Manual Orientativo LGPD

DADOS PESSOAIS E CUIDADOS

OMETTO SOCIEDADE INDIVIDUAL DE ADVOCACIA | WWW.OMETTOADVOCACIA.ADV.BR

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

Manual orientativo | Atendimento diretrizes gerais da LGPD | Programa de compliance em privacidade de dados | Padrão interno da Ometto Advocacia | Indicação para clientes | Parceiros de negócios

A OMETTO SOCIEDADE INDIVIDUAL DE ADVOCACIA, sociedade individual de advocacia, inscrita no CNPJ/MF sob nº 03.043.553/0001-10, com sede em Piracicaba, Estado de São Paulo, na Rua Santa Cruz, 883, Bairro Alto, CEP 13401-630, fundada em 1998, sempre com o foco individualizado e diferenciado para seu cliente, preservando princípios da informação adequada e da privacidade dos serviços prestados, entende como relevantes a exposição do presente documento que produzido com o intuito de ser um Manual Orientativo da LGDP, sem a pretensão de esgotar a matéria, para contribuir como um roteiro básico de adequação e revisão de processo para um programa de Compliance em Privacidade de Dados

Tais bases constituem alicerçam Ometto Sociedade Individual de Advocacia, junto com o Aviso de Privacidade de Dados Pessoais são documentos utilizados como padrão interno de atuações, bem como, serve de orientação para clientes e parceiros de negócios, sempre com o objetivo da estar em conformidade com a lei Geral De Proteção De Dados Pessoais (LGPD) e com as melhores práticas no mercado, com foco na privacidade dos dados pessoais dos titulares, que podem ser analisadas no site www.omettoadvocacia.adv.br, e em todas as redes socias,

Em caso de dúvidas adicionais ou requisições, por favor, entre em contato com a Encarregada de Proteção de Dados (DPO), a sócia Rosália Toledo Veiga Ometto, através do e-mail: dpo@omettoadvocacia.adv.br

VER | DICAS LGPD SEM JURIDIQUÊS | OMETTO ADVOCACIA

VER | AVISO DE PRIVACIDADE DE DADOS | OMETTO ADVOCACIA

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

I. OBJETO

1. Documento produzido para atender as normativas da Lei 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD) nos trabalhos e nos serviços prestados pela Ometto Sociedade Individual de Advocacia junto com o Aviso de Privacidade de Dados Pessoais e as Dicas Básicas para Compreender a LGPD, como práticas de atuação interna, bem como, para orientar os trabalhos dos clientes e parceiros de negócio visando as melhores práticas no mercado relativo à Lei Geral de Proteção de Dados Pessoais, com as orientações e diretrizes abaixo dispostas. Sempre destacando que a lei foca no interesse e na privacidade dos dados pessoais dos titulares. Quatro etapas fundamentais para o sucesso de um programa de Conformidade | Compliance | Adequação em Privacidade de Dados são:

- ✓ Compreensão: do que se trata da LGPD e o programa, a partir do negócio específico, da estrutura concreta, como se dará a governança desses dados pessoais, quais adequações jurídicas serão necessárias e, por fim, como ocorrerão as transferências de dados.

- ✓ Avaliação: como se encaixará no plano estratégico, valores da organização e quais a matriz de risco a ser implementada, como será realizado o mapeamento dos dados pessoais, qual a maturidade em privacidade de dados a organização se encontra, qual grau de conscientização e de quanto já está absorvido privacidade nos negócios realizados, quais trilhas a percorrer para adequação à LGPD.

- ✓ Definição: a estratégia a ser seguida pela organização, políticas, modelo de governança de privacidade, o fluxo de dados, quais os impactos à privacidade dos negócios já existentes e os a serem desenvolvidos, método de uso dos dados, acesso do titular de dados aos seus diretos, soluções de proteção de dados que contemple confidencialidade, integridade e disponibilidade, como serão realizadas as medidas de prestação de contas, gestão de terceiros, aplicações em todos os processos do negócio, monitoramento e tratamento de incidentes, processos e ferramentas de conscientização e comunicação com os colaboradores sobre a privacidade de dados pessoais, modelos de relatórios e métricas de trilhas auditáveis.

