Política de Privacidade e Proteção de dados

Quadro resumo

Código documento:

Processo:
Diretrizes e regras para tratamento de dados pessoais

Última atualização:
14/08/2024

Áreas impactadas:
Todas as áreas da empresa

Objetivo:
Definir como, quando e para quais finalidades a empresa poderá tratar dados pessoais

Resumo:
Documento base sobre proteção de dados na empresa

Sumário:

1. Introdução

Este documento estabelece as diretrizes fundamentais para a governança em privacidade e proteção de dados na FUNDAÇÃO DOM AGUIRRE. Nosso objetivo é comunicar claramente a nossos públicos de interesse (clientes, colaboradores, parceiros e fornecedores) sobre como tratamos essas questões essenciais. Além disso, buscamos reafirmar nosso compromisso com a privacidade e proteção de dados, destacando nossos valores e os processos internos que implementamos para garantir a segurança e a conformidade com as normas vigentes.

1.1. O direito à privacidade

O direito à privacidade assegura aos cidadãos a proteção contra a intervenção de terceiros em sua esfera privada, sendo também conhecido como o "direito de estar só". Trata-se de um direito fundamental, consagrado pela Constituição Federal (art. 5º, inciso X) e pelo Código Civil brasileiro (art. 21). A violação desse direito pode resultar em reparação financeira por danos, e pode manifestar-se de diversas formas, incluindo o uso inadequado de informações pessoais.

1.2. O direito à proteção de dados pessoais

As informações pessoais têm o potencial de afetar diversos direitos dos cidadãos, incluindo a privacidade, a intimidade, a honra e a imagem. Reconhecendo a necessidade de uma proteção específica devido às particularidades e aos impactos desses dados nas relações privadas, o Brasil promulgou a Lei Geral de Proteção de Dados (LGPD) em 2018. Em 2022, a proteção de dados foi oficialmente reconhecida como um direito fundamental, sendo incorporada ao inciso LXXIX do art. 5º da Constituição Federal.

2. Política de Proteção de Dados da FUNDAÇÃO DOM AGUIRRE

A **Política de Proteção de Dados e Privacidade** da FUNDAÇÃO DOM AGUIRRE é um documento formal que visa proporcionar transparência sobre o tratamento de informações pessoais. Este documento detalha quais dados podem ser coletados, os métodos e os momentos em que esses dados serão tratados, bem como as finalidades do processamento. Além disso, a política estabelece diretrizes e padrões rigorosos que adotamos para assegurar a proteção dos dados pessoais, garantindo que todos os indivíduos que interagem conosco possam confiar na segurança e na integridade com que gerenciamos suas informações.

2.1. São objetivos desta política:

1. Garantir a transparência e boa-fé no trato das informações pessoais;

2. Estabelecer diretrizes de conduta e governança para garantir o cumprimento das metas de privacidade definidas pela FUNDAÇÃO DOM AGUIRRE, conforme os princípios e responsabilidades descritos no Capítulo 2.2 desta Política;

3. Orientar as pessoas que integram ou atuam com a FUNDAÇÃO DOM AGUIRRE para a execução de suas atividades de forma uniforme e transparente, promovendo a implementação dessas regras como base para o desenvolvimento da organização, garantindo assim não apenas a manutenção da nossa imagem e reputação no mercado, mas também o nosso compromisso com a privacidade;

4. Conscientizar a respeito das normas, boas práticas e diretrizes sobre proteção de dados pessoais;

5. Capacitar para tratar os dados pessoais com responsabilidade, segurança e confidencialidade;

6. Informar a todos que se relacionam com a FUNDAÇÃO DOM AGUIRRE sobre nosso empenho em garantir a conformidade com a privacidade e proteção de dados pessoais, bem como orientá-los sobre como exercer os direitos previstos na legislação.

2.2. Nossa política se destina a:

Todas as atividades desenvolvidas dentro ou em nome da FUNDAÇÃO DOM AGUIRRE que impliquem em tratamento de dados e informações pessoais, independentemente do tipo de relação mantida entre as partes.

