POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

Emissão: 01/07/2015
Revisão: 16/04/2025

Ver.:13.0

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

AUTOR: Juliana Silveira

APROVADORES: Comissão de Proteção de Dados Pessoais

CARGO DOS APROVADORES: Comissão de Proteção de Dados Pessoais

HISTÓRICO DE ALTERAÇÕES:

Versão	Descrição da alteração	Data
1	Caminho do formulário na Intranet	25/11/2019
2	Nomes das Políticas e Documentos	04/03/2020
3	Definição de LGPD e e-mail de acionamento ao DPO	29/06/2021
4	Alteração do item i, nome do comitê de privacidade	29/06/2021
5	Correção de texto no item F de responsabilidades	29/06/2021
6	Item G - Inclusão do link para abertura de incidentes de privacidade no ServiceNow. Item H – Criação.	29/06/2021
7	Item X – Inclusão da política de Uso e Gestão de consentimento e plano de resposta a incidentes de dados pessoais	29/06/2021
8	Alteração do aprovador da política	29/06/2021
9	Inclusão do anexo I	29/06/2021
10	Todas as páginas; Incluída a Comissão de Proteção de Dados e Executivos das áreas de negócio; Atividades de Controle; Políticas e Documentos relacionados; Classificação da informação interna; Abrangência da política; Revisão e aprovação da política pela Comissão de Proteção de Dados	21/06/2022
11	Revisão completa anual e ajustes para incluir objetivos estratégicos; direito do titular; privacy by design; decisão automatizada (IA) e documentos relacionados	09/03/2023
12	Revisão completa anual e ajustes para incluir “objetivos estratégicos” (p.6); inclusão das Políticas de Retenção e Descarte de Dados Pessoais, Privacy by Design e Uso e Gestão de Consentimento no “Item A”; inclusão da área de Governança de Dados e complementação da atuação do CCO, no “Item B”; atualização item H; revisão item 9; retirada do TIN/SSN e inserção de “dados pessoais” e avaliação pela DPO dos riscos e controles compensatórios, na Seção 1; retirada do TIN/SSN e revisão da seção 3; atualização de “controles”, “restrição à transmissão”, retirada do SSN/TIN e inclusão de dados sensíveis na sessão 5; atualização e retirada do SSN/TIN, na Seção 6; inclusão da Política Privacy by Design, Programa de Proteção de Dados Pessoais e Código de Ética e Conduta da Prudential do Brasil, no item 10.	03/04/2024
13	Inclusão do Chief Legal Officer (CLO) e DPO Substituto no tópico “B - FUNÇÕES E RESPONSÁVEIS PELO PROGRAMA DE PRIVACIDADE”; Exclusão da Política HOLD ORDER – Ordem de Extensão de Período de Retenção de Registros e Documentos (POB); Inclusão sobre a Política de Anonimização. Inserção de trechos sobre transferências internacionais de dados e inteligência artificial (IA).	16/04/2025

Emissão: 01/07/2015
Revisão: 16/04/2025

Ver.:13.0

SUMÁRIO:

SÍNTESE

OBJETIVO: Proteger a privacidade e segurança de dados pessoais de acordo com toda a legislação /regulamentação brasileira.

PRINCIPAIS PRINCÍPIOS NORTEADORES DA PROTEÇÃO DE DADOS PESSOAIS

- **BOA-FÉ E TRANSPARÊNCIA**
- **SEGURANÇA E PREVENÇÃO**
- **NÃO DISCRIMINAÇÃO**
- **NECESSIDADE: SOLICITAR SEMPRE O MÍNIMO DE INFORMAÇÕES NECESSÁRIAS**

CONSIDERA-SE "DADO PESSOAL" QUALQUER INFORMAÇÃO RELATIVA A UMA PESSOA NATURAL IDENTIFICADA OU IDENTIFICÁVEL


RG


CPF


CNH


SOCIAL SECURITY NUMBER (SSN)*


TAXPAYER IDENTIFICATION NUMBER (TIN)*


PIS


DADOS BANCÁRIOS

CONSIDERA-SE "DADO PESSOAL SENSÍVEL":

dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado genético ou biométrico, quando vinculado a uma pessoa natural.

CICLO DE VIDA DO DADO

COLETA

Sempre coletar apenas os dados pessoais necessários

Usar métodos de coleta seguros

Documentar motivos da coleta

ACESSO

Conceder acesso aos dados pessoais apenas se necessário para a realização das atividades de cada indivíduo

Não compartilhar nomes de usuário (*logins*) e/ou senhas

USO

Cada "Dono de Processo" deve manter inventário dos locais em que dados pessoais estão armazenados

Todos os registros devem ser mantidos apenas pelo tempo estabelecido pelas políticas da POB

RETENÇÃO

Somente fazer uso dos dados em conformidade com as necessidades ou com as exigências legais/ regulatórias

TRANSMISSÃO

Garantir a proteção de todas as transmissões eletrônicas e do transporte de arquivos físicos

Não enviar dados pessoais, a menos que exista necessidade ou exigência legal/ regulatória

Garantir que as transferências internacionais de dados sejam realizadas em conformidade com exigências legais/regulatórias

DESCARTE

Deve estar em conformidade com as políticas da POB.

Após prazo de retenção, dados pessoais devem ser destruídos ou anonimizados.

QUALQUER VIOLAÇÃO DE DADOS PESSOAIS DEVERÁ SER REPORTADA À POB

Aponte a câmera do seu celular para o QR Code ou clique no nome do canal de comunicação para acessá-lo.

Canal de Integridade e Ética

Portal de Serviços

EXCEÇÕES: ***Qualquer exceção a esta política, a área de Privacy deve ser envolvida para submeter o tema à Comissão de Proteção de Dados Pessoais, DPO e Compliance. O Escritório Global de Privacidade (GPO) pode ser demandado, quando aplicável.***

ABRANGÊNCIA: ***Todas as unidades da POB; Funcionários, Prestadores de Serviços; Parceiros Comerciais; Corretoras Franqueadas; Participantes do Programa de Estudo de Viabilidade de Negócio.***

1. RESUMO

Este documento indica os procedimentos e atividades necessários para assegurar que os controles mínimos aqui estabelecidos sejam implantados e observados de forma consistente na Prudential do Brasil (POB), a fim de proteger os dados envolvendo qualquer informação relacionada à pessoa natural, direta ou indiretamente, identificada ou identificável "Dados Pessoais" sob a guarda da Prudential.

Ainda, nos termos da Lei Geral de Proteção de Dados, qualquer dado pessoal que diga respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico, são considerados “Dados Pessoais Sensíveis”.

2. HISTÓRICO

A Política de Proteção de Dados Pessoais (“Política”) descreve os controles mínimos necessários para proteger a privacidade e segurança tanto de dados pessoais em forma física quanto eletrônica, uma vez que contém as instruções da POB para que suas políticas e padrões que tratem sobre dados pessoais sejam seguidas.

Esta Política observa toda a **legislação/regulamentação brasileira aplicável para o tratamento de dados pessoais**, principalmente, mas não se limitando às disposições da **Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais ou “LGPD”)**. Caso haja divergência entre qualquer aspecto da Política e a legislação/regulamentação brasileira, a legislação/ regulamentação prevalecerá.