- ✓ Implementação: a partir dos dados coletados, do mapeamento realizado, das definições do modelo de governança de proteção de dados, priorizar as atividades, orientar um modelo de gestão de riscos específico para os negócios, especialmente com difusão de uma cultura de privacidade de dados pessoais.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

II. COMPREENSÃO | CONSCIENTIZAÇÃO

2. A Ometto Sociedade Individual de Advocacia, seus clientes e parceiros de negócio deverão compreender e conscientizar seus sócios, colaboradores, dirigentes e demais partes interessadas das obrigações decorrentes da Lei Geral de Proteção de Dados Pessoais, visto que a referida lei é obrigatória a toda a qualquer pessoa física ou jurídica que tenha algum proveito econômico e tratem dados pessoais, e quem tem obrigações para com o titular de dados pessoais nos termos da lei. Para tanto, recomenda-se:

- ✓ Elaboração de plano estratégico de treinamento e comunicação, que contemple as necessidades específicas dos negócios envolvidos nos clientes e parceiros de negócio, disseminando a importância da cultura da privacidade de dados pessoais em todos os projetos, procedimentos, processos, e sobretudo, que faça parte dos valores da organização.
- ✓ Promover a cultura da educação continuada de privacidade de dados, realizando treinamentos contínuos internos e/ou externos, com a objetivo de promover interação das partes envolvidas com a temática, bem como, fomentar a conscientização da importância da proteção de dados pessoais e a cultura da privacidade como padrão.
- ✓ Realização de ações efetivas para engajamento das altas lideranças para difundir a cultura e a importância da proteção de dados pessoais ser incorporada à cultura da organização, elevando o padrão de compliance e de reconhecimento público da preocupação e atuação consciente dos cuidados com os dados pessoais dos titulares dos quais trata e de quais obrigações de respostas ao titular de dados pessoais.

III. CONSTITUIÇÃO | ATUAÇÃO COMITÊ LGPD OU DE PRIVACIDADE DE DADOS PESSOAIS

3. Constituição de Comitê LGPD ou Comitê de Privacidade de Dados Pessoais, com regulação em que esteja determinado as principais atuações, atividades e, responsabilidade das tomadas de decisão, e ser o guardião da cultura da privacidade de dados como padrão da organização, nos seguintes termos:

- ✓ Atuar na implementação do Projeto de Compliance em Privacidade de Dados da organização e permanecer no comando do Programa de Compliance em Privacidade de Dados da organização, que deve estar ligado diretamente à alta

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

direção e que deve ser consultado para análise dos riscos de privacidade de dados pessoais em todos os negócios da organização.

- ✓ Promover a conscientização e o envolvimento efetivo dos colaboradores, terceiros e parceiros nos negócios da organização, sobre o tema da privacidade e proteção dos dados pessoais, que a legislação foca a proteção e a privacidade dos dados pessoais, bem como seus direitos.

- ✓ Promover o efetivo conhecimento de todas as áreas sobre os indicadores e etapas vencidas e a evolução do Projeto e posteriormente, do Programa de Privacidade, destacando as principais atividades, ações e documentos elaborados e qual etapa do projeto se encontra a organização.

- ✓ Estabelecer a privacidade por padrão desde a concepção em novos projetos da organização que envolvam o tratamento de dados pessoais, especialmente os de maior risco, propondo reavaliação, restruturação e medidas de segurança, a serem adotadas preliminarmente.

- ✓ Estabelecer e realizar o comando interno do Projeto de Implementação de Compliance em Proteção de Dados Pessoais, atribuindo em grande medida, esforços necessários para adequações, correções e eventuais vulnerabilidades relacionada ao tratamento de dados pessoais, incentivando ajustes necessários para cada área de negócios da organização.

- ✓ Realizar, junto dos parceiros e clientes da organização, atividades e ações conjuntas para a conscientização da necessidade de tratamento de dados pessoais para que todos os agentes de tratamentos de dados pessoais estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais.

- ✓ Como sugestão, na medida e na possibilidade da realidade de cada organização, quer parceira quer cliente, o Comitê LGPD ou Comitê de Privacidade de Dados Pessoais cuja composição deve ter um diretor responsável e técnicos das áreas diretamente envolvidas no processo de implementação e governança da Lei Geral de Proteção de Dados Pessoais, deve ser composto e estruturado da seguinte maneira:

i. Participantes do Comitê LGPD ou de Privacidade de Dados: Encarregado, Diretor Responsável (sponsor), Jurídico, Tecnologia da Informação, Segurança da Informação, Relações Públicas, Comunicação e Marketing, Compliance e/ou Qualidade, Gestão de Riscos, Recursos Humanos e Departamento Pessoal, Gerentes/Gerentes de áreas.

ii. Estabelecer qual a atividade preponderante da organização como agente de tratamento: na maioria dos negócios como Controlador ou Operador para estabelecer prioridades de desenvolvimento de ações do Projeto e depois do Programa de Compliance de Privacidade de Dados Pessoais.

