessita de conhecimento prévio sobre a empresa e seu modelo de negócio. É preciso saber quais as principais atividades desempenhadas pela organização que envolvem dados pessoais, que tipos de dado são utilizados, quais as ferramentas etc. Somado a esse aspecto técnico, também devem ser levados em conta os valores, os objetivos e a estrutura de Governança corporativa pré-existente. Assim, é possível identificar o que precisará ser construído ou adaptado;

2. Aderente ao modelo de negócio:

Não adianta criar um Programa de Governança cujas normas e procedimentos não consigam ser cumpridos;

3. Orientado a risco:

É basicamente impossível querer atacar todos os problemas e deficiências da empresa de uma única vez. Assim, uma avaliação de risco que indique quais pontos necessitam de maior atenção, recursos e dedicação do DPO é indispensável. Neste ponto, o mapeamento de dados ajuda, inclusive, a definir melhor o risco. Por exemplo: uma empresa que não possui nenhuma operação de tratamento baseada no consentimento não precisará, em um primeiro momento, investir recursos para criar uma estrutura de gestão de consentimento;

4. Buscar engajamento:

Prática contínua de treinamento e comunicação assertiva, com linguagem e conteúdos adequados, e que faça sentido no contexto das atividades da organização. Nesse sentido, o Programa deve ser cumprido e encorajado por todos, desde o presidente até o estagiário – o exemplo vem de cima; e

5. Continuidade:

O Programa de Governança necessita de gestão e atualização contínua, e, para tanto, deverá sempre ser revisado e reavaliado, de modo a garantir que continue fazendo sentido para a organização. Ou seja, o Programa de Privacidade e Proteção de Dados vai muito além de criar políticas e procedimentos.

Dito isso, a construção de um Programa de Privacidade não ocorre do dia para a noite e, sim, no longo prazo, posto que é, antes de mais nada, uma questão de cultura organizacional.

4. Privacy by design: inovação com segurança

4. Privacy by design: inovação com segurança

A Lei Geral de Proteção de Dados (LGPD - Lei 13.709/2018) estabelece novo paradigma no contexto legislativo brasileiro ao amoldar as atividades de tratamento, cada vez mais conexas com as práticas de sociedade, que encontram nas informações potencial para novos modelos de negócios.

Como forma de garantir que esses novos padrões tenham atenção às regras de Privacidade, a LGPD adota a figura do Privacy by Design (Privacidade desde a concepção), prestigiada também no regulamento europeu, que engloba obrigatoriedade de que aos novos produtos ou serviços (incluídos o desenvolvimento de sistemas, hardware ou software e processos internos) seja feita análise sobre aderência a medidas de segurança, técnicas e administrativas que garantam a proteção dos dados e evitem formas de tratamento inadequados ou ilícitos.

Em contexto prático, é de extrema importância que no cenário de adequação à LGPD os agentes de tratamento definam processos para cumprir com esta obrigação da lei (artigo 46, §2º), ou ainda ajustem as atividades de inovação ou melhoria de produtos e serviços já internalizadas, de forma compatível com as regras de Governança internamente instituídas.

Vale ressaltar que os estudos sobre a implementação do Privacy by Design, assim como as discussões sobre Privacidade e Proteção de Dados pessoais, antecedem a LGPD. Sua origem é intrinsicamente relacionada ao framework de Privacidade desenvolvido por Ann Cavoukian, na década de 1990, no Canadá.

Tal estudo foi responsável por estabelecer alguns princípios, dentre os quais se destacam os da proatividade para análise preventiva dos temas de proteção, a predeterminação da Privacidade como padrão (privacy by default), incorporação das regras dispostas na LGPD desde o desenho, assegurando a funcionalidade ao titular, conferindo transparência e objetivando a segurança em todo o ciclo de vida das informações utilizadas.

O diferencial para sua prática eficaz é a interlocução entre os princípios indicados e as características das atividades desenvolvidas pelos agentes de tratamento.

É importante a construção dos meios de análise com sensibilidade aos interesses das empresas, para que sejam verificados os riscos atrelados ao tratamento de forma assertiva, bem como que exista harmonização com o fundamento da lei para o desenvolvimento tecnológico e a inovação. Tal premissa pode ser adotada pelo Encarregado (*Data Protection Officer)* quando da orientação das áreas a respeito da análise de projetos.

O *Privacy by design* deve nortear - não impedir - as atividades inovativas e, nesse aspecto, pode ser importante ferramenta para garantir a conformidade com a legislação, identificar medidas de mitigação de conflitos, além de resultar em vantajoso diferencial competitivo. Para esse objetivo, é importante a visão estratégica nas distintas formas de adequação.

5. Quatro perguntas que devem guiar a escolha do Plano de Adequação a ser contratado por uma Organização

5. Quatro perguntas que devem guiar a escolha do Plano de Adequação a ser contratado por uma Organização

A publicação da Lei 13.709/2019 trouxe diversas discussões e questionamentos acerca do que fazer para se adequar a essas novas regras. É preciso fazer um mapeamento? Como fazê-lo? Quais sãos os documentos de que preciso para me adequar? Como identifico a maturidade do nível de Governança? Como adequar os contratos? Como fazer gestão de terceiros? Essas e muitas outras perguntas vêm sendo amadurecidas dentro dos mais diversos tipos de organizações.

No entanto, antes de respondê-las, cabe promovermos uma reflexão – tão necessária fundamental – sobre como escolher o Plano de Adequação correto para a minha organização. É nesse contexto que apresentamos quatro perguntas cujas respostas devem guiar a análise e a decisão de qual Plano de Adequação deve ser contratado. São elas:

1. Houve uma etapa para compreensão da dimensão da minha organização?

Essa avaliação é essencial para que o projeto de adequação seja confeccionado de forma compatível com o seu modelo de negócio. Conhecer particularidades, como o ramo de atuação, frente de negócio, quantidade de funcionário, número de departamentos, forma de controle e gestão (centralizada ou não), é essencial nesse contexto. Um Plano de Adequação apresentado sem essa avaliação inicial corre sério risco de não se amoldar ao que a organização precisa ou pode suportar.