Portanto, essa Política se aplica a você:

- Alunos;
- Parceiros;
- Prestadores de Serviços;
- Representantes;
- Fornecedores e;
- Colaboradores.

Além das regras e orientações desta Política, tais profissionais também estarão sujeitos às **obrigações** e **responsabilidades** específicas, a depender do volume e categorias de dados aos quais têm acesso e trata, quando estabelecidas em:

- Contratos;
- Convênios;
- Termos;
- Manuais;
- Acordos de Compartilhamento;
- Procedimentos;
- Regulamentos;
- Regimentos;
- Treinamentos.

2.3. Nossa Visão de Privacidade e Proteção de Dados

A FUNDAÇÃO DOM AGUIRRE preza pelo ambiente acadêmico seguro e respeitoso, onde a privacidade e a proteção de dados pessoais são prioridades fundamentais. Comprometemo-nos a tratar todas as informações pessoais com o mais alto nível de confidencialidade e integridade, em conformidade com as leis e regulamentos aplicáveis.

Esta Política visa:

- **Garantir a Transparência**: Assegurar que nossos alunos, funcionários, pesquisadores e parceiros estejam plenamente informados sobre como suas informações pessoais são coletadas, usadas e protegidas, promovendo a transparência em nossos processos de gestão de dados.

- **Proteger Dados Pessoais**: Implementar e manter medidas de segurança robustas para proteger os dados pessoais contra acesso não autorizado, perda, divulgação e outros riscos. Investir em tecnologias e práticas atualizadas para manter a segurança da informação.

- **Respeitar os Direitos dos Indivíduos**: Facilitar o acesso, correção e exclusão de dados pessoais conforme solicitado pelos indivíduos e conforme previsto pela legislação. Garantir que os direitos de privacidade das partes interessadas sejam respeitados e atendidos.

- **Promover a Conformidade**: Cumprir rigorosamente todas as leis e regulamentos de proteção de dados aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD) e outras normas pertinentes. Implementar políticas e treinamentos contínuos para assegurar a conformidade em todas as áreas da Fundação.

- **Fomentar a Cultura de Privacidade**: Educar e conscientizar nossa comunidade acadêmica sobre a importância da privacidade e proteção de dados. Promover uma cultura de responsabilidade e respeito em relação ao tratamento de informações pessoais.

Na FUNDAÇÃO DOM AGUIRRE, estamos comprometidos em manter a confiança que nossos alunos, funcionários e parceiros depositam em nós, garantindo que a privacidade e a proteção de dados pessoais sejam sempre uma prioridade em nossas operações diárias.

2.4. Compromissos que assumimos e que você deve cumprir

Estamos empenhados em buscar sempre a conformidade com a proteção de dados pessoais e garantir a privacidade de todos que se relacionam conosco. Para tanto, no âmbito da FUNDAÇÃO DOM AGUIRRE, é obrigatório a todos os representantes, colaboradores e prestadores de serviços:

1. Cumprir as disposições legais aplicáveis à proteção de dados pessoais e privacidade, tendo como norma principal a Constituição Federal do Brasil e, em sequência, a Lei Geral de Proteção de Dados (LGPD).

2. Cumprir as regras estabelecidas nesta Política e demais regras internas aplicáveis à proteção de dados pessoais, tais como, exemplificativamente, a Política de Segurança da informação (PSI), Política de Descarte, Código de Conduta, Termos de Usos e Avisos de Privacidade;

3. Fomentar, permanentemente, a plena observância dos termos desta **Política de Proteção de Dados e Privacidade**, por meio de Planos de Treinamentos e Conscientização periódicos sobre o tratamento de dados pessoais, bem como orientações, materiais e recomendações visando ao fortalecimento da compreensão e aplicação das diretrizes aqui estabelecidas.