Todos os Funcionários, Prestadores de Serviços, Participantes do Programa de Estudo de Viabilidade de Negócio, Parceiros Comerciais, Corretoras Franqueadas, sejam eles pessoas físicas ou jurídicas, com acesso a dados pessoais por meio da POB devem observar a Política.

É possível que alguns países estrangeiros tenham exigências legais mais restritivas ou diferentes a respeito de dados pessoais. Por exemplo, é possível que a transferência de dados pessoais às operações da Prudential em outros países seja proibida sem uma autorização expressa. Adicionalmente, alguns tipos de dados pessoais que não são considerados sensíveis no Brasil podem ser sensíveis em outros países, e uma autorização poderá ser requerida para coletar tais informações. **Todos deverão seguir a legislação/regulamentação de proteção de dados pessoais local e consultar a Área Jurídica e/ou Privacidade da POB para orientações específicas**.

3. RISCOS

A POB coleta, acessa, processa, armazena e transmite dados pessoais na condução dos seus negócios. Dados pessoais devem ser processados e protegidos com controles apropriados a fim de minimizar o risco de perda, acesso não autorizado e mau uso. Incidentes envolvendo a segurança de dados pessoais poderiam resultar, por exemplo, em fraudes, danos aos titulares, bem como em fiscalização, aplicação de penalidades legais ou regulatórias, ações judiciais e, ainda, danos à marca e reputação da POB.

Os controles e procedimentos descritos nesta Política têm como objetivo mitigar esses riscos, dentre outros.

4. BENEFÍCIOS E OBJETIVOS ESTRATÉGICOS

Consolidar os requisitos para proteção de dados pessoais em um único documento, o que proporciona uma abordagem prática para todos os que tenham responsabilidade na proteção de dados pessoais.

Adotar processos e regras que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

Promover a transparência na forma em que a POB trata dados pessoais.

Proporcionar uma maior conscientização e compreensão dos riscos inerentes ao manuseio de dados pessoais, bem como as funções e responsabilidades criadas para salvaguardá-las e o compromisso com melhorias contínuas.

Proteger a companhia, bem como seus colaboradores, clientes, fornecedores e parceiros comerciais, de riscos envolvendo incidentes de segurança com dados pessoais.

Detalhar orientações sobre as atividades de controle requeridas para salvaguardar dados pessoais de forma consistente na Prudential.

Além dos benefícios acima, a Prudential do Brasil possui OBJETIVOS ESTRATÉGICOS de proteção de dados e privacidade os quais pretende atingir em linha com o *Global Privacy Office* (GPO) e alinhados aos objetivos abaixo:

- Aculturamento sobre Proteção de Dados Pessoais e Privacidade, conhecimento e consciência interna da importância do tema para o negócio;
- Governança do tema Proteção de Dados Pessoais e Privacidade, incluindo a constituição de uma Comissão de Proteção de Dados Pessoais;
- Governança sobre ocorrências (eventos, incidentes e violações) envolvendo dados pessoais.

5. ABRANGÊNCIA

Esta Política:

- Abrange todas as unidades da POB, bem como suas franquias, no que lhes for aplicável.
- Se aplica a todos os funcionários, prestadores de serviço, Corretoras Franqueadas e colaboradores que em algum momento possam ter contato com dados pessoais tratados pela, ou em nome da POB, em especial quando:

- A operação de tratamento tenha sido ou almeja ser realizada dentro território nacional Brasileiro;

- A atividade de tratamento objetivar a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados dentro do território nacional Brasileiro;

- Os dados pessoais objetos do tratamento tenham sido coletados dentro do território nacional Brasileiro.

- Suplementa, mas não substitui, as exigências de governança das informações documentadas em outras políticas e padrões. Políticas adicionais podem ser criadas em casos específicos, principalmente se exigido por lei ou regulamento.

- Abrange os dados pessoais sob a guarda da POB.

- Deve ser observada por terceiros com acesso a dados pessoais sob a guarda da POB, sendo certo que estes poderão aderir a esta Política por suas próprias atividades de controle.

- Deve ser observada por Participantes do Programa de Estudo de Viabilidade de Negócio, Parceiros Comerciais, Corretoras Franqueadas e respectivas pessoas que atuam em parceria com estes dois (02) últimos na comercialização dos produtos do grupo Prudential, sejam eles pessoas físicas ou jurídicas, no que se refere ao tratamento de dados pessoais de clientes da POB ou em nome da POB.

FIQUE DE OLHO

Esta política se aplica a todos que em algum momento possam ter contato com dados pessoais tratados pela POB.

6. DEFINIÇÕES

Para o propósito desta Política, considera-se "Dado Pessoal" qualquer informação relativa a uma pessoa natural identificada ou identificável ("Titular"). É considerada identificável uma pessoa natural que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.

SÃO CONSIDERADOS DADOS PESSOAIS:

- As principais categorias de Dados Pessoais tratadas pela Prudential envolvem:
  - Dados de identificação
  - Dados de contato
  - Dados financeiros
  - Dados de saúde*
  - Dados pessoais sensíveis

* Dados de saúde são considerados dados sensíveis, mas merecem especial atenção por serem objeto de regulação específica, como a HIPAA (Health Insurance Portability and Accountability Act) nos EUA.

EXEMPLOS

- **DADOS DE IDENTIFICAÇÃO:** Nome, nacionalidade, CPF, número da carteira de identidade/RG ou outro número de identificação emitido pelo governo ou com validade como forma de identificação reconhecida oficialmente pelo governo endereço, telefone, e-mail, data de nascimento, título de eleitor, estado civil, gênero, filiação, número de registro/matrícula de funcionário ou qualquer outro número de identificação reconhecido oficialmente pelo governo (ex: PIS/PASEP, CTPS, NIS, etc), CNH, placa do veículo, foto, gravação de imagem, nome do representante legal, CPF do representante legal, currículos, número de passaporte.
- **DADOS DE CONTATO:** endereço, e-mail, telefone.
- **DADOS FINANCEIROS:** Números da agência, conta bancária, PIX, número de apólice em conjunto com senhas, código de segurança ou outro dado que permita acesso a contas, informações sobre movimentações financeiras.
- **DADOS PESSOAIS SENSÍVEIS:** origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político , dados de saúde ou à vida sexual , dado genético ou biométrico.
- **DADOS DE SAÚDE:** Atestado de Saúde Ocupacional (ASO), atestados de afastamento, prontuário médico, dados sobre doenças graves, dados sobre vacinação.
- **DADOS DE NAVEGAÇÃO:** IP, geolocalização, histórico da Web.

Os “Dados pessoais” são classificados como informações RESTRITAS. Consulte a Política de Classificação de Informações – anexo 2 - Outros exemplos de classificação de informações.

Os “Dados Pessoais” também abrangem aqueles elementos de dados que possibilitem o acesso de Clientes a uma conta online, especificamente no caso de: nome/ID de usuário ou endereço de e-mail em conjunto com senha ou frase de segurança. As informações de acesso não precisam necessariamente incluir o nome de um indivíduo.