iii. Estabelecer o projeto de inventário (fotografia do estado) ou mapeamento (detalhamento do processo) de dados pessoais na organização.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

iv.	Estabelecer classificações de níveis risco, com matriz de criticidades
v.	Estabelecer responsabilidades no Projeto e depois do Programa de Compliance de Privacidade de Dados Pessoais, dos componentes do Comitê LGPD ou de Privacidade de Dados Pessoais
vi.	Estabelecer diretrizes para instalação do Comitê de Gestão de Crise
vii.	Elaborar um Regimento ou Manual do Comitê LGPD ou de Privacidade de Dados Pessoais e realizar as devidas comunicações internas sobre a evolução dos trabalhos desenvolvidos.

IV. REALIZAÇÃO | AVALIAÇÃO DO INVENTÁRIO OU DO MAPEAMENTO DOS TRATAMENTOS DE DADOS PESSOAIS

4. O mapeamento do tratamento dos dados pessoais de uma organização é uma das obrigações impostas pela Lei Geral de Proteção de Dados, com registro de todas as informações necessárias para avaliação de processo, sendo possível realizar uma trilha auditável dos dados pessoais nos todos os processos de negócios da organização. Para tanto, destaca-se algumas ações necessárias para que os colaboradores, parceiros e clientes tenham conhecimento dos que vão desenvolver a execução do inventário ou do mapeamento do tratamento dos dados pessoais, a saber:

- ✓ Dar conhecimento para colaboradores, clientes, terceiros e parceiros de negócios os fundamentos básicos da Lei Geral de Proteção de Dados Pessoais para que consigam estabelecer minimamente as tarefas necessárias que envolvam o tema da privacidade e proteção dos dados pessoais, que o foco da legislação é a proteção da privacidade dos dados pessoais do titular, pessoa natural (física e viva).
- ✓ Fazer a difusão dos conceitos fundamentais dos elementos envolvidos para a avaliação de processo. Tais como: escopo abrangido pela Lei Geral de Proteção de Dados Pessoais, conceitos de dados pessoais, dados pessoais sensíveis, dados pessoais de crianças e de adolescentes, princípios fundamentais da Lei Geral de Proteção de Dados Pessoais, conceitos de titular de dados pessoais e de agentes de tratamento (Controlador e Operador de Dados Pessoais), figura do Encarregado e suas responsabilidades legais, autoridade reguladora Autoridade Nacional de Proteção de Dados Pessoais (ANPD), sanções administrativas e judiciais decorrentes da não conformidade à legislação possíveis para as organizações.
- ✓ Para ampliar a exemplificação sobre dados pessoais, elenca-se alguns possíveis dados pessoais que não se esgotam nessa listagem, a saber:

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

- Os dados pessoais são dados de pessoas naturais (pessoas físicas, vivas que são os titulares) que identifica o indivíduo ou pode, com a soma de variáveis, levar à identificação da pessoa (art. 5º, I LGPD), nesse contexto, para facilitar a compreensão, pode-se atribuir os seguintes campos facilitadores:

i. Quaisquer tipos de dados que identifiquem direta ou indiretamente uma pessoa natural, mas que não tenha a natureza comportamental, financeira ou sensível, podem ser classificados como dados pessoais simples. Tais como: CPF, CNH, RG, título de eleitor, endereço, gênero, idade, profissão, ID (identidade de usuário em ambientes digitais de um determinado programa), documento profissional (OAB, CREA, CRO, CRM, COREN), estado civil, data de nascimento, filiação, idade, entre outros

ii. Quaisquer tipos de dados pessoais que identifiquem direta ou indiretamente uma pessoa natural com características e informações tratadas com o intuito de monitorar o seu titular, especialmente, para lhe oferecer produtos ou serviços, que precisam da autorização por consentimento ou base legal que deixam de exigir o consentimento do titular podem ser classificados como dados pessoais comportamentais. Tais como: Geolocalização, dados de consumo, preferência, hábitos, endereço IP (Protocolo da Internet, tem como função identificar um computador em uma rede), cookies (arquivos de internet que armazenam temporariamente o que o titular está visitando na rede), logs de conexão (horários do início e fim de cada conexão e o endereço IP do titular), logs de acesso (processo de registro de todos os acessos feitos pelos browsers de visitantes de seu site, que podem ser processadas e gerar estatísticas de acesso ou comprovação de utilização e até de vazamento de dados por aquela via de acesso), entre outros.

iii. Quaisquer tipos de dados pessoais que identifiquem direta ou indiretamente uma pessoa natural com características e informações tratadas com o intuito de monitorar suas atividades financeiras, desde que haja consentimento ou base legal autorizadora da captação, podem ser classificados como dados pessoais financeiros Tais como: dados de conta bancária, número de cartão de crédito e/ou débito, códigos de acesso, senhas para fins financeiros, salário, imposto de renda, benefícios, valor de consultas profissionais, valor de serviços profissionais, token de conta bancária.