2. O Plano de Adequação considera o mapeamento das principais atividades que envolvem tratamento de dados pessoais?

O mapeamento de forma isolada é insuficiente para que uma organização esteja adequada à LGPD. Mas conhecer as principais atividades que envolvem tratamento de dados pessoais é essencial para entender o modelo de negócio, atribuir riscos e orientar a construção do plano de Governança, para além da obrigação legal de se manter os registros da operação. Assim, a depender da compreensão do modelo de negócio e da dimensão da organização, um Plano de Adequação sólido deve guiar a organização para um mapeamento mais efetivo e adequado à realidade de cada negócio;

3. O Plano de Adequação considera o diagnóstico e a construção de uma Estrutura de Governança orientada ao modelo de negócio da organização?

É importante que o Plano de Adequação contemple uma fase de diagnóstico da maturidade de Governança, de modo a propor a construção de uma estrutura que faça sentido para a organização. Em outras palavras, que seja aderente à sua cultura. Neste ponto, o convidamos a ler o segundo artigo desta série sobre o Dia Internacional da Proteção de Dados. O referido texto indica os cinco elementos necessários para a criação de um programa de Privacidade e Proteção de Dados;

4. O Plano de Adequação contempla o envolvimento da Organização e seus colaboradores?

Um bom plano de Adequação deve prever o envolvimento da Organização e dos seus colaboradores na execução das tarefas e análises a serem desenvolvidas. Para além do engajamento, esse envolvimento garante que o plano de adequação que está sendo construído faça sentido junto ao modelo de negócio da organização.

As respostas aos questionamentos acima têm como intenção indicar os primeiros passos para a escolha do formato ideal do Plano de Adequação. É claro que o orçamento, a empatia com os consultores, a qualificação da equipe, entre outros fatores também são importantes na hora de decidir qual Plano de Adequação contratar.

No entanto, neste momento tão embrionário de formação cultural das organizações brasileiras em relação à Proteção de Dados, o que essas perguntas também podem revelar é se realmente existe uma preocupação por parte da consultoria responsável por criar o Plano de Adequação em buscar conhecer a organização e moldar seus entregáveis ao negócio. Ou será que o plano apresentado é um modelo no formato “tudo ou nada” para entregar o mais rápido possível?

Após entender essas questões, o que resta fazer para tornar a sua empresa aderente à LGPD é escolher o Plano de Adequação que melhor se adequa à realidade da sua organização e, enfim, colocar a “mão na massa”.

6. Data Protection Officer (DPO): a profissão de 2020

6. Data Protection Officer (DPO): a profissão de 2020

As discussões em torno de como se adequar à Lei Geral de Proteção de Dados já possuem caminho quase que certo e bem delineado pelo mercado, independentemente de a condução do projeto ser interna, por consultoria de segurança e tecnologia, por escritório de advocacia ou ser feita a 4 ou mais mãos. Primeiro é feito diagnóstico que resulta em diversos planos de ação, depois começa a ser estruturado o Programa de Privacidade, o qual usualmente pressupõe a criação de regras e processos internos, além do ajuste em sistemas.

Porém, quando toda essa estrutura começa a ser colocada em prática, as organizações precisam de alguém que vá gerir o Programa de Privacidade que acaba de nascer, função essa que deve ser atribuída ao Encarregado pela Proteção de Dados Pessoais ou DPO (*Data Protection Officer*). Em que pese nossa legislação não atribuir essa responsabilidade diretamente ao Encarregado, ela traz diversos dispositivos que indiretamente apontam para essa necessidade.

Para cumprir o princípio da responsabilização e prestação de contas (art. 6º, inciso X, da LGPD), comumente chamado de *accountability*, é indispensável que a organização gere evidências de que está em conformidade com a LGPD, o que pode ser feito, por exemplo, por meio dos relatórios de impacto à proteção de dados, geração de indicadores (quantidade de incidentes, pessoas treinadas, alertas gerados por ferramentas de DLP etc.), manutenção do registro das atividades de tratamento, atas de reunião do Comitê de Privacidade, entre outras atividades.

As políticas que foram criadas e implantadas pela organização precisam ser incorporadas ao dia a dia das áreas e colaboradores, além de ser necessário que alguém monitore o cumprimento delas, com medidas de investigação e resposta para os casos de não conformidade. Áreas de negócio desenvolvem novos produtos, serviços, processos, práticas de negócio que envolvem o tratamento de dados pessoais e irão precisar de apoio para garantir que todas as iniciativas nasçam adequadas às regras de privacidade.

Mesmo não previsto no enxuto rol de atribuições do artigo 41 da LGPD, nada mais natural que a organização utilize o Encarregado para desempenhar estas atividades.

O grande desafio é que profissionais que já possuam a experiência e conhecimentos necessários para assumir este papel são escassos no mercado, uma vez que, idealmente, reúnem conhecimentos de áreas muito diferentes, como tecnologia e segurança da informação, direito e governança.