A POB deve fornecer aos Titulares de Dados a habilidade de exercer direitos individuais (**Direito dos Titulares de Dados**) com relação aos seus dados pessoais, que incluem, entre outros, a capacidade de fazer o seguinte:

- Confirmação da existência de tratamento e acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.

Adicionalmente, FATCA é uma lei dos Estados Unidos que busca evitar a evasão fiscal por indivíduos sujeitos à tributação americana. Ela se aplica as instituições financeiras estrangeiras e essas instituições devem identificar e reportar informações desses clientes. O Brasil tem um acordo com os EUA para troca de informações. O CRS, por outro lado, é uma iniciativa da OCDE para combater a evasão fiscal global. Ele exige que países reportem dados sobre patrimônio e rendimentos obtidos fora do país de residência fiscal do cliente. Para tanto, a PoB deve solicitar o Social Security Number (SSN) ou Tax Information Number (TIN) de seus clientes que se encaixam nos casos previstos.

Por fim, com relação as **decisões automatizadas**, que é a existência de operações de tratamento de dados pessoais que envolvam decisões estritamente automatizadas envolvendo **Inteligência Artificial**, tecnologia que habilita ao computador tarefas que tradicionalmente precisam de inteligência humana. A POB entende que o uso dessa tecnologia deve ser feito dentro de padrões éticos e com o compromisso de sempre buscar o melhor para o titular da dados. Cumpre ressaltar que no momento da revisão dessa política, não existia na POB operações de tratamento de dados pessoais que envolviam decisões estritamente automatizadas.

Entretanto, existem processos de negócio que envolvem a utilização de Inteligência Artificial (IA), com o objetivo de fomentar a inovação e aumentar a eficiência da Prudential. Nesses casos, devemos nos guiar pelos **Princípios Éticos para a Inteligência Artificial**. Em suma, os Princípios determinam que o uso de IA deve ser alinhado com os valores da Prudential, sendo sempre transparente, ético, lícito e supervisionado pelo ser humano. Além disso, todas as iniciativas que envolvem IA deverão respeitar a privacidade dos titulares de dados e observar tanto a legislação quanto as políticas da empresa.

DEMAIS DEFINIÇÕES:

LGPD Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709 de 14 de agosto de 2018.

FATCA – Foreign Account Tax Compliance Act.

CRS – Common Reporting Standard.

ACESSO – A capacidade de leitura; inserção; edição ou remoção de dados pessoais.

ANPD (**Autoridade Nacional de Proteção de Dados)** - Autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

ANONIMIZAÇÃO – Processo por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, considerados os meios técnicos razoáveis e disponíveis no momento do tratamento.

ARQUIVAMENTO – Refere-se ao tempo em que a POB armazena todos os seus registros, inclusive dados pessoais, seja na forma física ou eletrônica.

COLETA – É composta pelos vários métodos pelos quais os dados pessoais são recebidos; registrados; transferidos ou digitados nos sistemas e aplicativos, ou de qualquer forma introduzidos dentro do ambiente da POB.

CONTROLADOR(A) – Pessoa a quem competem as decisões sobre o tratamento dos dados pessoais.

DESCARTE – Refere-se aos meios pelos quais a POB remove, apaga, exclui e/ ou destrói dados pessoais de suas instalações, equipamentos, mídias físicas e sistemas/aplicativos.

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO) – Pessoa responsável pela Proteção de Dados Pessoais na Companhia, pela comunicação com a ANPD e com os titulares, bem como demais responsabilidades conforme Resolução CD ANPD Nº 18/2024.

INTELIGÊNCIA ARTIFICIAL – Tecnologia que permite que sistemas de computador realizem tarefas que tradicionalmente exigiam inteligência humana.

OPERADOR(A) – Pessoa que realiza o tratamento de dados pessoais em nome do(a) controlador(a).

SSN Social Security Number – Número de identificação pessoal única nos Estados Unidos.

TITULAR(ES) – Pessoa(s) a quem os dados pessoais se referem.

TRATAMENTO – Qualquer operação efetuada sobre dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

TRANSMISSÃO – Refere-se aos meios pelos quais a POB transfere os dados pessoais entre indivíduos, localizações geográficas, instalações ou sistemas/aplicativos.

TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS – Refere-se à transmissão, compartilhamento ou disponibilização, para país estrangeiro, de dados pessoais.

TIN Tax Information Number – Número único atribuído a cada indivíduo para fins fiscais em alguns países, o TIN de pessoa física é baseado no número de identidade nacional, como o Social Security Number nos Estados Unidos.

USO – Os vários processos de negócio envolvendo o processamento de dados pessoais.

7. PRINCÍPIOS NORTEADORES DA PROTEÇÃO DE DADOS PESSOAIS

A POB cuidará para que todas as atividades de tratamento de dados pessoais estejam em conformidade com os princípios trazidos pela legislação sobre privacidade e proteção de dados. São eles:

- **Princípio da boa-fé:** todas as operações de tratamento deverão ser pautadas em boas intenções, na moral e bons costumes aceitos pela sociedade.

- **Princípio da finalidade e adequação:** O tratamento de dados pessoais deve se limitar aos propósitos legítimos, específicos, explícitos e informados ao Titular, e somente deve ocorrer de formas compatíveis com estas finalidades. Dados pessoais não poderão ser coletados/obtidos para uma finalidade, e depois utilizados para outra. Todos os usos de um dado devem ser compatíveis com o motivo original da coleta/obtenção.

- **Princípio da necessidade:** a coleta e utilização de dados pessoais deverá ser limitada ao mínimo necessário para o cumprimento das finalidades pretendidas e expostas ao titular, garantindo também, que tais informações sejam armazenadas pelo menor tempo possível/necessário.

- **Princípio do livre acesso e qualidade dos dados:** aos titulares deverá ser garantida a consulta facilitada e gratuita quanto a forma e duração do tratamento e integralidade de seus dados pessoais, estando assegurada a exatidão, clareza, relevância e atualização destes.

- **Princípio da transparência:** serão garantidas aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

- **Princípio da segurança e prevenção:** a segurança e confidencialidade dos dados pessoais devem ser garantidas por meio de medidas técnicas e organizacionais, abaixo exemplificadas, a fim de prevenir a ocorrência de incidentes de segurança envolvendo dados pessoais.

- **Princípio da não discriminação:** as atividades de tratamento de dados pessoais jamais poderão objetivar fins discriminatórios, ilícitos ou abusivos.

- **Princípio da responsabilização:** a POB deverá armazenar registros de todas as atividades de tratamento de dados pessoais e as respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e proteção de dados pessoais, comprovando a eficácia e eficiência de tais medidas.

8. GESTÃO E GOVERNANÇA DO PROGRAMA DE PROTEÇÃO DE DADOS PESSOAIS

Programa de Proteção de Dados Pessoais da POB: conjunto de políticas, procedimentos e boas práticas adotadas pela organização.

Para que o referido Programa se mostre efetivo e produza resultados positivos, é importante que os pilares e procedimentos abaixo sejam constantemente observados durante as operações de tratamento de dados pessoais.

