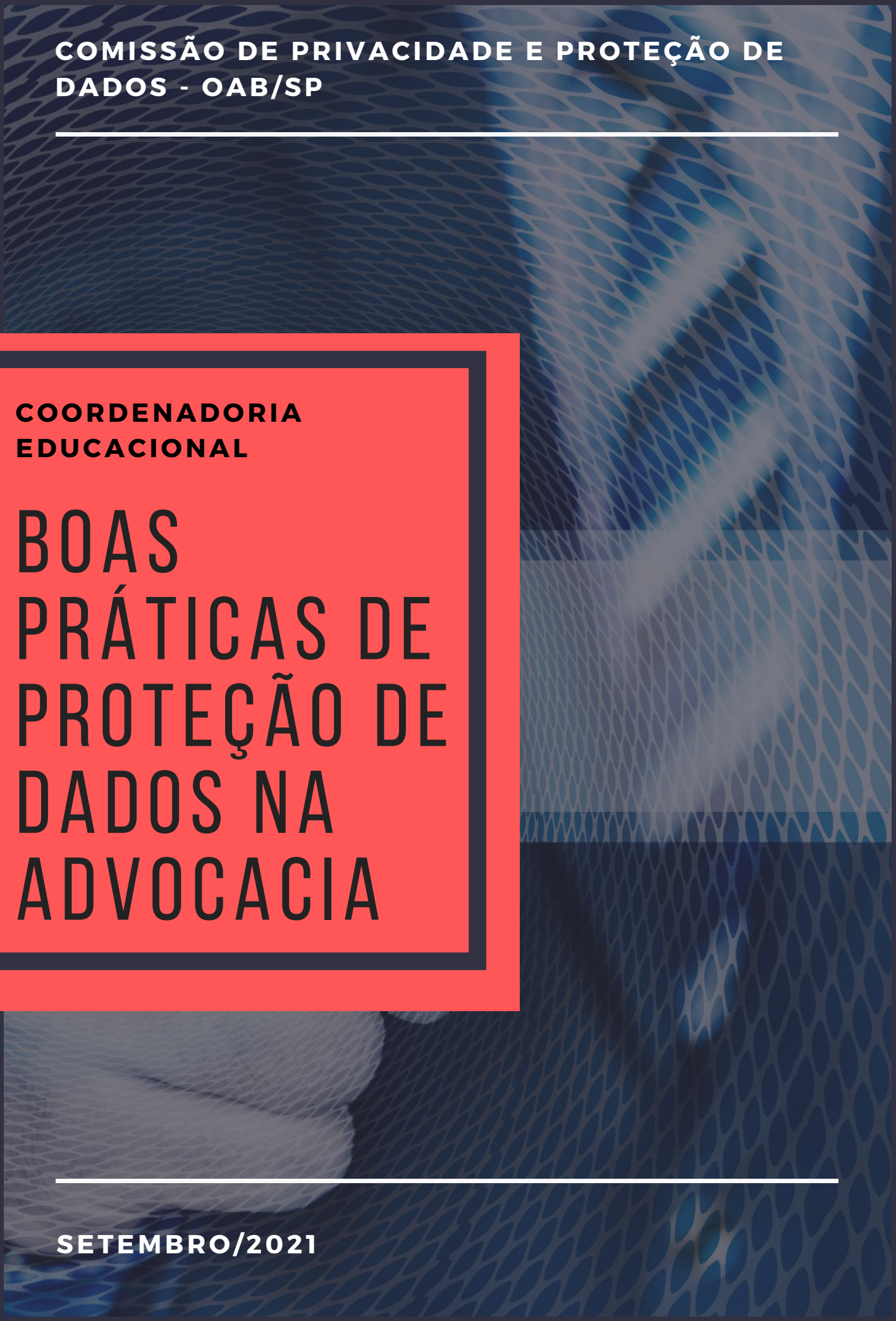

COMISSÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS - OAB/SP

COORDENADORIA EDUCACIONAL

BOAS PRÁTICAS DE PROTEÇÃO DE DADOS NA ADVOCACIA

SETEMBRO/2021

INTRODUÇÃO

Reconhecendo que a segurança e a proteção de dados pessoais no ambiente corporativo dependem de uma estrutura baseada em padrões, diretrizes e práticas existentes para reduzir os riscos cibernéticos e sobretudo pela existência da Lei n. 13.709/2018 (LGPD), com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, a Coordenadoria da Educação da Comissão de Privacidade e Proteção de Dados Pessoais da OAB/SP elaborou esse guia.