4. Implementar os melhores padrões de segurança da informação para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais, com base nas boas práticas internacionais e, sempre que possível, nas diretrizes das normas técnicas da ABNT ISO/IEC 27000, 27001, 27002 e 27701;

5. **Limitar** o uso, retenção, divulgação e transferência de dados pessoais ao **necessário para cumprir com objetivos específicos, explícitos e legítimos**;

6. **Zelar pela origem e qualidade dos dados**, além da prevenção da ocorrência de incidentes de segurança decorrentes do tratamento desses dados;

7 Implementar, antes de iniciar qualquer novo desenvolvimento que envolva o tratamento de dados pessoais, é essencial adotar os princípios de 'Privacy by Design' (privacidade desde a concepção) e 'Privacy by Default' (privacidade por padrão). Isso significa que, desde a fase de planejamento, devem ser integradas medidas de proteção de dados pessoais, e que as configurações padrão devem garantir a máxima proteção da privacidade dos indivíduos.

8 **Minimizar a coleta de dados pessoais**, restringindo-os àqueles estritamente necessários para a finalidade previamente informada ao titular de dados, sem prejuízo da eficiência de nossas atividades;

9 **Conservar os dados apenas durante o período necessário para a execução das finalidades informadas**, salvo quando existir uma disposição legal em contrário, uma ordem da Autoridade Nacional de Proteção de Dados (ANPD) ou Judicial.

10 **Eliminar, após o término do tratamento**, os dados utilizados com a garantia do emprego das melhores técnicas de segurança da informação;

11 Durante todo o processo de tratamento de dados, garantir o pleno exercício dos direitos estabelecidos pela lei aos titulares de dados pessoais;

12 Garantir a manutenção da conformidade com as regras de proteção de dados, por meio de:

a) Atualização permanente desta Política e demais normas aplicáveis à proteção de dados no ambiente da empresa;
b) Atualização anual das análises de conformidade dos processos de tratamento de dados e sua adequação à legislação. Isso inclui garantir uma gestão eficiente do consentimento fornecido pelo titular para o tratamento de dados autorizado por ele, conforme a lei, e, na ausência desse consentimento, considerar a aplicação de outra base legal apropriada;
c) Atualização, ao menos uma vez ao ano, das verificações de vulnerabilidades de tecnologia e segurança da informação;
d) Correção de quaisquer não conformidades ou vulnerabilidades decorrentes das atividades descritas nos itens anteriores;
e) Elaboração de planejamento e orçamento anual para as ações necessárias para garantia da manutenção da conformidade com a lei;

f) Obrigatoriedade da elaboração do Relatório de Impacto à Proteção de Dados (RIPD), anteriormente ao desenvolvimento de novas atividades que impliquem em tratamento considerado de risco;

g) Exigência de elaboração da Avaliação de Legítimo Interesse (LIA) antes do início de novas atividades baseadas na hipótese legal do legítimo interesse, conforme o artigo 7º, inciso IX da LGPD;

h) Revisão anual dos bancos de dados mantidos pela FUNDAÇÃO DOM AGUIRRE e descarte de acordo com as regras estabelecidas de Descarte e nas normas técnicas internacionalmente reconhecidas;

i) Oferta de treinamento contínuo, durante toda a jornada do colaborador e prestador de serviços na FUNDAÇÃO DOM AGUIRRE sobre a proteção de dados, as regras de segurança, a gestão de processos e o tratamento de incidentes de segurança;

j) Revisão e atualização permanente do grau de maturidade dos nossos parceiros comerciais com a LGPD;

k) Aperfeiçoamento contínuo dos integrantes do Comitê de Proteção de Dados;

l) Revisão anual dos processos de *Privacy by design* (privacidade por concepção), sua aplicabilidade, eficiência e possibilidades de aperfeiçoamento;

m) Revisão anual dos processos de *Privacy by default* (privacidade por padrão), sua aplicabilidade, eficiência e possibilidades de aperfeiçoamento;

n) Criação do banco de evidências dos processos de tratamentos de dados;

o) Registro permanente de acesso a bancos de dados, sistemas e quaisquer meios digitais disponíveis, visando o combate a acessos indevidos, bem como instrumentalizar meios de defesa e exercício de direitos;

p) Registro permanente de acesso ao perímetro onde arquivados documentos e informações em suportes físicos, visando o combate a acessos indevidos, bem como instrumentalizar meios de defesa e exercício de direitos.