A

ESTRUTURA DE POLÍTICAS, NORMAS E PROCEDIMENTOS

A delimitação de regras sobre privacidade e proteção de dados pessoais é disposta por meio dos seguintes instrumentos:

Política de Proteção de Dados Pessoais: Trata-se desta PPDP – Política de Proteção de Dados Pessoais, que estabelece os princípios e fundamentos que deverão nortear os demais instrumentos.

Política de Retenção e Descarte de Dados Pessoais: Tem como objetivo fornecer as diretrizes para os Colaboradores sobre as práticas de retenção e descarte dos Dados Pessoais tratados pela POB, com objetivo de atender às exigências regulatórias da LGPD e definir as formas de encerramento do tratamento dos Dados Pessoais.

Política *Privacy by Design*: Tem como objetivo estabelecer a adoção de boas práticas para garantir o adequado desenho de sistemas e/ou operações de negócio, tato em relação aos produtos quanto aos serviços ofertados pela POB, em conformidade com boas práticas de mercado em proteção de dados pessoais, LGPD e normativos da Autoridade Nacional de Proteção de Dados (ANPD).

Política de Anonimização: Tem como objetivo detalhar a governança de Anonimização que inclui o mapeamento dos dados, as técnicas e regras para a Anonimização nos bancos de dados estruturados, a fim de fornecer as diretrizes para os Colaboradores e Terceiros, em conformidade com as Legislações Aplicáveis para a devida proteção das informações pessoais dos titulares, enquanto mantendo a capacidade analítica dos dados.

Política para Uso e Gestão de Consentimento: Tem como objetivo determinar as regras aplicáveis ao uso do consentimento como base legal para o tratamento de dados pessoais, devendo ser observada por todos os colaboradores que tratarem dados pessoais por meio de consentimento.

Plano de Resposta a Incidentes de Dados Pessoais: Destinado a determinar a forma de atuação da Prudential do Brasil em caso de ocorrências envolvendo dados pessoais (Eventos de Privacidade, Incidentes de Privacidade ou Violação de Privacidade).

Procedimentos de Privacidade (SOPs): Outros procedimentos de Privacidade deverão observar as regras estabelecidas nas Normas de Privacidade e devem ser observados por todos os membros da Companhia (quando aplicável).

Para facilitar o controle de conteúdo, datas de publicação e prazos para revisão, os documentos de governança relacionados à privacidade (incluindo esta Política) devem ser controlados e gerenciados de forma centralizada pelo processo de Gestão de Políticas e Manuais da Prudential, pelo Encarregado de Proteção de Dados e pela área de Privacidade.

B

FUNÇÕES E RESPONSÁVEIS PELO PROGRAMA DE PRIVACIDADE

A gestão e aplicação do programa de privacidade deverá ser conduzida pelos responsáveis abaixo:

- **Escritório Global de Privacidade (GPO)** – Supervisiona o Programa de Privacidade da Prudential em nível global e é o responsável pela Política de Privacidade Global. Define as estratégias e lidera os esforços de todas as operações da Prudential para alcançar os objetivos de curto e longo prazo relacionados à Privacidade durante o ciclo de vida dos dados pessoais. Desenvolve, implementa e mantém políticas de privacidade, treinamentos de conscientização, procedimentos e práticas sobre o tema, além de auxiliar na adequação da Companhia às leis e regulamentações que tratam da questão da privacidade.

- **Comissão de Proteção de Dados** – A Comissão de Proteção de Dados, criada pela Prudential do Brasil, é responsável pela guarda, conformidade e zelo de boas práticas com relação ao tratamento e proteção dos dados. Seu funcionamento, membros e atribuições estão descritos no Regimento Interno da Comissão de Proteção de Dados.

- **Área de Privacidade** – Responsável operacional do programa de privacidade da POB, definido nesta política, conforme direcionamentos estratégicos do (a) Encarregado (a) pela proteção de dados pessoais. A área de privacidade detém o conhecimento necessário das leis, regulamentações e políticas aplicáveis a questões de privacidade, e interage com o Escritório Global de Privacidade (GPO) para esclarecer dúvidas e alertar sobre potenciais lacunas entre as necessidades de negócio e esta Política.

- **Encarregado pelo Tratamento de Dados Pessoais (DPO)** – O Encarregado (Data Protection Officer – DPO), nomeado pela Prudential do Brasil, atua como canal de comunicação entre a companhia, os titulares e a ANPD. Além disso, internamente, o Encarregado lidera as atividades e esforços necessários para o fiel cumprimento das obrigações e boas práticas de Privacidade e Proteção de Dados Pessoais. Para tanto, atua no estabelecimento da estratégia de conformidade e no monitoramento dos pilares do Programa de Privacidade da POB, com o apoio da Área de Privacidade, e participa da Comissão de Proteção de Dados nos termos de seu Regimento Interno.

- **Encarregado pelo Tratamento de Dados Pessoais Substituto (DPO Substituto)** – Assumirá as mesmas responsabilidades e deveres do DPO Titular nas ausências, impedimentos e vacâncias deste.

- **Área Jurídica da POB** – Fornece consultoria e orientação sobre leis e regulamentações sobre privacidade aplicáveis à POB, interagindo com a Área Jurídica da PII, quando necessário, responsável por questões envolvendo Privacy Law. A equipe de Privacy Law da PII poderá fornecer consultoria e orientação em questões legais de privacidade corporativas, multinacionais.

- **Business Information Security Officer (BISO)** – Administra e monitora a aderência da POB ao Programa de Segurança da Informação. Esta função e as correspondentes responsabilidades estão definidas nas Políticas de Segurança da Informação.

- **Governança de Dados -** Responsável pela orquestração dos processos de Governança de Dados que consiste em definição e consolidação do Levantamento, Catalogação, Classificação, Qualidade, Conformidade, Mascaramento e Anonimização realizado pelas equipes de sistemas e áreas negócios, para consolidar as informações dos dados em sistemas da POB.

- **Business Process Owner ("Dono do Processo")** – É o responsável por um determinado processo de negócio onde dados pessoais são utilizados. Os "Donos dos Processos" são apontados pela própria área de negócio no "Inventário de Dados Pessoais".

- **Information Owner ("Dono da Informação")** – É a pessoa responsável por proteger um determinado tipo ou categoria de informação dentro dos sistemas/aplicativos que utiliza, conforme atribuição dada pelos Padrões de Controle de Segurança de Informações (Intranet > Princípios e Processos > Políticas > Segurança da Informação). Os "Donos da Informação" devem estar identificados no "Inventário de Dados Pessoais".

- **Chief Information Officer (CIO)** – É responsável por garantir que os sistemas e aplicativos sejam desenvolvidos em conformidade com as normas da POB e trabalhar em conjunto com o "Dono da Informação" no sentido de garantir que a tecnologia da informação atenda às necessidades da POB. Este papel e as correspondentes responsabilidades estão definidos na Política de Padrões de Controles de Segurança da Informação.