- Os dados pessoais sensíveis são quaisquer tipos de dados pessoais que identifiquem direta ou indiretamente uma pessoa natural com características e informações tratadas que tenham o potencial de discriminação, de alto dano ou de risco relevante, de acordo com o rol taxativo da LGPD (art. 5º, II da LGPD), que elenca os seguintes dados vinculados pessoas naturais sobre:

i. Origem racial ou étnica

ii. Convicção religiosa

iii. Opinião política

iv. Filiação a sindicato | organização de caráter religioso, filosófico ou político.

v. Dado referente à saúde ou à vida sexual.

vi. Dado genético ou biométrico.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

- É importante destacar, mesmo não sendo abrangido pela Lei Geral de Proteção de Dados Pessoais, é fundamental para as organizações que os colaboradores tenham ciência de conceitos correlacionados, tais como, segredos negocial, comercial e industrial que são quaisquer tipos de conhecimentos e informações e dados utilizáveis na organização, protegidos pela Lei nº 9.279/96 (Lei da Propriedade Industrial) e não pela LGPD. Tais como: processos de negócios, processos de fabricação, plantas de fábricas, planos de negócios, planos de marketing. Sendo que a divulgação ou exploração indevida desses dados são considerados crimes de concorrência desleal.

- Outro conceito importante para as organizações que estão correlacionados com a Lei Geral de Proteção de Dados Pessoais é o da segurança da informação compreende um conjunto de medidas técnicas, comportamentais e de regras de boas práticas para salvaguardar tanto a proteção de dados pessoais quanto de segredos comerciais, industriais e de negócios. Com uma estrutura de controles adequados, com políticas, processos e procedimentos que incluem mapeamento, controle, treinamentos, níveis de acesso segmentados, monitoramento de sistemas, entre outros

✓ A partir dos conhecimentos dos conceitos básicos da Lei Geral de Proteção de Dados, ao promover a conscientização, facilitar o reconhecimento das categorias e aplicações necessárias para o mapeamento, tais como:

i. Preencher o mapeamento de dados pessoais que permitirá a identificação dentro de cada processo da organização.

ii. Saber classificar e categorizar quem são os titulares de dados pessoais, tais como: colaborador, fornecedor, cliente, consumidor, visitante, paciente, entre outros

iii. Saber qualificar de quem a organização recebe dados pessoais de titulares, qual a fonte dos dados pessoais da organização como um todo e em cada processo (cliente externo ou cliente interno), tais como: direto do titular, de outra área da organização, de terceiros (clientes, parceiros, fornecedores), entre outros.

iv. Conseguir atribuir as finalidades (a que se destina especificamente o tratamento daquele dados pessoais), forma (quais formas de tratamento são realizadas para cada um dos dados pessoais) e duração do tratamento de dados pessoais (estabelecer o prazo final do ciclo de utilização dos dados pessoais armazenados ou como realizará a portabilidade de dados pessoais solicitados pelos titulares que é um de seus direitos, desde que não haja uma base legal impeditiva, que configura uma exceção ao direito do titular).

✓ Saber Identificar a base legal (exceções definidas na LGPD) que justifica o tratamento dos dados pessoais quando Controlador dos dados pessoais ou, na qualidade de Operador, seguir as atribuições de bases legais definidas pelo Controlador.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

	▪ **Bases legais para dados pessoais (art. 7º, II a X da LGPD)**
i.	Cumprimento de obrigação legal ou regulatória do Controlador.
ii.	Dados para políticas públicas pela administração pública, previstas em leis, regulamentos ou contratos.
iii.	Estudo por órgãos de pesquisa
iv.	Execução de contrato ou tratativas preliminares relacionadas a contrato do qual o titular é parte
v.	Exercício regular de direito em processos judicial, administrativo ou arbitral
vi.	Proteção da vida ou da incolumidade física do titular dos dados
vii.	Tutela da saúde, exclusivamente, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária
viii.	Legítimo interesse do controlador ou de terceiros.
ix.	Proteção do crédito.