Nesse sentido, possível alternativa é a contratação de Encarregado terceirizado (modalidade comumente chamada de DPO as a Service nos países sob escopo do GDPR), modalidade que a LGPD tornou possível após as alterações sofridas com o advento da Lei nº 13.853/2019. Como principais benefícios da contratação de DPO terceirizado podemos mencionar:

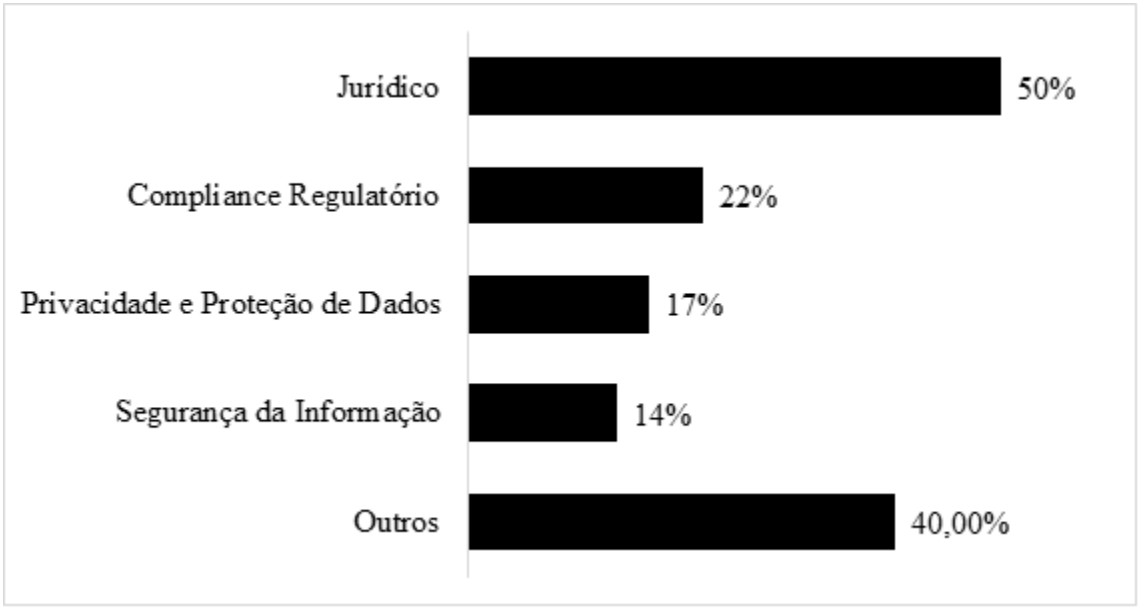
- Maior expertise e experiência em todas as linhas de conhecimento desejáveis: o prestador deste serviço pode contar com equipe multidisciplinar, envolvendo profissionais de tecnologia, direito e governança, empregados conforme a necessidade do cliente;
- Independência: dependendo do contexto da organização, o DPO terceirizado pode contar com nível de independência maior que DPO interno, uma vez que não terá envolvimento na determinação de como e de qual forma dados pessoais serão tratados por seu contratante;
- Flexibilidade: nos estágios iniciais do Programa de Privacidade, provavelmente será necessário esforço muito maior do Encarregado, posto que ainda não se tem a cultura de proteção de dados e todas as novas regras e processos precisam ser incorporados ao dia a dia da empresa. Passada essa fase, a demanda para este profissional será menor e DPO terceirizado conseguirá se adequar mais facilmente a estas mudanças.
- Benchmarking: normalmente, o DPO terceirizado irá prestar este tipo de serviço para diversas empresas, sendo possível compartilhar as boas práticas e experiências observadas nestas organizações.

Porém, alguns cuidados devem ser tomados antes de se contratar DPO terceirado. Alguns aspectos são mais gerais, como: certificar-se da experiência e qualificação do profissional e do time de profissionais que prestarão este serviço.

Outros são mais específicos, incluindo a questão de estabelecer contratualmente o nível de responsabilização do contratado em casos de danos causados ao titular ou sanções sofridas pelas empresas, por conta da atividade do DPO.

Especificamente em relação ao contrato firmado com o DPO terceirizado, é também altamente recomendável que seja bem delineada todas as atividades que deverão estar no escopo deste profissional e quais seriam passíveis de contratação à parte, evitando a existência de questões ou áreas não cobertas pelo serviço deste profissional.

Nessa linha, trazemos pesquisa publicada pela International Association of Privacy Professionals (IAPP), que mostra onde, normalmente, a função de privacidade está alocada nas organizações (neste caso, para profissionais in-house, mas cujo racional pode ser empregado na contratação de terceiros):



Adicionalmente, o ideal é que esse terceiro tenha livre acesso à alta liderança da organização e seu contrato seja gerenciado por áreas com baixo nível de conflito de interesses com a atividade desempenhada pelo DPO.

7. Como cumprir os Direitos dos titulares

7. Como cumprir os direitos dos titulares

Até a aprovação da Lei Geral de Proteção de Dados, existiam no Brasil diversos direitos esparsos sobre o assunto, como na área consumerista, trabalhista, de direitos no ambiente digital, telecomunicações, entre outros. Não existiam, contudo, direitos específicos relacionados à Privacidade e Proteção de Dados que possibilitassem maior controle, por todos nós, sobre os nossos dados.

Assim, a LGPD trouxe em seu Capítulo II os direitos dos titular de dados pessoais que podem ser exercidos a qualquer momento e mediante requisição ao controlador. Como exemplo, temos o direito de acesso; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; eliminação dos dados pessoais tratados com o consentimento do titular; revogação do consentimento; entre outros.

Porém, como os controladores podem dar efetividade a esses direitos que podem ser solicitados pelos titulares a qualquer momento? Como se adequar à LGPD e estar preparado a dar vazão às solicitações que as empresas receberão a partir de agosto de 2020?

1) Governança em Privacidade e Proteção de Dados

É importante que a empresa crie programa de Governança em Privacidade e Proteção de Dados, como boa prática trazida pelo art. 50 da LGPD. Com isso, garantirá que a organização atinja o nível adequado de conformidade, evitando, por exemplo, que as respostas dadas aos titulares abram espaço para futuros litígios ou ações por parte da Autoridade Nacional de Proteção de Dados (ANPD).

Dentro desse programa de Privacidade, é importante que esteja claro quem são os responsáveis por todo o processo de recebimento, tratamento e resposta das requisições dos titulares, garantindo que estas sejam atendidas dentro do prazo legal, com a qualidade necessária e sem expor dados de terceiros e segredos de negócio do controlador.