- **Funcionários, Prestadores de Serviços, Participantes do Programa de Estudo de Viabilidade de Negócio, Parceiros Comerciais, Corretoras Franqueadas e respectivas pessoas que atuam em parceria com estes dois (02) últimos na comercialização dos produtos do grupo Prudential, sejam eles pessoas físicas ou jurídicas** – São as pessoas que, tendo acesso a dados pessoais sob a guarda da POB, são responsáveis por zelar pelos dados com a devida diligência e atender a essa política em conformidade com leis e regulatórios aplicáveis.

- **Executivos das áreas de negócio** – são responsáveis por garantir conformidade com a referida Política e Normas da POB relacionadas com a proteção de dados pessoais em suas áreas de negócio. Os executivos das áreas de negócios também são responsáveis por garantir que todos os processos de negócios e ativos envolvendo dados pessoais sejam inventariados e quando aplicável documentado o PIA (Análise de impacto de privacidade) em conjunto com a área de Privacidade e DPO. Os Executivos devem garantir que suas áreas de negócio quando demandados realizem os treinamentos de privacidade e atendam aos processos de inventários de dados pessoais e PIA a fim de estarmos em conformidade com leis e regulatórios aplicáveis.

- **Chief Risk Officer (CRO)** – Oferece suporte aos gestores da POB realizando um programa de gerenciamento de riscos desenhado na medida das necessidades da Companhia.

- **Vendor Governance Officer** – É responsável por manter um inventário atualizado de todos os fornecedores da POB, inclusive aqueles que tenham acesso a dados pessoais. Deve seguir as políticas e diretrizes de Vendor Governance relacionadas à condução de auditorias (due diligence); condições contratuais e monitoramento frequente, além de, em conjunto com a área de Privacidade, realizar uma avaliação da conformidade dos fornecedores com esta Política.

- **Chief Compliance Officer (CCO)** – Mantém uma base de conhecimento relativa a normas e leis sobre privacidade aplicáveis à POB e, ainda, aos requisitos da Prudential, bem como acompanha tendências de mercado e notícias sobre o assunto. Oferece apoio ao treinamento e conscientização de aspectos envolvendo privacidade. Atua como segunda linha de defesa em proteção de dados pessoais e monitora periodicamente os controles previstos no programa global de gerenciamento de riscos de compliance (CRMP).

- **Chief Legal Officer (CLO)** – Suportar com o DPO o programa e o conjunto de políticas de proteção de dados pessoais, bem como objetivos de proteção de dados pessoais na POB; fornecer recursos necessários para estabelecer, implementar, operar, monitorar, manter e melhorar o SGSPI da POB; analisar criticamente em conjunto com o CIO, o sistema de gestão de segurança e privacidade da informação; acompanhar os resultados das avaliações de riscos e compliance, e seu plano de tratamento (se necessário), a fim de garantir níveis de riscos aceitáveis pela estrutura da área de gestão de riscos e controles internos.

- **Records Managements/Gestão Documental** – Responsável por garantir que os requisitos e políticas do Programa de Gestão Documental e TTDD (Tabela sejam implementados e monitorados, em parceria com a Corporate Records Management da Prudential. Responsável por estabelecer controles eficazes e consistentes para manter, preservar, proteger e descartar registros, incluindo aqueles que envolvem Dados Pessoais Identificáveis.

C

INVENTÁRIO DE PROCESSOS DE NEGÓCIO, FORNECEDORES E DE ATIVOS QUE REALIZAM O TRATAMENTO DE DADOS PESSOAIS

A POB manterá registro de seus processos de negócio, fornecedores e ativos que realizam o tratamento de dados pessoais contendo, no mínimo, as seguintes informações:

- **Descrição do fluxo da informação em cada etapa de seu ciclo de vida** (coleta, armazenamento, uso, compartilhamento – e neste caso, a finalidade para transferência – e descarte/anonimização);
- **Base legal** para tratamento;
- **Tipos** de dados pessoais coletados;
- **Finalidades** para os quais os dados são tratados;
- **Local** lógico (nuvem, servidor etc.) e geográfico onde o dado é tratado;
- **Área responsável** pelo processo de negócio ou ativo;
- **Volume** aproximado de titulares.

D

TREINAMENTOS

Os funcionários, prestadores de serviço, Corretoras Franqueadas e colaboradores (quando aplicável) deverão receber treinamentos, especificamente, sobre conceitos gerais de Privacidade e Proteção de Dados Pessoais, incluindo os princípios da LGPD.
Adicionalmente, aborda a importância do sistema de gestão de privacidade da informação (SGPI).

O treinamento referido deverá fazer parte do procedimento de integração dos colaboradores da Companhia (*Onboarding*).

E

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (PIA)

Os relatórios de impacto à proteção de dados pessoais são documentos que contêm a descrição dos processos que envolvem o tratamento de dados pessoais que, por sua natureza, são passíveis de gerar riscos às liberdades civis e individuais dos titulares dos dados pessoais. A elaboração deste documento será exigível em especial quando:

Da realização de operações de tratamento de dados pessoais sensíveis;

Da realização e condução de operações que, por sua natureza, possuam tratamento de dados críticos, passíveis de gerar altos riscos aos titulares de dados pessoais em caso de ocorrência de incidentes envolvendo tais informações; e

A operação de tratamento de dados pessoais estiver amparada na base legal do interesse legítimo.

Em caso de necessidade de elaboração deste documento, deverá ser cadastrado o questionário de avaliação de impacto (PIA) a ser preenchido pela área responsável pela operação.

A POB disponibilizará um modelo específico a ser seguido, o qual, dentre outras coisas, conterá: (i) a descrição dos tipos de dados coletados; (ii) a metodologia utilizada para a coleta e para a garantia da segurança das informações; e (iii) a análise do controlador com relação a medidas salvaguardas e mecanismos de mitigação de risco adotados.

Via de regra, tais documentos não deverão ser publicados ou disponibilizados, contudo, poderão ser objeto de requisição da Autoridade Nacional de Proteção de Dados (ANPD) a qualquer tempo.

F RESPONSABILIDADES

Para que a presente Política produza os efeitos pretendidos, é de grande importância que todos observem as disposições contidas neste documento, levando em consideração que os atos contrários a essa política poderão repercutir para a Companhia como um todo, produzindo efeitos de magnitudes não previsíveis.

Assim, para a garantia do cumprimento das normas de privacidade e proteção de dados pessoais, os pontos a seguir devem ser observados por todos, sem prejuízo dos demais pontos desta política:

Os colaboradores possuem como dever primário o de garantir a integridade, disponibilidade e confidencialidade dos dados pessoais tratados no exercício de sua função;

O tratamento dos dados pessoais deverá, necessariamente, observar as finalidades propostas, não permitido o tratamento incompatível ou excessivo ou para finalidades diversas, sem que haja a expressa autorização da Prudential, a qual previamente validou esta nova finalidade com o titular das informações;

O colaborador deverá se utilizar do mínimo de informações necessárias para o cumprimento das finalidades pretendidas e regular exercício de suas funções;

Os dados pessoais tratados no exercício da função deverão necessariamente ser armazenados em local seguro e oficialmente aprovados pela Prudential, sendo vedado o armazenamento não autorizado em ambientes próprios, como notebooks ou área de trabalho de computadores;

Os dados pessoais tratados no exercício da função, como regra, não poderão ser enviados para endereços de e-mail pessoal ou dispositivos remotos como *pen drives*;

Os dados pessoais tratados no exercício da função não poderão ser apagados, deletados ou anonimizados, sem que haja comando direto da Prudential para tanto.