	▪ **Base legal para dados pessoais sensíveis (art. 11, II da LGPD)**
i.	Cumprimento de obrigação legal ou regulatória do Controlador.
ii.	Dados para políticas públicas pela administração pública, previstas em leis ou regulamentos.
iii.	Estudo por órgãos de pesquisa.
iv.	Exercício regular de direito em processos judicial, administrativo ou arbitral.
v.	Proteção da vida ou da incolumidade física do titular dos dados
vi.	Tutela da saúde, exclusivamente, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária.
vii.	Legítimo interesse do controlador ou de terceiros.
viii.	Garantia de prevenção à fraude e à segurança do titular, nos processos de identificação de cadastro em sistemas eletrônicos.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

- **Base legal para dados pessoais crianças e adolescentes (art. 14 da LGPD):**

i.	Ser realizado no melhor interesse das crianças e de adolescentes
ii.	Consentimento específico e em destaque de um dos pais ou pelo responsável legal para dados pessoais
iii.	Controlador deve dar publicidade sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares
iv.	Não poderão condicionar a participação de titulares em jogos, aplicações de internet ou outras atividades ao fornecimento de informações de um dos pais ou do responsável, além das estritamente necessárias à atividade
v.	As informações sobre o tratamento de dados deverão ser fornecidas de maneira simples, clara e acessível, considerada as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário
vi.	Utilização de recursos audiovisuais quando necessário, de forma a proporcionar a informação necessária aos pais ou ao responsável legal
vii.	Adequada ao entendimento da criança

- ✓ Saber realizar a forma e o registro do documento utilizado para a coleta do Consentimento do Titular, quando for necessário, em cada processo de tratamento de dados pessoais
- ✓ Estabelecer o fluxo do tratamento dos dados pessoais em cada processo da organização, identificando quais dados pessoais estabelecendo a origem desses dados, com quem são compartilhados (quer internamente, quer externamente à organização) e de que forma são compartilhados tais dados pessoais. O compartilhamento pode ocorrer entre áreas ou setores da organização, bem como, com clientes externos (parceiros, clientes, fornecedores, entre outros).
- ✓ Saber identificar e destacar no mapeamento se há compartilhamento de dados pessoais com transferência internacional. Em caso positivo, identificar e registrar em quais países são receptores de tais dados pessoais, para que se estabeleça matriz de risco apropriada a partir do país receptor.
- ✓ Saber identificar e especificar claramente os locais de armazenamento dos dados pessoais, tanto em suportes físicos quanto digitais, para que se possa estabelecer critérios de acesso a tais dados pessoais.
- ✓ Identificar e estabelecer, a partir da tabela de temporalidade do tratamento dos dados pessoais da organização, o ciclo de vida dos dados pessoais tratados na organização.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

- ✓ Saber definir a forma de exclusão dos dados pessoais, quer por eliminação com expurgo seguro e com trilha auditável, quer por portabilidade dos dados com trilha auditável.

5. Antes da implementação, realizar uma análise do estágio de implementação do programa de Compliance em Privacidade de Dados Pessoais, em que se destacam pelo menos duas ações indicadas, revisão do mapeamento de dados pessoais e revisão das áreas mais impactadas:

- ✓ Realizar avaliação e revisão do mapeamento dos dados pessoais com reconhecimento dos pontos mais vulneráveis, estabelecer medidas de mitigação dos riscos detectados nessa fase, estabelecer um plano de ação com indicações de medidas concretas, responsáveis e prazos de conclusão, alinhados ao relatório de impacto à proteção de dados pessoais e monitoramento das metas indicadas.
- ✓ Realizar avaliação e revisão das áreas mais impactadas, como as com maior fluxo de dados pessoais nos processos da organização, sobretudo, quando tratar de dados pessoais sensíveis e estabelecer um controle mais específico e de atenção no monitoramento.

.

V. IMPLEMENTAÇÃO | PROGRAMA DE COMPLIANCE DE PRIVACIDADE DE DADOS PESSOAIS

6. A implementação do Programa de Compliance de Privacidade de Dados Pessoais, deve estar em consonância com o plano estratégicos da organização, a privacidade ser o padrão incorporado pela organização, inclusive como fundamento desde a concepção de novos projetos. Assim, alguns documentos devem ser estabelecidos como parte integrante do Projeto de Implementação e do Programa de Compliance de Privacidade de Dados:

- ✓ Política de Proteção de Dados Pessoais, matriz que deve prever a orientação dos valores da organização, as bases do funcionamento da governança de dados pessoais, integradas com as demais políticas, procedimentos e processos.
- ✓ Política de Ciclo de Vida de Dados Pessoais, com estabelecimento de bases legais aplicáveis aos negócios da organização, bem como, a temporalidade do tratamento dos dados pessoais, estabelecimento do ciclo de vida dos dados pessoais, da coleta até seu expurgo ou portabilidade dos dados pessoais.
- ✓ Política de Segurança da Informação, compreende ações e prevenções para informações como um todo a empresa, quer de dados pessoais quanto de dados do negócio, em qualquer tipo de suporte físico ou digital.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