Este compilado é baseado em materiais de organizações de referência internacional*, que orientam melhores práticas de gestão da segurança da informação, e observa o capítulo específico que dispõe sobre a segurança e boas práticas (art. 46 ao 51) contido na Lei n. 13.709/2018 (LGPD).

Assim, este guia tem por finalidade estabelecer um protocolo de conduta a ser seguido pelos advogados e sociedade de advogados no que tange a qualquer tipo de operação que envolva o tratamento de dados pessoais.

* Como Instituto Nacional de Padrões e Tecnologia (NIST) e Organização Internacional de Normalização (ISO)/ Comissão Eletrotécnica Internacional (IEC) - ISO/IEC 27002.

A LEI IMPÕE COMO DEVER AOS AGENTES DE TRATAMENTO A ADOÇÃO DE MEDIDAS DE SEGURANÇA, TÉCNICAS E ADMINISTRATIVAS, APTAS A PROTEGER OS DADOS PESSOAIS DE ACESSOS NÃO AUTORIZADOS E DE SITUAÇÕES ACIDENTAIS OU ILÍCITAS DE DESTRUIÇÃO, PERDA, ALTERAÇÃO, COMUNICAÇÃO OU QUALQUER FORMA DE TRATAMENTO INADEQUADO OU ILÍCITO. ALÉM DISSO, ORIENTA A FORMULAR REGRAS DE BOAS PRÁTICAS E A IMPLEMENTAR UM PROGRAMA DE GOVERNANÇA E PRIVACIDADE.

BOAS PRÁTICAS E GOVERNANÇA CORPORATIVA

De acordo com o IBGC, a governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo relacionamentos entre os sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. No contexto de proteção de dados, a governança é um elemento essencial na manutenção de um bom programa de privacidade.

PASSOS PARA PROTEÇÃO DE DADOS PESSOAIS

- Criação de um comitê ou a nomeação de um colaborador que seja responsável pelo acompanhamento das tarefas relacionadas à proteção de dados, como o mapeamento de dados, o contato com os demais colaboradores, a classificação das informações pessoais tratadas, a contratação de provedores de tecnologia e outras;

- O compartilhamento de responsabilidades entre todas as áreas envolvidas, inclusive RH, liderança jurídica e TI;

- A avaliação sobre a maturidade dos processos internos que já existem no escritório em relação à Lei Geral de Proteção de Dados Pessoais;

- A realização de treinamentos com os colaboradores que exercem atividades de tratamento com os dados de clientes, terceiros e dos próprios colaboradores, mesmo que a equipe seja enxuta;

- A atualização das políticas de compliance exercidas pelo escritório.

SIGILO PROFISSIONAL

SIGILO INERENTE À PROFISSÃO, FRUTO DA CONFIANÇA QUE O CLIENTE DEPOSITA EM SEU PATRONO PARA SUA DEFESA, SEJA EM PROCESSO JUDICIAL, SEJA EM QUALQUER OUTRA FORMA DE REPRESENTAÇÃO, DE FORMA QUE ESTE ADVOGADO DEVE AGIR OBSERVANDO ESTA RELAÇÃO DE CONFIANÇA

VS.

PROTEÇÃO DE DADOS

A PROTEÇÃO DE DADOS SE REFERE À PROTEÇÃO DOS DIREITOS FUNDAMENTAIS DA LIBERDADE E DA PRIVACIDADE, ALÉM DO LIVRE DESENVOLVIMENTO DA PERSONALIDADE DA PESSOA NATURAL, CONFORME O ARTIGO 1° DA LGPD.

CICLO DE DADOS PESSOAIS NO EXERCÍCIO DA ADVOCACIA

O art. 3° da Lei Geral de Proteção de Dados Pessoais (LGPD) não deixa dúvidas da extensão dos seus efeitos aos escritórios de advocacia.

Além de seus clientes, os escritórios possuem outros titulares envolvidos em suas atividades, como colaboradores, prestadores de serviços terceirizados, parceiros comerciais, cujos dados pessoais também devem ser tratados em conformidade com LGPD.

Estes cuidados serão considerados ao se averiguar a (des)necessidade de aplicação de sanções pela Autoridade Nacional de Proteção de Dados e por isso devem ser avaliados com cautela.