3. Governança em Privacidade e Proteção de Dados

A governança é o conjunto de decisões e responsabilidades explícitas e implícitas de uma instituição para com seus colaboradores, clientes, parceiros e à sociedade.

A Lei Geral de Proteção de Dados traz uma seção específica referente às regras de boas práticas e de governança que devem ser observadas pelos envolvidos no tratamento de dados, estabelecendo no inciso I, § 2º do art. 50, que "o controlador poderá implementar programa de governança em privacidade".

3.1. Objetivo

A proteção de dados pessoais deve ser abordada como um programa de *compliance* dinâmico, que requer atenção constante de todas as áreas da organização.

Nosso programa de governança em proteção de dados prioriza a proteção dos dados pessoais e o respeito à privacidade dos titulares antes de qualquer novo desenvolvimento na empresa. Esta iniciativa representa uma transformação cultural que afeta não apenas a FUNDAÇÃO DOM AGUIRRE, mas também todas as organizações públicas e privadas.

Esta Política resume os principais aspectos do nosso programa de governança em proteção de dados e privacidade, garantindo transparência nas nossas ações e na busca pela conformidade técnica e legal, além de fornecer um recurso prático e direto para informações sobre o tema.

3.2. Comitê de Proteção de Dados

É o órgão multidisciplinar composto por representantes de áreas estratégicas da Instituição, responsável por definir e implementar medidas e ações de atuação nas frentes de segurança da informação e privacidade de dados, bem como fomentar a cultura de proteção de dados visando a excelência da Instituição no que diz respeito as questões de privacidade e proteção de dados.

O Comitê também tem como missão contribuir para a uniformidade no registro das operações e no tratamento de dados pessoais da Instituição, manter a segurança de todo o sistema de informação e minimizar eventuais conflitos de interesse que possam surgir.

São funções do Comitê de Proteção de Dados:

1. Orientar os demais colaboradores no cumprimento da LGPD;
2. Adotar medidas que visem à melhoria contínua dos processos de privacidade e tratamento de dados;
3. Aconselhar sobre questões relativas à privacidade e proteção de dados;
4. Incentivar a adoção de práticas transparentes e a aplicação consistente das regras de privacidade e proteção de dados.

Contato: cpd@fda.com.br

3.2.1. Encarregado de Proteção de Dados

A LGPD instituiu o encarregado de proteção de dados como um representante, a ser designado pela FUNDAÇÃO DOM AGUIRRE para atuar como intermediário entre a instituição, os titulares de dados e a ANPD.

O encarregado será responsável por:

1. Receber e tratar reclamações e comunicações dos titulares de dados, bem como responder e tomar as devidas providências;
2. Receber comunicações da ANPD e adotar as medidas necessárias;
3. Orientar funcionários e contratados da entidade sobre as práticas relacionadas à proteção de dados pessoais;
4. Executar outras atribuições conforme determinado pelo controlador ou estabelecido por normas adicionais.

Nossa Encarregada de Proteção de Dados é a

Seusdados Consultoria em Gestão de Dados Ltda.

3.2.2. Administração da Fundação Dom Aguirre

As orientações do CPD e do Encarregado são submetidas à **Administração da Fundação Dom Aguirre**, que é responsável pela tomada de decisões administrativas da Instituição, incluindo aquelas relativas ao tratamento de dados pessoais, de modo que seja o principal propulsor da cultura de proteção de dados e privacidade, servindo de exemplo para as demais áreas da organização.