Idealmente, dentro desse fluxo de tratamento das requisições dos titulares, o Encarregado (DPO) terá participação ativa para que faça a correta gestão dos pontos mencionados acima, além de garantir que situações atípicas ou que tragam maior risco à organização sejam tratadas adequadamente.

2) Operacionalização procedimental

Definidas as regras internas e os atores responsáveis, a empresa deverá decidir como operacionalizar o cumprimento das solicitações de direitos dos titulares.

A ICO (Information Comissioner's Office - Autoridade de Proteção de Dados do Reino Unido) recomenda o seguinte checklist para a operacionalização do cumprimento dos direitos dos titulares, especialmente o direito de acesso[1], em tradução livre:

A) Preparação para as requisições de direito de acesso dos titulares:

i) sabemos como reconhecer uma solicitação de direito de acesso e entendemos quando o direito de acesso se aplica;

ii) temos uma política sobre como registrar solicitações que recebemos verbalmente (se for uma forma que a empresa recebe a solicitação);

iii) entendemos quando podemos recusar uma solicitação e estamos cientes das informações que precisamos para fornecer aos titulares quando recusarmos;

iv) entendemos a natureza da informação complementar que precisamos fornecer em resposta à solicitação de direito de acesso.

B) Cumprimento das solicitações de direito de acesso:

i) temos processos vigentes para garantir que respondamos a uma solicitação de direito de acesso sem atraso injustificado e dentro do prazo determinado pela legislação;

ii) estamos cientes das circunstâncias de quando poderemos estender o prazo de atendimento da solicitação;

iii) entendemos que há uma ênfase particular para se usar linguagem clara e simples quando revelarmos tratamento de dados de crianças e adolescentes;

iv) entendemos que precisamos considerar se uma solicitação inclui informação sobre terceiros.

A empresa controladora poderá usar canal especializado ou canal pré-existente (desde que preparado para tanto) para recebimento das solicitações dos direitos dos titulares, que deverá ser amplamente divulgado aos titulares de dados. Importante lembrar que os colaboradores do controlador também devem ter acesso a este canal.

O controlador deverá então verificar a identidade do titular dos dados, para evitar revelar dados pessoais sobre outros titulares. Se for o caso, o Encarregado ou alguém de sua equipe poderá remover menções ou dados de terceiros do documento que contenha dados pessoais do requisitante, para cumprir com o pedido sem expor dados de outros titulares.

Por fim, a depender do volume de requisições que se espera receber (empresas B2C podem esperar número mais elevado que aquelas que somente se relacionam com outras empresas), é recomendável que se use alguma solução para gerenciar as requisições que foram abertas, observando tempo de resposta e tipo de direito que foi requisitado, sendo tais dados, inclusive, utilizados pelo Encarregado para ter melhor panorama do Programa de Privacidade. É possível também utilizar ferramentas tecnológicas de data discovery para identificar rapidamente o local dos dados pessoais relacionados à solicitação do titular, bem como detalhes sobre o consentimento fornecido, quando aplicável.

3) Controle, evidências e armazenamento

Além de cumprir a solicitação do direito do titular em tempo hábil, o controlador deve gerar, ainda, todas as evidências sobre quando e por quem a solicitação foi feita, por meio de qual canal, quem respondeu e em qual prazo, para que possa se resguardar de quaisquer reclamações ou fiscalizações futuras relacionadas ao pedido do titular. É válido lembrar que essas solicitações podem, inclusive, ser feitas dentro de um contexto de relação de consumo, trazendo uma possível inversão do ônus da prova ao controlador, que deverá provar o que foi solicitado, quando e como foi respondido.

Essas evidências podem, ainda, ser requeridas, posteriormente, em ações judiciais, procedimentos perante entidades de defesa dos consumidores, investigações pelo Ministério Público ou fiscalizações pela Autoridade Nacional de Proteção de Dados.

Em resumo:

Para garantir a resposta aos direitos dos titulares, três grandes pilares devem ser observados:

I. Jurídico - Análise se a requisição é válida e se a resposta é correta, sem trazer riscos ao controlador, por exemplo, expor dados corporativos confidenciais;

II. Operacional – Canal para recebimento das requisições, gerando todas as evidências que poderão ser necessárias em momento posterior;

III. Tecnológico - Solução para gestão das requisições abertas, solução para identificação rápida dos dados nos sistemas da empresa e garantia de que os sistemas da empresa estão aptos a "acatar" os pedidos, por exemplo, de exclusão ou bloqueio dos dados.

[1] Disponível em <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>, acesso em 21 de janeiro de 2020.

8. Gestão de terceiros na era da LGPD

8. Gestão de terceiros na era da LGPD

A matriz de responsabilidades da Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018 ou "LGPD") tem como parâmetro a definição da posição de controlador ou operador numa atividade que envolve tratamento de dados pessoais.

De maneira simples e direta, o controlador é aquele que determina as finalidades e os meios pelos quais os dados pessoais serão tratados. Já o operador é aquele que "joga de acordo com as regras do jogo", ou seja, realiza o tratamento conforme as determinações do Controlador, não possuindo poder decisório sobre os meios ou finalidades do tratamento.

Para fins de responsabilidade civil, tanto o controlador quanto o operador são obrigados a reparar um dano causado a outrem em razão de uma atividade de tratamento de dados pessoais que esteja violando a LGPD. No entanto, a LGPD vai além e atribui a responsabilidade solidária para o Controlador, mesmo quando o dano é causado pelo Operador que trata dados pessoais sob suas ordens.

Nesse contexto, a gestão dos fornecedores e dos terceiros que tratem dados pessoais em nome ou para o controlador é essencial para garantir que as práticas de Privacidade e Proteção de Dados destes estejam alinhadas com os riscos que as atividades de tratamento trazem aos titulares dos dados pessoais.