Algumas sugestões:

1. REGISTRE AS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS

Além de ser uma obrigação legal (art. 37 da LGPD), tal documentação permitirá o pleno conhecimento dos dados tratados, seus titulares e o seu fluxo dentro do escritório.

É PRATICAMENTE IMPOSSÍVEL AFASTAR O TRATAMENTO DE DADOS PESSOAIS DAS ROTINAS JURÍDICAS, POIS AS ATIVIDADES DESENVOLVIDAS NA ADVOCACIA DEPENDEM DO USO DE DADOS PESSOAIS.

2. COLETE E ARMAZENE APENAS AS INFORMAÇÕES NECESSÁRIAS

Elimine todo o excesso de dados desnecessários, diminuindo o risco do tratamento.

3. CRIE UMA POLÍTICA DE PRIVACIDADE ALINHADA COM OS TRATAMENTOS REALIZADOS

Construa sua Política* e implemente medidas técnicas que garantam a proteção dos dados pessoais no ambiente digital e físico do escritório.

4. ADAPTE MINUTAS CONTRATUAIS DEFININDO RESPONSABILIDADES DOS AGENTES DE TRATAMENTO

A lei exige a comprovação da adoção e eficácia de tais medidas.

5. DEFINA QUAL O PAPEL OCUPADO PELO ADVOGADO/SOCIEDADE

Definir em cada um dos contratos firmados se o advogado/sociedade é controlador ou operador dos dados.

6. FIQUE ATENTO AOS CUIDADOS SE ATUAR COMO CONTROLADOR

Caso o advogado ou sociedade atue como controlador é importante evidenciar nos instrumentos contratuais a determinação da finalidade do tratamento, o respeito aos termos da LGPD e à Política de Privacidade de Dados Pessoais adotada, o procedimento para o exercício dos titulares de seus direitos, as medidas técnicas de segurança utilizadas, o dever de confidencialidade e o modo de comunicação em caso de incidentes.

7. ADEQUE SEUS PRESTADORES

Exija a mesma conformidade dos seus prestadores de serviço nas situações envolvendo o compartilhamento de dados pessoais.

8. FORNEÇA TREINAMENTO

Inclua colaboradores e prestadores de serviços ao processo de adequação fornecendo treinamento na lei para que eles possam aplicar estes conhecimentos em seu trabalho.

*A política de Privacidade (*privacy policy*) é um documento interno endereçado aos colaboradores determinando a forma pela qual dados pessoais serão manuseados, armazenados e transmitidos a fim de atender às necessidades organizacionais e cumprir requisitos legais.

PERÍODO DE RETENÇÃO

É necessário determinar uma política de retenção dos dados pessoais, ou seja, o período que os dados permanecerão sob sua guarda até a sua eliminação, devolução ou anonimização. Esta política de retenção de dados pessoais deverá contemplar basicamente **4 itens fundamentais**:

1. Quais são os dados pessoais objeto da retenção, se de clientes (oriundos de processos, consultivo ou potenciais), dados dos colaboradores, advogados e correspondentes;
2. Período de retenção, considerando prazos prescricionais e o prazo de retenção determinado por obrigação legal;
3. Qual será o "termo a quo"; e
4. Qual a fundamentação jurídica de cada retenção.

O período de guarda de dados pessoais - via de regra - irá variar de acordo com o tipo de operação de tratamento realizada e é fundamental que seja apontado de forma clara e precisa ao titular de dados, com vistas ao princípio da transparência.

É IMPORTANTE OBSERVAR, TAMBÉM, O PERÍODO DE RETENÇÃO OBRIGATÓRIA DISPOSTO EM OUTRAS LEGISLAÇÕES E RESOLUÇÕES.

COMPARTILHAMENTO DE DADOS PESSOAIS COM TRIBUNAIS E CORRESPONDENTES

O compartilhamento dos dados pessoais com tribunais e com correspondentes deverá obedecer ao ditame da LGPD com relação ao compartilhamento sem necessidade de consentimento do titular, conforme expressa o art. 7°, incisos II a X, do diploma.

Também se faz necessário que cada tribunal tenha um setor específico para tratamento de dados, um comitê gestor de proteção de dados pessoais, na essência da recomendação do Conselho Nacional de Justiça aprovada na 323ª sessão ordinária.