Contato: cpd@fda.com.br

3.2.3. Colaboradores e prestadores de serviços

São todas as aquelas pessoas que possam representar os nossos interesses como organização e participem, direta ou indiretamente, dos tratamentos de dados pessoais necessários para o funcionamento da nossa organização.

São responsabilidades específicas de todos os colaboradores e prestadores de serviços, conforme aplicável, no que tange à proteção de dados e à privacidade:

1. Firmar termo de compromisso e confidencialidade sobre a gestão e o tratamento de dados pessoais que tiverem acesso por força da relação mantida com a FUNDAÇÃO DOM AGUIRRE;

2. Garantir que as informações às quais tenha acesso, independentemente de sua natureza (comercial, estratégica, tecnológica ou que tornem identificável uma pessoa) sejam tratadas com sigilo e confidencialidade, com observância às regras da Lei Geral de Proteção de Dados (LGPD), Lei 13.709 de 18 de agosto de 2018;

3. Manter as informações na esfera exclusiva das pessoas envolvidas no processo e jamais utilizá-las para uso particular, inclusive após o desligamento da organização, exceto para cumprimento de obrigação legal e/ou exercício regular de direito em processo;

4. Comunicar imediatamente ao superior hierárquico ou ao canal de contato designado qualquer ato ou omissão que se considere em desacordo com os princípios estabelecidos na LGPD, bem como com as normas, leis e regulamentos que a FUNDAÇÃO DOM AGUIRRE deve observar em suas atividades, ou ainda quando não se sentir devidamente capacitado para decidir sobre a forma de tratamento de dados pessoais;

5. Comunicar imediatamente ao superior hierárquico, quaisquer hipóteses de incidentes de segurança ou uso indevido de dados que tiver conhecimento, abstendo-se de comentar sobre o assunto com terceiros;

6. Atuar para evitar e/ou minimizar eventuais impactos de incidentes de segurança ou uso indevido de dados.

3.3. Estrutura de gestão de riscos

Nosso modelo de **governança em proteção de dados** está alinhado com a **governança em segurança da informação** e a **governança de tecnologia da informação**, que envolvem também a **gestão de riscos**.

Nossa estrutura de **gestão de riscos** é baseada em **três linhas de defesa:**

A 1º LINHA DE DEFESA é composta pelas funções de gerência operacional, que são os responsáveis por monitorar e controlar as atividades operacionais, de forma que os controles incorporados aos sistemas e processos de trabalho sejam executados sob sua responsabilidade. Estes controles de gestão, quando exercidos de modo adequado, funcionam para garantir a conformidade com leis e regulamentos, evitando a execução inadequada de processos e a ocorrência de eventos inesperados.