E como fazer essa gestão? Primeiramente, é preciso estabelecer qual o nível de risco que este terceiro traz ao controlador, o que pode ser mensurado observando-se a quantidade de dados que o terceiro tem acesso (trata), o nível de criticidade destas informações (dados sensíveis, dados de crianças etc) e para qual finalidade o tratamento é realizado.

Definindo o risco, pode-se determinar qual o nível de maturidade e controles de Privacidade e Proteção de Dados pessoais será exigido deste terceiro, incluindo o que ele deverá apresentar como evidência destes controles.

Em sendo decidida pela contratação, é preciso refletir no contrato as obrigações desse fornecedor ou parceiro, de modo a garantir que não haverá tratamento contrário aos princípios da LGPD, que não haverá desvio de finalidade ao tratamento que originou a reação contratual, que o operador comunicará ao controlador caso haja qualquer incidente ou tratamento de dados irregular, dentre outras.

Nesse ponto, é válido destacar que os papeis do controlador e operador são dinâmicos, ou seja, uma mesma pessoa poderá assumir a posição de controlador ou operador, a depender da operação realizada. Além disso, é importante sempre se atentar para o fato de que o papel assumido, de controlador ou operador, é inerente à função desempenhada na operação, não podendo ser modificado contratualmente.

Por isso, só contemplar e escrever as cláusulas contratuais não deve ser suficiente. É preciso conhecer a operação e monitorar se o fornecedor ou parceiro, que no caso é operador dos dados pessoais, de fato está respeitando o acordado.

Para ajudá-los, trazemos 03 sugestões que podem ser úteis nesse sentido:

a) Classifique os contratos, considerando aqueles que apresentam maior ou menos risco relacionados à Privacidade e Proteção de Dados;

b) Conheça seus fornecedores, e estruture um cadastro com exigências compatíveis com os riscos dos contratos que eles estão inseridos; e

c) Crie um processo interno, e se possível, use uma ferramenta de gestão, para registrar as comunicações e evidencias solicitadas junto ao operador.

Adotar essas providências não garantirá o afastamento da responsabilidade, mas poderá ajudar a evitar ou mitigar a ocorrência de um dano, e, em última instancia, é um excelente elemento de *accountability*, demonstrando que o controlador se preocupa e acompanha o processamento dos dados pelo operador.

9. Ferramentas e softwares de Privacidade são necessários?

9. Ferramentas e softwares de Privacidade são necessários?

A conformidade com as novas obrigações trazidas pela Lei Geral de Proteção implica uma série de desafios para as organizações. Requisitos como a manutenção de um registro atualizado das atividades de tratamento de dados pessoais, o atendimento aos direitos dos titulares, a gestão do consentimento e a adoção de medidas de segurança são exemplos de fatores cuja operacionalização não somente requer a implementação de um programa de Governança em Privacidade e Proteção de Dados, mas, muitas vezes, poderá acarretar na necessidade de investimento em sistemas e/ou ferramentas tecnológicas especializadas.

Hoje já estão disponíveis no mercado ferramentas próprias para a gestão e operacionalização de processos relacionados à Privacidade, as quais poderão desempenhar um papel fundamental no auxílio às organizações durante a implementação, gestão e manutenção dos seus programas de Privacidade, tendo em vista o seu objetivo principal, que é garantir a conformidade com a legislação.

A IAPP (International Associaton of Privacy Professionals), em relatório divulgado contendo um levantamento das soluções disponíveis para gestão de programas de Privacidade, elencou algumas das principais funcionalidades disponibilizadas por essas ferramentas, entre as quais vale destacar:

- Data Mapping;
- Data Discovery;
- Monitoramento de atividades;
- Gestão e Automatização de Avaliações;
- Gestão de Consentimento;
- Gestão das Respostas a Incidentes; e
- Anonimização/Pseudonimização.

Além dessas funcionalidades, considerando as disposições da LGPD, é possível identificar outros fatores que também poderiam ser operacionalizados com o auxílio de soluções tecnológicas, entre eles a análise de Privacidade desde a concepção dos novos projetos que envolvam dados pessoais (Privacy by Design), elaboração de relatórios de impacto, gestão de terceiros e de riscos envolvidos no tratamento do dados pessoais, por exemplo.

Paralelamente, a eficiência de um programa de Privacidade depende essencialmente do atendimento ao princípio da responsabilização e prestação de contas, por meio da produção de evidências pelas organizações. Tais evidências são mecanismos de accountability e poderão ser produzidas a partir de ferramentas próprias de monitoramento e avaliação da maturidade do programa de Privacidade.

Vale ressaltar que nenhuma ferramenta é efetivamente obrigatória para cumprir os requisitos das leis sobre Privacidade e Proteção de Dados. Entretanto, elas podem ser recursos estratégicos para auxiliar na implementação, monitoramento e gestão dos programas de Privacidade, garantido que o seu funcionamento não somente ocorra de forma mais estratégica, assertiva e eficaz, mas que ele se mantenha dessa forma ao longo do tempo e, assim, permitindo que as organizações estejam mais próximas da tão cobiçada conformidade com a legislação.

10. Data breach: cinco pilares de um plano de resposta a incidentes de segurança em dados pessoais

10. Data breach: cinco pilares de um plano de resposta a incidentes de segurança em dados pessoais

Não é mais novidade que as tecnologias da informação têm provocado profundos debates e alterações no dia a dia de quem atua no contencioso. Os exemplos são incontáveis: um alinhamento feito via mensagens no WhatsApp, alguma contratação por meio da troca de e-mails, o uso de mídias sociais, o desenvolvimento de ferramentas digitais para todos os modelos de negócio, o uso de dispositivos eletrônicos por funcionários, fraudes eletrônicas das mais diversas, direito ao esquecimento, etc.