De acordo com o Guia de Boas Práticas para Implementação na Administração Pública*, na hipótese de tratamento de dados necessário ao exercício regular de direitos do titular em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas, deve-se avaliar:

- O tratamento de dados pessoais se faz necessário para o exercício de direitos do titular em processo judicial, administrativo ou arbitral?
- O titular do dado será informado com destaque quando essa hipótese de tratamento for aplicada?

A resposta para as questões acima deve ser SIM para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD. Além disso, é útil listar todas as organizações com as quais o advogado/sociedade de advocacia compartilha dados regularmente, sendo importante distinguir se operador ou controlador posto que as obrigações diferem.

Isso permite assegurar o controle dos dados que possui e, se solicitado, que reporte aos titulares onde estão e como está sendo realizado o tratamento, garantindo que o advogado/sociedade de advocacia faça uma gestão ativa dos dados pessoais sob sua responsabilidade.

*Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

DIRETRIZES NA SALVAGUARDA DOS DADOS TRATADOS PELO ADVOGADO/SOCIEDADE DE ADVOCACIA

Violações de privacidade e ameaças cibernéticas são um dos maiores desafios enfrentados pela profissão na atualidade. Dentre os princípios que nortearão o tratamento de dados, destaca-se o artigo 6° da LGPD (princípios a serem observados). Assim, priorizar a segurança da rede, sistemas, senhas e dados do escritório e de seus clientes é de extrema importância, sobretudo considerada a responsabilidade na custódia e guarda.

NÃO HÁ NECESSIDADE DE SER UM EXPERT NA ÁREA, MAS É CERTO QUE COMPREENDER NOÇÕES BÁSICAS E RELEVANTES DA TECNOLOGIA PERMITE AO ADVOGADO EXERCER ADEQUADAMENTE SUA ATIVIDADE E DEVE SER CONSIDERADO UM DOS ASPECTOS DE SUA COMPETÊNCIA PROFISSIONAL.

DIRETRIZES

Elencamos abaixo algumas estratégias básicas ao advogado, para não só adequadamente proteger os dados mantidos sob sua custódia por força contratual, mas também implementar a competente representação jurídica.

Mapear e identificar todos os ativos digitais utilizados pelo escritório, advogados e funcionários é o início sugerido. Nesse inventário todas as práticas de TI, bem como a tecnologia usada devem ser detalhadas e listadas, quais sejam:

1) Infraestrutura de Rede;
2) Sistemas e Hardware;
3) Dados e Aplicativos; e
4) Usuários.

A CARTILHA DE INCIDENTES DE SEGURANÇA DA COORDENADORIA DE EDUCAÇÃO DA COMISSÃO ESPECIAL DE PRIVACIDADE E PROTEÇÃO DE DADOS DA OAB/SP TRAZ INFORMAÇÕES VALIOSAS PARA CONSULTA

GESTÃO DOS DADOS PESSOAIS

UMA BOA GESTÃO DE DADOS NECESSITA DA ELABORAÇÃO DE UM PLANO QUE LEVE EM CONTA TODOS OS NÍVEIS DO CICLO DE VIDA DA INFORMAÇÃO

Esse documento deve ser simples, aditável, adequado aos objetivos e infraestrutura do negócio, de fácil implementação e deve responder às seguintes questões:

Fases do ciclo de vida do dado		
Coleta	Os dados pessoais coletados devem obedecer ao princípio da necessidade e finalidade.	• Quais tipos de dados serão coletados ou gerados? • São estes compatíveis e necessários à prestação do serviço? • Qual a origem dos dados e quem são os destinatários? • Qual a finalidade do tratamento? • Os titulares foram informados ou outorgaram seu consentimento quando da coleta?
Processamento	Os dados deverão ser tratados nos termos do art. 7º ou 11 da LGPD (atentando para as particularidades no tratamento dos dados sensíveis).	• Por que o dado pessoal é coletado? • Quais serão as pessoas responsáveis por cada etapa da gestão? • Qual será a política aplicada à cada tipo de dados: financeiros, saúde, etc..? • Como serão descritos os dados (documentação e padrões de metadados)?
Análise	A análise de dados deve levar em consideração a finalidade da coleta, obedecidos os princípios do tratamento, com propósito legítimo, específico e explícito.	• Os dados pessoais são revisados regularmente? • É feito o controle da qualidade dos dados, de modo a assegurar sua exatidão e pertinência?