- ✓ Aviso de Privacidade de Dados Pessoais documento que seja um roteiro para os colaboradores da organização seguirem para entenderem o fluxo de dados pessoais e as diretrizes da organização.

vii.	Quais, como coletar e como tratar dados pessoais de acordo com as regras internas da organização, a partir da base legal de tratamento estabelecida pelo Controlador.
viii.	Como e em quais situações os dados pessoais podem ser transferidos para terceiros ou para outros países.
ix.	Quais, quando e como eles devem ser apresentados aos titulares de dados pessoais e quais os procedimentos para eventuais revisões, conhecimento da utilização, compartilhamento ou até possíveis exclusões ou portabilidade.
x.	Instituir regras internas para a função do Encarregado pelo Tratamento de Dados Pessoais, que mantenham: pré-requisitos mínimos para a função, estabelecimento das atividades, obrigações e responsabilidades.
xi.	Quando e como dados pessoais devem ser descartados, excluídos, em qualquer tipo de suporte, físico ou eletrônico. Estabelecendo regras para o expurgo auditável
xii.	Estabelecer regras específicas para dados pessoais, para dados pessoais sensíveis e para dados de crianças e de adolescentes.
xiii.	Estabelecer regras para como serão direcionadas, tratadas e respondidas requisições de titulares de dados pessoais, tanto na qualidade de Controlador de Dados Pessoais quando for na qualidade de Operador de Dados Pessoais.
xiv.	Estabelecer processo para resposta à comprometimentos e até incidentes de violação de dados pessoais.

- ✓ Instituir regras internas para a função da(o) Encarregada(o) pelo Tratamento de Dados Pessoais, que mantenham: pré-requisitos mínimos para a função, estabelecimento das atividades, obrigações e responsabilidades.

i.	Se a(o) Encarregada(o) for colaboradora interna(o), estabelecer as atribuições e responsabilidades específicas, constantes do contrato de trabalho.
ii.	Se a(o) Encarregada(o) for parceira(o) terceirizada(o), estabelecer as atribuições e responsabilidades específicas em contrato de prestação de serviços.

- ✓ Estabelecer procedimento de classificação de dados pessoais para os processos internos da organização, em todas as áreas de negócios.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

- ✓ Estabelecer procedimentos para coleta e tratamento de dados pessoais, sensíveis e especiais de crianças e adolescentes. A partir do critério fundamental de coleta do mínimo necessário para a realização do processo específico da organização.
- ✓ Estabelecer procedimento para atendimento das requisições e direitos dos titulares de dados pessoais. Quais os canais de acesso, formulários para os canais telefônicos de atendimento ao titular, fluxo de encaminhamentos das requisições dos titulares ao Comitê LGPD ou de Privacidade de Dados Pessoais e à(ao) Encarregada(o) para diligências necessárias para realizar as respostas ao titular no prazo legal.
- ✓ Estabelecer procedimento para elaboração e registro de Relatório de Impacto à Privacidade de Dados Pessoais, de acordo com as especificações legais e com a juntada das evidências realizadas durante todo o Projeto de Implementação e, posterior, Programa de Compliance de Privacidade de Dados.
- ✓ Estabelecer procedimento para transferência de dados pessoais para terceiros, quer como fluxo operacional entre Controladores e Operadores de Dados Pessoais, quer como portabilidade de dados solicitados pelo titular de dados pessoais.
- ✓ Estabelecer procedimento para quando ocorrer a internacionalização dos dados pessoais, proceder a adequada informação ao titular e reconhecer para qual país está sendo tratado os dados pessoais e se estão com padrão de conformidade estabelecidos pela legislação vigente.