Violações desta política, por parte dos colaboradores, serão classificadas e avaliadas por Integridade Corporativa de acordo com o nível de relevância, bem como pelo número de ocorrências, que poderão ocasionar a aplicação de medidas disciplinares pelo Comitê de Ética. Para mais informações, consultar Código de Ética e Conduta da Prudential do Brasil.

G INCIDENTES DE DADOS PESSOAIS

Incidentes podem ser definidos como qualquer falha na observância dos pontos descritos nesta política, que podem gerar risco de dano aos titulares de dados pessoais.

A POB MANTERÁ CANAL ABERTO PARA RECEBIMENTO DE INFORMAÇÕES SOBRE INCIDENTES, QUAIS SÃO:

Canal de Integridade e Ética

canaldeintegridade.com.br/prudential/

Portal de Serviços

prudentialdobrasil.service-now.com/pobportal?id=cat_item_itsm&sys_id=bd408e8fdbdc8410e6ab0fbca39619b9

Aponte a câmera do seu celular para o QR Code ou clique no nome do canal de comunicação para acessá-lo

Qualquer pessoa que tenha conhecimento ou suspeita de uma violação de dados pessoais deverá reportar, dentro de 24 horas, a situação com o máximo de detalhes possível. Ao fazer o reporte, devem ser observadas as seguintes orientações:

- Forneça uma descrição clara e concisa do ocorrido, evitando o uso de siglas ou outras abreviaturas que possam não ser de fácil compreensão;
- Inclua quaisquer informações pertinentes relacionadas ao ocorrido;
- Não inclua nenhuma informação pessoal.

A partir do recebimento de eventual Incidente de Dados Pessoais, a POB seguirá com o previsto no Plano de Resposta a Incidentes.

H EXCEÇÃO DA POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

Qualquer exceção considerada como desvio a esta política de proteção de dados pessoais, a área de Privacidade avaliará e submeterá para avaliação da área de Compliance, DPO e Comissão de Proteção de Dados Pessoais.

9. CICLO DE VIDA DO DADO – ORIENTAÇÕES E PROCEDIMENTOS

Em vista do constante advento de novas tecnologias que permitem, de forma cada vez mais ampla, a coleta, retenção, transmissão e descarte de dados pessoais, é importante estar sempre atento às implicações sobre a privacidade de tais dados em relação ao seu ciclo de vida. Essa abordagem é conhecida como *"Privacy by Design"*, um conceito que visa garantir o adequado desenho de sistemas e/ou operações de negócio em conformidade com a governança regulatória e LGPD, ou seja, todo o produto ou serviço deve ser disponibilizado no mercado com as configurações de privacidade no modo mais restrito, por padrão.

É fundamental que seja consultada a Política *Privacy by Design*.

O *Privacy by Design* deve ser realizado de forma antecipada, por meio de medidas proativas, para antecipar e evitar ocorrências de privacidade. Para uma melhor compreensão, abaixo exemplos da implementação do *Privacy by Design* na POB:

- No desenho de um produto novo, parceria de negócio, sistema de informações envolvendo o tratamento de dados pessoais, procure em antecipado a área de Privacidade e o DPO (Data Protection Officer) para a devida avaliação de privacidade.

- Na contratação de um fornecedor ou mudança da prestação de serviços envolvendo dados pessoais, inicie o processo pelo Portal de Serviços - Vendor Governance para a devida avaliação das áreas envolvidas, especialmente diante de fornecedores localizados no exterior ou que realizem transferências internacionais de dados pessoais.

- Em conformidade com os princípios da Transparência, Necessidade e Finalidade, os sites, apps e sistemas publicados na Internet de propriedade da Prudential do Brasil, devem ser implementado com adequado Cookies Banner e Aviso de Privacidade.

Para os fins desta Política, o conceito de *Privacy by Design* preceitua que se deve fazer os seguintes questionamentos para cada fase do Ciclo de Vida do Dado:

Estamos limitando a coleta, acesso e uso dos dados pessoais ao estritamente necessário para (i) atingir-se um objetivo de negócio devidamente documentado e aprovado e/ou (ii) atender/cumprir a uma exigência legal ou regulatória? (iii) foi avaliada a base legal para a coleta desses dados? (iv) caso seja a base legal de consentimento, existe gestão desse consentimento?

Estamos compartilhando dados pessoais com terceiros de forma controlada e apenas quando necessário?

Estamos guardando dados pessoais de acordo com os prazos de retenção estabelecidos? Os registros são descartados de forma segura?

As respostas a essas questões estão traduzidas na forma de controles e atividades durante a coleta; o acesso; o uso; a retenção; a transmissão; e o descarte de dados pessoais. Em qualquer momento do Ciclo de Vida do Dado, todos são responsáveis por assegurar a segurança e confidencialidade dos dados pessoais e que o acesso a tais dados seja restrito, apenas, a pessoas que necessitem das informações para realizar suas atividades.

SEÇÃO 1. COLETA

CONTROLES

Coletar Dados Pessoais apenas quando necessário para atender uma necessidade de negócio documentada e aprovada, ou cumprir uma exigência legal ou regulatória.

Coletar o mínimo necessário de Dados Pessoais para atender uma necessidade de negócio documentada e aprovada ou cumprir uma exigência legal/regulatória.

Usar métodos de coleta seguros para a proteção dos dados pessoais.

1. Atividades de Controle

As seguintes atividades de controle deverão ocorrer em todos os processos de negócio individuais (e não em cada ação individual) que requeiram a coleta de dados pessoais.

1. Limitar a coleta de dados pessoais e documentar os seus motivos

Manter um inventário de dado pessoal coletado em processo de negócio.

Um “Dono do Processo” deve ser nomeado para processo de negócio do inventário, bem como deve haver uma descrição da necessidade de negócio ou exigência legal/ regulatória que tenha gerado a necessidade de coleta do referido dado pessoal.

2. Restringir a coleta de dados pessoais

Antes de coletar informações pessoais médicas ou de saúde, dado genético ou biométrico, quando vinculado a uma pessoa natural, dados bancários e dados de cartão de crédito o “Dono do Processo” deverá:

Documentar opções alternativas e para justificar a necessidade de seu uso.

Envolver a Área de Privacidade e DPO para avaliar os riscos e controles compensatórios;

Ambos, o “Dono do Processo” e a Área de Privacidade/DPO, deverão manter documentadas eventuais aprovações relacionadas.

3. Métodos Seguros de Coleta

É necessário seguir os seguintes passos ao coletar dados pessoais:

Armazenar os documentos em papel em área segura (p.ex.: armário, gaveta ou sala trancada, guarda externa) e longe do alcance visual de pessoas não autorizadas;

Para aquelas áreas ou atividades que tenham um processo de digitalização/ imagem estabelecido, os documentos devem ser escaneados e as versões em forma física destruídas ou enviadas para guarda externa, de acordo com a Política de Descarte de Informações, Políticas de Gestão Documental, Tabela de Temporalidade e Destinação de Documentos (TTDD).