A Privacidade enquanto direito e verdadeiro marco regulatório, sobretudo com a Lei Geral de Proteção de Dados no País, tem expandido ainda mais essa atuação.

Posturas extrajudiciais ou judiciais ativas e passivas das empresas em relação ao tema têm recebido cada vez mais atenção. Cuidar de carteiras de procedimentos administrativos e processos judiciais é, ao mesmo tempo, desafiador e gratificante. Enfrentar investigações promovidas pelas autoridades brasileiras (Ministério Público, SENACON, etc.), tem sido um ponto cada vez mais sensível de todo modelo de negócio.

A prática tem revelado que o ápice de atenção de toda essa situação é, sem medo de errar, o incidente de segurança em dados pessoais. É o incidente que é noticiado em portais de comunicação especializados. É a partir do incidente que a maioria das pessoas e clientes tem ciência do ocorrido, ingressando com ações judiciais indenizatórias em face das empresas. São também os incidentes que têm demonstrado possíveis falhas de segurança e de organização no trato da questão de Privacidade pelas empresas, justificando o início de investigações pelos órgãos públicos.

Inclusive, como esperado e tem sido visto, o Judiciário brasileiro, mesmo antes da vigência da LGPD, tem protegido os usuários que tenham tido a Privacidade violada de alguma forma. Como exemplo, em Dezembro, se posicionou o STJ que é devida a indenização por danos morais se informações pessoais forem disponibilizadas ou comercializadas sem conhecimento dos consumidores (confira em **https://opiceb.lu/STJ-DecideCadastro**). A tendência é, claramente, a multiplicação cada vez maior do número de ações dos usuários em face das empresas pedindo indenizações em relação ao trato dos dados pessoais.

Nessa realidade, é imprescindível prepararmos as organizações para que não só compreendam essas novas demandas como possam atuar preventiva e reativamente em relação a elas. Claro que o envolvimento de parceiros jurídicos no patrocínio especializado dessas ações faz todo sentido.

Mas faz mais sentido, ainda, desenvolver um plano de resposta a incidentes de segurança em dados pessoais, ou seja, um verdadeiro plano de ação, que fique pronto para start assim que o incidente ocorra, com uma lista consolidada de várias tarefas coordenadas e quem, na organização, serão os responsáveis por executá-las. A ideia é admitir que, infelizmente e em que pesem todas as medidas preventivas técnicas e de Governança adotadas, um incidente pode ocorrer. É fundamental estar pronto e saber como agir diante do episódio.

Inclusive, lembra-se que como a organização se planeja para responder ao incidente e como atua em resposta a um episódio dessa natureza é uma das boas práticas elencadas pela própria LGPD, ao dizer que um programa de Privacidade deve contar com, no mínimo, "planos de resposta a incidentes e remediação" (Art. 50, §2º, I, g, Lei nº 13.709/2018). Além disso, como a resposta ao incidente se deu e o time que a empresa teve de reação, são elementos importantes no estabelecimento da sanção e na sua quantificação: "As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: [...] II - a boa-fé do infrator; [...] VII - a cooperação do infrator; [...] X - a pronta adoção de medidas corretivas.".

É preciso entender, portanto, o que deve constar nesse plano de ação para que ele atenda ao desafio de ser prático, completo, executável e efetivo ao mesmo tempo.

1. Designação prévia de um comitê de crise

O primeiro ponto que deve constar em um plano de resposta é a identificação prévia dos colaboradores que atuarão diante de um incidente e as respectivas funções.

Significa que a organização tem de preparar um comitê de crise que será acionado assim que identificado o incidente? Isso mesmo! Quem irá integrá-lo é uma pergunta própria de cada modelo de estruturação interna, mas a recomendação é que, no mínimo, o Encarregado ou o DPO e colaboradores das áreas jurídica, *Compliance*, TI e comunicação estejam envolvidos.

E mais, também é preciso definir se a organização contará com parceiros externos no apoio desse comitê de crise e quem serão. As áreas técnicas e jurídicas estão estruturadas para atender à situação? Essa é uma pergunta que precisa ser respondida, pois se a conclusão for negativa, é preciso ter a contratação dos parceiros previamente, deixando-os, na medida do possível, em stand by para atuarem imediatamente após o episódio. O prazo de contratação, por exemplo, tem se demonstrado decisivo na contenção da crise.

2. Estruturação prévia das respostas necessárias

O segundo ponto é ter uma cadeia interna de validação (e parceiros jurídicos, como mencionado) de resposta aos titulares de dados pessoais já previamente definida. Como sabido, a LGPD define que os titulares dos dados têm direito à confirmação da existência de tratamento, de acesso aos dados, de informação sobre os compartilhamentos, etc. (art. 18). Além disso, diante do incidente, deve a organização (controlador, especificamente) comunicar ao titular sua ocorrência, se o incidente puder acarretar risco ou dano relevante aos titulares (art. 48, §1º).

Espera-se, assim, que a organização já esteja preparada atender a tais demandas. Porém, um plano de resposta deve constar especificamente mecanismos próprios de resposta ao questionamento dos titulares em relação ao incidente em si. E mais que isso, quem serão os colaboradores e parceiros responsáveis por redigir a resposta e validá-la. Isso deve ser pensado antes!

A mesma ideia se aplica a questionamentos de parceiros comerciais que saibam do ocorrido e estejam preocupados, da imprensa e de colaboradores internos da própria organização. É fundamental que as respostas sejam rápidas e alinhadas a todos os riscos existentes. Quem responderá? Como? O que será apresentado na resposta?

Tudo tem de estar absolutamente estabelecido antes. Já teve casos, por exemplo, em que jornalista consultou a área da comunicação da empresa e, em razão da demora da resposta, a notícia do incidente foi levada a público, gerando problemas reputacionais irrecuperáveis.