- ✓ Estabelecer procedimentos para comprometimento e/ou incidente de dados pessoais contemplando, adequando-se à realidade da organização

  i. Participantes do Comitê de Gestão de Crise de Privacidade de Dados: Encarregado, Diretor Responsável (sponsor), Jurídico, Tecnologia da Informação, Segurança da Informação, Relações Públicas, Comunicação e Marketing, Compliance e/ou Qualidade, Gestão de Riscos, Gerentes de áreas.

  ii. Estabelecer o fluxo de comunicação de violações ou suspeitas de violações de dados pessoais, tais como o Controlador dos Dados Pessoais, os parceiros e terceiros envolvidos e por quais canais de comunicação serão reportados.

  iii. Estabelecer o responsável pela manutenção dos registros de incidentes reportados e quais informações devem estar nos registros.

  iv. Estabelecer classificações de níveis de incidentes, com matriz de criticidade.

  v. Estabelecer como ativar o Comitê de Gestão de Crise de Privacidade de Dados.

  vi. Estabelecer diretrizes de responsáveis pela comunicação interna e externa do incidente.

  vii. Estabelecer diretrizes para notificação dos incidentes para autoridades e/ou titulares de dados pessoais.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

- ✓ Estabelecer processos e ferramentas de conscientização e comunicação com os colaboradores sobre a privacidade de dados pessoais, tais como: questionários rápidos de revisão (quiz), podcast, vídeos internos, vídeos no site, vídeos e *post* para redes sociais da organização (Instagram, LinkedIn, Facebook, Twitter, Tik Tok, entre outros), boletins internos, divulgação de notícias no site e nas redes sociais como conteúdo informativo e educacional, reuniões rápidas, aplicação de técnicas de Visual Law para documentos e políticas da organização.

- ✓ Estabelecer modelos de relatórios com métricas de trilhas auditáveis, tais como: formulários de solicitações, respostas aos titulares, respostas à Autoridade Nacional de Proteção de Dados Pessoais, modelos de informações para redes sociais, modelos de informações para a Imprensa para comunicação de comprometimento de dados, modelos de informações para os titulares e para ANPD sobre incidentes de vazamento e/ou violação de dados pessoais, entre outros.

- ✓ Estabelecer controle das políticas, regras, procedimentos e processos, em especial, dos pontos de maiores riscos da organização. Com a matriz de risco bem definida, a partir do Inventário ou do Mapeamento de Dados, é possível estabelecer prioridade de atuação para conformidade nos pontos de mais risco e adequação aos de maior vulnerabilidade.

VI. REVISÃO PERIÓDICA DOS RISCOS

7. Estabelecer a periodicidade de revisão de riscos de privacidade, que deve ser no mínimo anual, com o objetivo de identificar a variação das métricas auditáveis para que sejam elaborados planos de ação para mitigação específica de pontos encontrados na auditoria interna ou externa.

- ✓ Com o resultado das revisões de riscos de privacidade deve ocorrer adequações de processos e planejamento de atividades, tais como: treinamentos, aprimoramento nas comunicações em todos os níveis da organização e para o público externo (atendendo os princípios da publicidade e da transparência da legislação).

- ✓ Com base nas revisões periódicas de risco realizar adequação dos documentos da organização, em especial, o Relatório de Impacto à Privacidade de Dados Pessoais, sobretudo, quando houver alguma alteração substancial no resultado.

VII. GESTÃO DE TERCEIROS RELACIONADOS COM A ORGANIZAÇÃO

8. Estabelecer na organização, a partir do mapeamento dos dados, de quem a organização recebe os dados pessoais e para quais terceiros compartilha tais dados

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

pessoais. Realizar as adequações contratuais necessárias, especialmente para elencar direitos, atribuir responsabilidade de cada parte, em que categoria de agentes de tratamento cada parte se insere (Controlador e Operador de Dados Pessoais), estabelecer as bases legais para o tratamento dos dados pessoais e quais as garantias de cumprimento às exigências legais, regulatórias e específicas de cada setor de negócios será necessário especificar.

VIII. EVIDÊNCIAS | TRILHAS AUDITÁVEIS | PROVAS DE CONFORMIDADE

9. Estabelecer evidências, trilhas auditáveis e provas de conformidade de todo o Programa de Conformidade | Compliance | Adequação de Privacidade de Dados, com medidas e ações devem ter evidências, que são a comprovação da realização concreta do que a organização efetivamente adotou, que podem servir como elementos de prova para responder a solicitações do titular, da Autoridade Nacional de Proteção de Dados Pessoais, dos órgãos públicos de proteção do consumidor, fazer defesa em processos administrativos, judiciais e de mediação, sobretudo para comprovar as ações e a boa-fé da organização.