SEÇÃO 2. ACESSO

CONTROLES

Conceder acesso aos dados pessoais (no formato físico ou eletrônico) apenas se necessário para a realização das atividades desempenhadas por cada indivíduo (need-to-know basis);

Restringir o acesso a (i) documentos impressos contendo dados pessoais; (ii) salas de arquivos, (iii) salas de servidores, (iv) impressoras, (v) mídias de backup, (vi) equipamentos de rede e (vii) consoles de servidores, por meio de medidas de segurança física em tempo integral;

Administrar de forma apropriada, conceder e controlar o acesso eletrônico aos dados pessoais. Não compartilhar nomes de usuário (*logins*) e/ou senhas;

Os sistemas/aplicativos desenvolvidos ou adquiridos para uso da POB que contenham dados pessoais devem: (i) Oferecer níveis de segurança que permitam acesso apenas aos usuários autorizados;
(ii) Oferecer métodos seguros para que seja concedido o mínimo de privilégios de acesso aos sistemas para que o usuário execute suas funções (p. ex.: leitura, digitação, criação, deleção); (iii) Fornecer recursos de geração de relatórios, a qualquer momento, sobre usuários autorizados e seus privilégios de acesso.

Atividades de Controle

1. Controles de Processos

Os *Information Owners* ou seus delegados devem aprovar ou negar a concessão de acesso aos dados pessoais a cada indivíduo baseando-se nas necessidades de negócio identificadas, para todos os sistemas pelos quais são responsáveis;

O BISO recertifica os acessos junto aos gestores e *Information owners* para todos os sistemas/ aplicativos que contenham dados pessoais como parte do processo de revisão periódica.

SEÇÃO 3. USO

CONTROLES

Somente fazer uso dos Dados Pessoais em conformidade com as necessidades de negócio documentadas e aprovadas ou com as exigências legais/regulatórias;

CONTROLES

Garantir segurança apropriada aos dados pessoais durante o seu uso e processamento;

Não divulgar dados pessoais na Intranet da POB ou em quaisquer websites externos, tais como, mas não limitados a: webmails, blogs, sites pessoais ou newsgroups;

Dados Pessoais sensíveis: **(a)** Poderá ser usado apenas (i) em processos ou sistemas/aplicativos ou (ii) baixados; impressos ou transmitidos a partir de sistemas homologados pela POB quando o Information Owner tenha documentado o propósito de uso e a Área de Privacidade e DPO tenham aprovado com base na necessidade de negócio ou de exigência legal/regulatória. **(b)** SSN/TIN e cartão de crédito não poderão ser usados como elementos primários ou de rotina para autenticação de usuário e não poderão estar acessíveis ou serem exibidos nos sistemas/aplicativos, relatórios, transmissões de dados ou outros meios sem a aprovação formal por parte da Área de Privacidade, DPO e Segurança da Informação. **(c)** SSN/TIN não poderá ser usado como, ou estar incorporado a (i) números de matrícula de funcionários ou clientes ou (ii) identificadores/autenticadores principais, sem a aprovação documentada da Área de Privacidade e o escritório global de privacidade.

1. Atividades de Controle

1. Restrições de uso de dados pessoais

Novos sistemas/aplicativos e processos de negócio devem ser desenvolvidos com as restrições apropriadas para o uso de dados pessoais. A Área de Privacidade em conjunto com a área interna de negócio deverá:

Manter documentados os sistemas/aplicativos e processos de negócio no inventário de dados pessoais, sempre que necessário;

Avaliar os casos de uso dos dados pessoais tratados na Prudential do Brasil baseado na necessidade de negócio ou legal/regulatória;

Em conjunto com o BISO, implementar soluções técnicas para bloquear a impressão de documentos contendo informações pessoais afim de evitar impressões desassistidas nas impressoras.

2. Restrições ao download de dados pessoais

Os dados pessoais não poderão ser baixados para dispositivos móveis, conforme disposto na Política de Padrões de Controle de Segurança de Informações.

Pedidos de exceção a esta restrição devem ter sua justificativa documentada e submetida à aprovação do BISO, a qual poderá ser revisada pelo ISO (*Enterprise Information Security Officer*), se necessário. As justificativas para a concessão de exceções serão reavaliadas pelo BISO pelo processo de renovação de exceções.

3. Restrições no Ambiente de Testes:

Dados pessoais como nome completo, endereços, telefones, registros de identificação (RH, CPF, CNH, SSN/TIN e outros), dados bancários, dados de cartão de crédito dos titulares e informações pessoais médicas ou de saúde, dado genético ou biometria quando vinculada a pessoa natural, armazenadas ou utilizadas fora do ambiente de produção, deverão ser mascarados ou embaralhados, conforme *Transformation of Test Information/Data Standard* (a área de Segurança da Informação deve ser consultada para maiores detalhes).

4. Uso de dados pessoais em ambientes não-seguros:

Ao realizar atividades em ambientes públicos ou instalações sem os controles de segurança necessários de acordo com as políticas da POB, devem ser tomadas as seguintes precauções (As áreas de Segurança da Informação e Privacidade devem ser consultadas para maiores detalhes):

Apenas levar informações, inclusive dados pessoais, quando autorizado e necessário.

Estar atento aos seus arredores e tomar medidas de segurança adequadas para reduzir o risco de furto, roubo ou perda de dados.

Garantir que o *log off* dos sistemas/aplicações que estiver utilizando seja completamente executado.

Evitar a impressão de dados pessoais, a menos que seja necessário.

5. Novos usos de dados pessoais:

Os dados pessoais não podem ser usados para fins diferentes para os quais foram coletados a menos que haja uma base legal apropriada em conformidade com a LGPD.

Caso esteja envolvido em alguma iniciativa que envolva o uso de inteligência artificial (IA), esteja atento às políticas da companhia, em especial aos Princípios Éticos para Inteligência Artificial. Caso tenha dúvidas sobre a adequação da iniciativa, não deixe de consultar as equipes de Privacidade, Jurídico e Segurança da Informação.

SEÇÃO 4. RETENÇÃO

CONTROLES

Cada "Dono de Processo" deve manter um inventário dos processos, sistemas/aplicativos e outros locais nos quais haja dados pessoais armazenados na POB.

Os registros, incluindo aqueles com dados pessoais, devem ser mantidos apenas pelo tempo estabelecido pelas políticas de Gestão Documentos, e Tabela de Temporalidade e Destinação de Documentos (TTDD).

1. Políticas de Gestão de Documental (Records Management):

A área de Gestão Documental deve assegurar:

A existência de procedimentos devidamente documentados e aprovados para o monitoramento periódico do descarte/anonimização (para os casos aplicáveis) de registros contendo dados pessoais que tenham atingido ou ultrapassado o seu prazo de retenção.

A existência de procedimentos devidamente documentados e aprovados para manter, preservar e proteger informações, inclusive registros que contenham dados pessoais, que a POB seja obrigada a manter com base nos seus prazos de retenção para dar suporte a auditorias, investigações, etc.