3. Comunicação às autoridades competentes

Como terceiro ponto, lembra-se que a LGPD cria um órgão administrativo específico para fiscalização e aplicação das sanções pela violação da Lei, a Agência Nacional de Proteção de Dados – ANPD.

Assim como para os titulares de dados pessoais envolvidos no incidente, a ANPD também deverá ser comunicada em caso de incidente relevante de dados pessoais. A comunicação deve apresentar, pelo menos: "I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV -os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo".

Deve a organização, portanto, estar preparada previamente para fazer tal comunicação de forma mais completa e rápida possível, lembrando que o prazo da comunicação será fatalmente considerado na aplicação das sanções.

Inclusive, a seu critério e considerando a "eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los" (art. 48, §3º), pode a Autoridade realizar a ampla divulgação do fato em meios de comunicação (art. 48, §2º, I), o que pode será muito relevante em termos jurídicos e reputacionais.

Mais que imaginar, é previsível a quantidade imensa de ações judiciais propostas após a informação vir a público. A comunicação correta e rápida à ANPD é absolutamente decisiva.

Além disso, embora se espere que a ANPD esvazie, por lei, a atribuição de fiscalização administrativa, a responsabilidade civil individual ou coletiva ficará a cargo dos titulares atingidos e das entidades legitimadas à adoção das providências judiciais de ordem coletiva. Assim, também é preciso que um plano de resposta preveja quais serão as entidades informadas e qual o teor das informações.

Por fim, se eventualmente, o incidente envolver a prática de algum crime, por exemplo nos casos de ransomware em que há, em termos amplos, o sequestro da base de dados e a exigência de valor em contrapartida para liberação, recomenda-se a apresentação de pedido de instauração de inquérito policial para que a apuração se dê no âmbito da Polícia Judiciária. A proposta do plano de incidente, nesse ponto, é a organização demonstrar que fez tudo que estava ao seu alcance.

4. Identificação, coleta e preservação das evidências

O quarto ponto está associado a também como a organização reagirá em relação ao episódio e como identificará, coletará e preservará as evidências.

Descobrir sua causa (ou tentar no máximo estado da técnica) e fazer prova positiva da investigação realizada são providências muito importantes, não só para traçar um caminho ou rastro positivo de que, de fato, a organização tratou o incidente com a gravidade que possui, como também para minimizar condenações civis e sanções administrativas.

Por exemplo, a identificação/responsabilização do usuário responsável pelo vazamento de dados pessoais ou ao menos a tentativa, por exemplo, tem sido considerado um argumento válido de redução de sanções, demonstrando, na prática, que a organização adotou as providências que estavam ao seu alcance. Mais que a gravidade do incidente em si, é a organização desprezá-lo.

As condenações em dano moral para os titulares são em valor mais alto se a organização não faz absolutamente nada, se comparado aos casos em que, embora o incidente tenha ocorrido, a organização reagiu prontamente, informou o titular e buscou a identificação/responsabilização dos responsáveis.

É necessário, portanto, que a identificação e coleta das evidências necessárias para provar o episódio sejam devidamente adotadas, evitando qualquer espécie de adulteração ou dúvida sobre o procedimento, sob pena de resultar na total invalidade jurídica e consequente inutilidade das provas. Além disso, considerando que evidências dessa natureza são facilmente apagáveis, o time na identificação e coleta é também decisivo.

Recomenda-se que um plano de resposta, portanto, conte com as primeiras providências nesse sentido e com os profissionais internos e de parceiros que serão responsáveis por adotá-las. O plano de resposta deve responder a perguntas como: (i) quem identificou o incidente deve fazer o que e deve encaminhar as evidências para qual área?; (ii) as evidências devem ser preservadas como?; (iii) quem conduzirá os trabalhos de lavratura de atas notariais ou da preservação da prova em blockchain; (iv) quem elaborará um relatório técnico interno circunstanciado do incidente?; (v) o que ele deve apresentar de essencial; (vi) quais os parceiros jurídicos e técnicos externos auxiliarão nas tarefas?

5. Elaboração de relatório final do incidente e revisão dos procedimentos

Ainda, como quinto ponto, um plano de resposta deve indicar um profissional que deverá acompanhar todos os trabalhos realizados diretamente, pode ser o próprio Encarregado ou DPO, ou outro colaborador por ele indicado, e que elabore um relatório devidamente circunstanciado de todas as providências que tiverem sido adotadas.

A ideia é que esse relatório apresente, ao menos: (i) o que aconteceu de fato;(ii) quais providências de preservação das evidências foram adotadas; (iii) quem integrou o comitê de crise responsável pelos trabalhos; (iv) quais foram as funções desempenhadas pelos colaboradores envolvidos; (v) quais os parceiros envolvidos e por quais motivos; (vi) os questionamentos dos titulares, da imprensa e das autoridades recebidos; (vii) as respostas apresentadas; e (viii) quais as medidas de correção técnicas e de Governança adotadas.

Esse relatório é fundamental não só como consolidação das provas positivas de atuação da organização diante o incidente, para todos os fins, sobretudo aqueles dos quais já foi conversado nesse artigo, mas também para que o

episódio fique concretizado e documentado na organização, não se perdendo depois de tratado e que sirva de ponto de partida para a revisão de procedimentos internos e até do próprio plano de resposta aos incidentes. Não raramente, já se verificou casos em que a organização responde ao incidente, mas após o assunto perde força internamente, prejudicando a criação de uma cultura positiva de preservação da Privacidade.

A ideia é também que a cada novo incidente se tenha um relatório, sendo possível para a organização visualizar a evolução dos procedimentos de Governança em dados pessoais a cada novo fato, podendo explorar isso, inclusive de forma gráfica, em sua defesa em fiscalizações e ações judiciais.