Compartilhamento	Deve ser consentido pelos titulares, ressalvadas as hipóteses de dispensa de consentimento previstas na LGPD.	• Como serão compartilhados os dados? • Quais os custos e ferramentas necessárias à gestão e ao compartilhamento de dados? • São estas medidas técnicas e organizacionais adaptadas aos riscos e garantias do compartilhamento? Direito de acesso e confidencialidade (minimização)
Armazenamento	Os dados pessoais devem ser armazenados e mantidos por prazos definidos (até que a finalidade seja alcançada ou enquanto pertinentes ao seu alcance.	• Como e onde serão organizados, salvos, armazenados e protegidos os dados? • Quem tem acesso? • Por quanto tempo serão mantidos? • Como serão preservados os dados à longo termo? • Quais as medidas de segurança adotadas na proteção dos dados coletados?
Reutilização	Um novo consentimento deve ser solicitado sempre que houver mudança de finalidade para o tratamento do dado.	
Eliminação	Os dados pessoais devem ser eliminados após o término de seu tratamento.	• Os titulares podem facilmente exercer os seus direitos? • Portabilidade • Direito ao esquecimento.

A **Governança da Informação** não é mais um conceito. Assim, entender e classificar corretamente os dados é um processo importante para estar em conformidade com a lei.

NÃO SE ESQUEÇA DE REVISAR AO LONGO DO TRATAMENTO!

GESTÃO DE DADOS FÍSICOS

Um dado pode ser físico ou eletrônico.

Um dado físico (não eletrônico) é um dado tangível, capaz de ser fisicamente tocado e que detém informação pessoal de um indivíduo. Exemplos disso são, documentos em papel, rascunhos, agendas, cartões de visita e anotações em post-it. O tratamento destes dados também deve seguir os requisitos da lei.

Nunca negligencie dados físicos. É fundamental ter um plano de gestão desses documentos, que garanta o acesso às informações, seu armazenamento e destruição correta. Para isso é necessário saber onde estão e como são processados. Seguem algumas sugestões:

GLOSSÁRIO

- LGPD: Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018);
- Dado Pessoal: toda informação relacionada à pessoa natural que identifique ou possa identificar uma pessoa (titular);
- Dado Sensível: toda informação relacionada à uma pessoa natural que possa gerar caráter discriminatório, como é o caso de informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação à sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico e de crianças e adolescentes;
- Tratamento de Dado: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado: também conhecido como DPO, é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (Autoridade Nacional de Proteção de Dados);
- Agentes de tratamento*: Controlador e Operador;
- ANPD: Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;
- Banco de Dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, de forma eletrônica ou física;
- Anonimização: é uma forma de tratamento de dados com a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais, um dado perde a possibilidade de ser associado, direta ou indiretamente a um indivíduo;

*Acesse aqui o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado publicado pela Autoridade Nacional de Proteção de Dados (ANPD).

GLOSSÁRIO

- Dados Anonimizados: embora originalmente referentes à um titular, por conta de um processo técnico de difícil reversão, não podem mais identificá-lo, ou seja, estão fora do escopo da LGPD;

- Dados Pseudonimizados: são dados tratados de forma a não poderem mais ser atribuídos ao respectivo titular sem que se recorra à outras informações adicionais a ele correlatas. Por possuírem o poder de (re)identificar determinado indivíduo, continuam sujeitos aos ditames da LGPD;

- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

- Relatório de Impacto à Proteção de Dados Pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

COMISSÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS - OAB/SP
COORDENADORIA EDUCACIONAL

Coordenação:
Carolina Chiavaloni

Criação:
Carolina Chiavaloni
Denise Berzin Reupke
Fernanda Natali Queiroz
Jane Karoline Carvalho de Aguiar Ramos
Karina Kaehler Marchesin
Marisol González Martinez
Mariana de Carvalho Rici
Silmara Alves Pinto dos Santos

Revisão de texto:
Silmara Alves Pinto dos Santos

Design:
Ana Carolina Paes de Mello
Camilla D'Agostino
Karina Kaehler Marchesin
Rosalia Toledo Veiga Ometto

Realização:
Comissão de Privacidade e Proteção de Dados OAB/SP

Diretoria Executiva:
Patrícia Peck Pinheiro – Presidente
Marcelo Lapolla – Vice-Presidente
Marcelo Crespo – 1º Secretário
Gabriela De Ávila Machado – 2ª Secretária

SETEMBRO/2021