✓ Pode-se exemplificar alguns tipos de evidências e comprovações das ações e medidas estabelecidas na trilha auditável e como provas de conformidade e de boa-fé, adequando-se à realidade da organização, entre outros:

i.	Atas de reuniões do Comitê LGPD ou de Privacidade de Dados Pessoais.
ii.	Atas de reunião do Comitê de Gestão de Crise de Privacidade de Dados.
iii.	Relatórios dos monitoramentos de dados pessoais.
iv.	Registros de logs de acesso.
v.	Relatório de Impacto à Proteção de Dados Pessoais.
vi.	Lista de presença de treinamentos internos.
vii.	Certificado de Treinamentos.
viii.	Certificados de Cursos relacionados com a prevenção e privacidade de dados.
ix.	Registro da evolução do Projeto de Implementação de Proteção de Dados Pessoais.
x.	Registro do Programa de Privacidade de Dados Pessoais da organização.
xi.	Registro da qualidade na adequação às normativas relacionadas à privacidade e proteção de dados pessoais.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

IX. TREINAMENTOS | PROGRAMA DE FORMAÇÃO CONTINUADA

10. Estabelecer um programa de treinamentos e de formação continuada da prevenção e da privacidade de dados, visando atender as adequações específicas necessárias para os negócios da organização, com treinamento gerais e específicos periódicos, e outras atuações necessárias, tais como:

i.	Treinamento e integração de novos colaboradores.
ii.	Treinamento e desenvolvimento especial para colaboradores de uma determinada área de negócio.
iii.	Treinamento e desenvolvimento para novos projetos.
iv.	Capacitação específica para gestores.
v.	Elaboração de novas regras e políticas internas adequadas à nova realidade.
vi.	Treinamento e desenvolvimento para adequação de um processo novo com foco na prevenção e na privacidade de dados pessoais, para os gestores, colaboradores, parceiros diretamente envolvidos no processo.
vii.	Fomentar a formação continuada da alta direção e dos sócios para manter a fidelidade à cultura da prevenção e privacidade de dados pessoais como essência da organização.

X. REVISÃO PERIÓDICA DO PROGRAMA | REVISÃO PERIÓDICA DO MANUAL

11. Com a efetiva implementação do Projeto de Conformidade com a LGPD, passará a ser considerado com um programa permanente da organização, definido como Programa de Conformidade | Compliance | Adequação em Privacidade de Dados, em que deve haver revisão periódica anual, ou sempre que necessário, para avaliar a eficácia das medidas até então tomadas com atualizações necessárias com implementação de novas orientações e adequação aos entendimentos estabelecidos pela Autoridade Nacional de Proteção de Dados, para que a adequação seja parte da rotina da organização, adotando as melhores práticas do mercado relacionadas à proteção e à privacidade de dados pessoais.

12. O presente manual deverá ser revisado, no mínimo anualmente, e sempre que houver alteração substancial da legislação pertinente, bem como, das diretrizes regulamentares da Autoridade Nacional de Proteção de Dados Pessoais.

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

XI. AVISO DE PRIVACIDADE DE DADOS | POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

13. Cada organização deverá dispor em seu site e suas redes sociais referência ao Aviso de Privacidade de Dados Pessoais, dependendo do tamanho da organização corresponda aos documentos internos, sobretudo a Política de Proteção de Dados Pessoais, disponíveis para terceiros, em especial, para os titulares de dados pessoais que podem ter melhor compreensão do comprometimento às melhores práticas de compliance e governança de proteção e privacidade de dados que realiza.

XII. CONTATOS

14. Quaisquer esclarecimentos, requisições devem ser enviadas para a Encarregada de Proteção de Dados, Rosália Toledo Veiga Ometto, através do endereço de e-mail: dpo@omettoadvocacia.adv.br, que serão respondidas para as pessoas solicitantes, bem como, para os titulares de dados pessoais possam ter melhor compreensão do comprometimento às melhores práticas de conformidade | compliance | adequação e governança de proteção e privacidade de dados que a OMETTO ADVOCACIA realiza.

Piracicaba, 01 de julho de 2.022.

ROSÁLIA TOLEDO VEIGA OMETTO
OABSP 120.022
OABDF 66.295
-Assinatura Eletrônica-

OMETTO SOCIEDADE INDIVIDUAL DE ADVOCACIA
OABSP 4422/98

Este documento foi assinado digitalmente por Rosalia Toledo Veiga Ometto.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 6676-3241-A130-A467.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal OAB. Para verificar as assinaturas clique no link: https://oab.portaldeassinaturas.com.br/Verificar/6676-3241-A130-A467 ou vá até o site https://oab.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 6676-3241-A130-A467

Hash do Documento

96A282FDDC1B7DD5CD9406187BC910FC47945DE03825A8167A57628E76B7476F

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 04/07/2022 é(são) :

- Rosalia Toledo Veiga Ometto (Advogada) - 139.608.448-75 em 04/07/2022 21:30 UTC-03:00
  Tipo: Certificado Digital