SEÇÃO 5. TRANSMISSÃO

CONTROLES

Garantir que todas as transmissões eletrônicas envolvendo dados pessoais estejam devidamente protegidas e que todas as transferências internacionais de dados pessoais cumpram com as exigências legais.

Garantir que arquivos físicos contendo dados pessoais estejam devidamente protegidos durante o transporte.

Garantir que e-mails ou correspondências postais não contenham dados bancários, dados de cartão de crédito dos titulares, informações pessoais médicas ou de saúde, dado genético ou biométrico quando vinculado a uma pessoa natural, a menos que, exista justificativa de negócio aprovada ou exigência legal/regulatória.

Atividades de Controle

1. Restrições à transmissão de dados pessoais sensíveis

Precauções extras devem ser tomadas com o uso de criptografia, MFA (Múltiplo fator de autenticação) e VPN (Virtual Private Network) quando da transmissão de informações pessoais médicas ou de saúde , dados bancários, dados de cartão de crédito, dado genético ou biométrico quando vinculado a uma pessoa natural.

Para a transmissão de arquivos que contenham dados pessoais conforme descrito acima deve ser feito uso de uma solução de transmissão corporativa homologada pela Prudential. (A Área de Segurança da Informação deve ser consultada para mais detalhes).

Cuidados devem ser tomados na manipulação de dados sensíveis, como restringir a quantidade de destinatários e rotular como informação restrita são requeridos.

2. Restrições quanto ao envio de dados pessoais por e-mail

Não enviar dados pessoais por e-mail, a menos que exista uma necessidade de negócio devidamente aprovada ou exigência legal/regulatória.

Usar um serviço de e-mail seguro e aprovado pela POB quando for enviar mensagens que contenham dados pessoais. (A área de Segurança da Informação deve ser consultada para mais detalhes.)

Em caso de necessidade de envio para um serviço de e-mail não considerado seguro, o documento contendo dados pessoais deverá ser enviado seguindo orientações da área de Segurança da Informação.

Verificar se há dados pessoais desnecessários no documento (ex., planilhas com abas, colunas ou linhas ocultas).

Revisar os campos de distribuição do e-mail (Para/To, CC, BCC) para ter certeza de que os destinatários estão corretamente inclusos.

3. Envio de e-mail em massa, personalizado ou correspondência postal

O conteúdo da mensagem está completo e preciso.

Os dados pessoais estão limitados ao mínimo necessário.

Dados pessoais e sensíveis não sejam enviados por e-mail, a não ser que haja justificativa de negócio ou exigência legal/regulatória devidamente aprovada.

A correspondência seja enviada apenas ao destinatário correto.

Adotar um processo automatizado com mecanismos de verificação para assegurar a inserção exata dos documentos aplicáveis conforme justificativa de negócio e registro dos totais enviados.

No caso de uso de envelopes, implantar um processo para garantir que o nome e endereço sejam os únicos elementos de dados pessoais visíveis.

4. Transferências internacionais de dados pessoais

As transferências internacionais de dados pessoais são regulamentadas pela ANPD, exigindo que as empresas tenham fundamentos legais para envio de dados pessoais para fora do território nacional.

As transferências internacionais podem ser realizadas diretamente pela Prudential ou por algum terceiro contratado pela Prudential (ex: caso este armazene dados da Prudential no exterior).

Exemplos mais comuns de transferências internacionais envolvem a contratação de sistemas de *cloud* (armazenamento em nuvem), de gerenciamento de bancos de dados e a contratação de fornecedores localizados no exterior. Sempre que lidarem com transferências internacionais, os Donos do Processo devem:

Garantir que os dados pessoais transferidos estão limitados ao mínimo necessário;

Utilizar meios seguros para transmitir os dados pessoais objeto de transferências internacionais;

Contactar as equipes do Jurídico e Privacidade para que possam avaliar se todos os requisitos legais estão sendo cumpridos;

Conferir se os dados pessoais são enviados para países permitidos pela LGPD e política interna.

SEÇÃO 6. DESCARTE

CONTROLES

O método de descarte ou anonimização (nos casos aplicáveis) de dados pessoais adotado deve estar em conformidade com as políticas de Segurança da Informação e/ou com as políticas de Gestão Documental em vigor (Records Management), Política de Retenção e Descarte de Dados Pessoais e Política de Anonimização, e não devem comprometer a segurança e confidencialidade dos dados pessoais.

Atividades de Controle

O Records Management/Área de Gestão Documental, com o apoio do BISO, deve assegurar que o processo de descarte/destruição de dados, documentos físicos, microfichas/microfilmes e mídias eletrônicas (CD/DVD/Fitas de Backup e outros) seja aplicado também para os registros contendo dados pessoais.

Todo documento em papel contendo dados pessoais que tenha atingido seu prazo de retenção de acordo com a TTDD deve ser destruído usando fragmentadoras *cross-cut*. Consultar a Área de Segurança da Informação para instruções para o descarte, incluindo, de mídias eletrônicas, como CDs e DVDs.

A Política de Retenção e Descarte de Dados Pessoais descreve em que ocasião se adotarão os processos de retenção, descarte ou anonimização, indicando os documentos corporativos que contém os procedimentos detalhados que se aplicarão aos sistemas e processos internos da POB, em estrita conformidade com a Legislação Aplicável e proteção legal do negócio e dos Titulares

A política de Anonimização detalha o processo de mapeamento dos dados, as técnicas e regras para a Anonimização, aplicável a todos os Dados Pessoais armazenados de forma estruturada digitalmente, fornecendo as diretrizes necessárias para os Colaboradores e Terceiros.

10. POLÍTICAS E DOCUMENTOS RELACIONADOS

- Plano de Resposta a Incidentes de Dados Pessoais (POB)
- Política de Segurança para Informações Comerciais e Relacionadas ao Negócio (POB)
- Política de Gestão de Acessos (POB)
- Política de Classificação de Informações (POB)
- Política de Gestão de Documentos
- Política de Programa de Governança de Fornecedores da *Prudential International Insurance*
- Política de Descarte de Informações (POB)
- Política de Retenção e Descarte de Dados Pessoais (POB)
- Política para Uso e Gestão de Consentimento
- Regimento Interno da Comissão de Proteção de Dados
- Política de Padrões de Controles de Segurança da Informação (PII)
- Tabela de Temporalidade e Destinação de Documentos (TTDD)
- *Transformation of Test Information/Data Standard*
- Política do Sistema de Gestão de Segurança e Privacidade da Informação (SGSPI)
- Conformidade com os Requisitos da ISO 27701
- Política *Privacy by Design*
- Programa de Proteção de Dados Pessoais
- Código de Ética e Conduta da Prudential do Brasil
- Política de Anonimização
- Princípios Éticos para Inteligência Artificial

11. DISPOSIÇÕES FINAIS

Sem prejuízo das disposições contidas nesta Política, a POB se reserva ao direito de revisá-la, na periodicidade que melhor entender, sempre respeitando o prazo máximo de 1 (um) ano.