Esses são apenas alguns pontos que devem constar no plano de resposta a incidentes que parecem explicar, em si, sua importância. Sua elaboração tem sido desafiadora, mas os resultados que têm sido obtidos são altamente satisfatórios! A Privacidade e o contencioso jurídico conversam cada vez mais!

10. M&A e a importância da due diligence de Proteção de Dados

11. M&A e a importância da due diligence de Proteção de Dados

Com a intensificação das operações de fusões e aquisições na área de tecnologia – em especial, de modelos de negócios em big data envolvendo algoritmos de Inteligência Artificial (IA) e Internet das Coisas (Internet *of Things - IoT*), que fazem uso massivo de dados pessoais –, crescem as preocupações com a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados – "LGPD").

Sem dúvida, a entrada em vigor da LGPD no próximo mês de agosto deverá afetar as operações de fusões e aquisições, na medida em que modelos de negócios *data driven* poderão implicar maiores riscos pós-operação para os compradores, seja no que concerne a modelos de negócios que não estejam devidamente adequados à nova Lei ou mesmo vulneráveis a ataques ou incidentes de segurança e vazamento de dados.

É nesse contexto que cresce a importância da realização de *due diligence* especializada em Proteção de Dados, possibilitando aos investidores dimensionar melhor os riscos da aquisição e o valor da empresa-alvo.[1]

É certo que o nível de maturidade em relação à adequação à LGPD interfere diretamente no valor de mercado das empresas, incluindo as startups. Desse modo, a opção pela não adequação ou pela não adoção de controles de cibersegurança poderá impactar negativamente o valor da operação de aquisição ou, até mesmo, levar à desistência por parte dos investidores, considerando os ricos envolvidos – não apenas de sanções e indenizações, mas principalmente os riscos reputacionais, que tendem a ser consideráveis nesses casos.

Segundo um estudo da Merril Corporation feito com 539 profissionais de M&A, 56% deles afirmam já ter desistido de acordos em função do pouco cuidado empregado nos tratamentos de dados pessoais pela empresa-alvo.

Sendo assim, a realização de *due diligence* em Proteção de Dados, precedendo às operações de fusões e aquisições, permite aos investidores:

- Identificar as contingências, inclusive aquelas ainda não materializadas, relacionadas aos dados e seu tratamento pela empresa-alvo;
- Estimar o impacto das contingências no *valuation* da empresa;

[1] https://www.merrillcorp.com/us/en/insights/reports/due-diligence-2022-m-a-in-the-digital-age.html?tab=emea

- Ter visibilidade acerca do investimento necessário pós-operação societária para adequar a empresa-alvo às normas nacionais e internacionais que tratam de Privacidade e Proteção de Dados;
- Verificar sob quais bases legais os dados são coletados pela empresa-alvo e se estas permitem eventual compartilhamento com a empresa adquirente; e
- Utilizar o relatório de due diligence no processo de integração entre as empresas-alvo e adquirente após o fechamento da operação, de modo a direcionar as medidas necessárias de adequação.

Durante essas averiguações do tratamento dos dados pessoais da empresa-alvo, devem ser analisados todos os aspectos envolvendo o uso de dados pessoais, como quem tem acesso a eles, quais são os controles e políticas de segurança da informação, se os dados poderão ser aproveitados pela empresa compradora, quais os riscos do modelo de negócios, dentre outros aspectos.

Nesse ponto, a exemplo do que acontece na due diligence convencional, todos os documentos da empresa-alvo relacionados ao tratamento de dados e pessoais e segurança da informação deverão ser minunciosamente analisados. Assim, deverão ser examinadas as políticas de Privacidade já elaboradas pela empresa-alvo, os contratos e termos de uso envolvendo tratamento de dados pessoais, certificações e registros de autoria, apólices de seguro que protejam a empresa-alvo contra perda de violação de dados, planos de resposta a incidentes, conteúdo e relatório sobre os treinamentos sobre Privacidade e Proteção de Dados realizados, contratos, processos e documentações de desenvolvimento de software, relatórios de impacto à Proteção de Dados, dentre outros.

Ademais, é muito importante identificar se já houve alguma violação de dados pessoais ou incidente de segurança na empresa-alvo, avaliando como a empresa reagiu, quais os impactos da violação ou incidente para a empresa, colaboradores, fornecedores e clientes, quais medidas foram tomadas para a correção da vulnerabilidade causadora do incidente, dentre outros aspectos relevantes.

Sendo assim, resta evidente que as organizações devem buscar sua conformidade da melhor forma possível e o quanto antes, já que seu nível de adequação à LGPD pode pautar o sucesso das operações de fusão e aquisição. Para os investidores, a realização de *due diligence* especializada em Proteção de Dados é indispensável para identificar os riscos da operação e medidas necessárias para sua mitigação.

FICHA TÉCNICA

Sócios

José Roberto Opice Blum
Renato Opice Blum
Marcos Bruno
Juliana Abrusio
Rony Vainzof
Camilla Jimene
Caio César Lima

Edição

Ana Maria Roncaglia
Lara Silbiger

Arte e diagramação

Heloisa Lago
Lucas Fernandes

Idealização e conteúdo

Marcos Bruno
Rony Vainzof
Caio César Lima
Henrique Fabretti
Tiago Furtado
Maurício Tamer
Nuria López
Paulo Lilla
Pedro Nachbar Sanches
Tiago Campanholi
Ana Maria Roncaglia
Bernardo Fico
Eduardo Curiati
Flávio Fujita
Gabriela Bueno
Fernanda Vilela
Guilherme Sicuto

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

28 DE JANEIRO
DIA INTERNACIONAL DA PROTEÇÃO DE DADOS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

contato@opiceblum.com.br www.opiceblum.com.br

Alameda Joaquim Eugênio de Lima, 680 - 1º andar Jardim Paulista,

São Paulo - SP, 01403001 – (11) 2189-0061