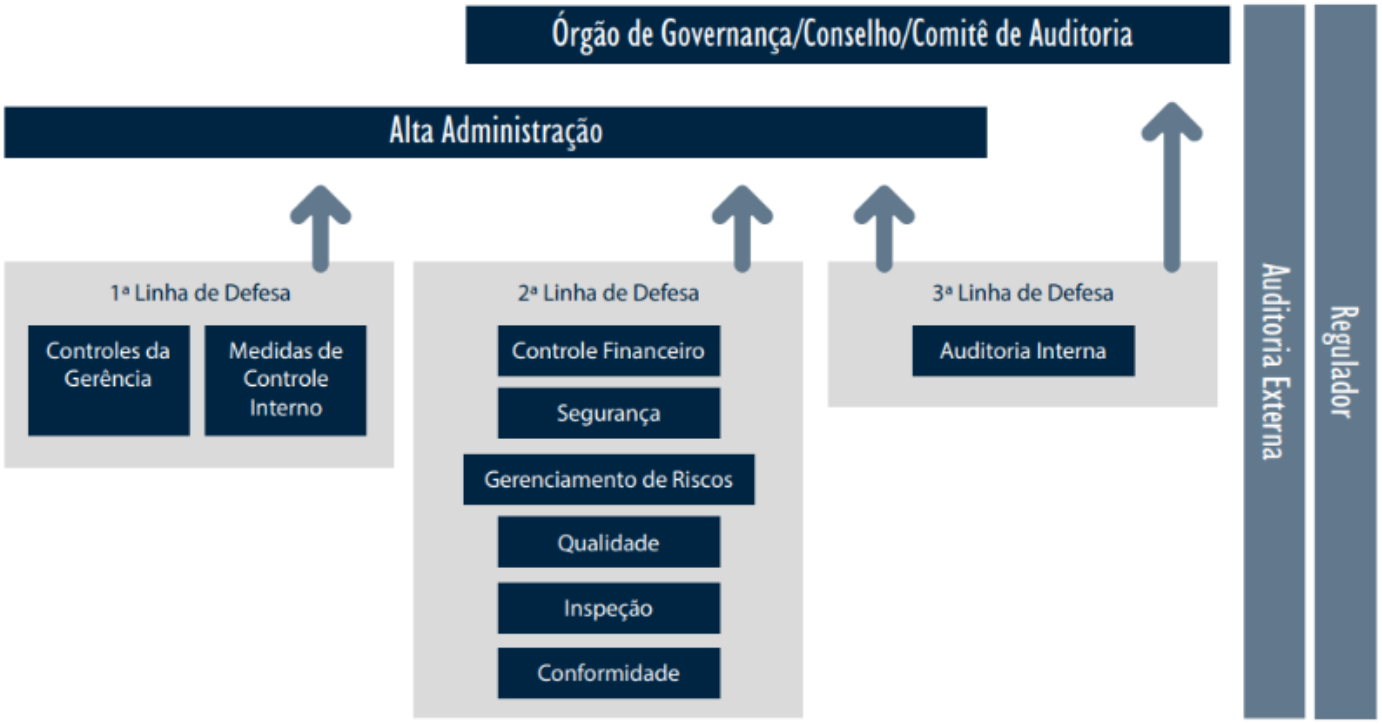
Dentre as atividades realizadas nesta função, destacam-se a identificação, a avaliação, o controle e a mitigação dos riscos, visando a construção de bases para o desenvolvimento e a implementação de políticas e procedimentos internos. É comum que a primeira linha de defesa abranja as atividades de risco e controle realizadas pela gerência imediatamente responsável pelo processo de trabalho diário e, também, aquelas executadas pela gerência de nível intermediário que de uma forma ou de outra estão relacionadas a este processo de trabalho.

A 2º LINHA DE DEFESA é composta por funções atreladas a gestão de risco e gestão de conformidade. Estas funções, também estão submetidas ao controle e direção da administração da Fundação Dom Aguirre, e são implementadas para garantir que os controles e os processos de gerenciamento de riscos executados pela primeira linha de defesa funcionem de acordo com o estabelecido, principalmente, através da atividade de monitoramento contínuo.

As funções que compõem a segunda linha de defesa podem variar de acordo com a estrutura organizacional da Instituição.

Já a 3º LINHA DE DEFESA é composta por uma Auditoria Interna que é responsável por realizar avaliações tanto na 1ª como na 2ª linha de defesa. A premissa da auditoria é relatar para a Administração se o Processo de Gestão de Riscos atende as expectativas de suportar os riscos da empresa e se a primeira linha está operacionalizando o respectivo processo. Este Órgão reportará suas descobertas à gestão e ao corpo administrativo para promover e facilitar a melhoria contínua na Instituição. **No âmbito do programa de privacidade e proteção de Dados, o Comitê de Proteção de Dados desempenhará essa função.**

Figura 2. Modelo das Três Linhas de Defesa



Fonte: Extraído de IIA (2013, p.2).

3.4. Prestação de contas e responsabilidade (*accountability*)

A vigência da LGPD trouxe como obrigação da FUNDAÇÃO DOM AGUIRRE o dever de prestação de contas e responsabilidade (art. 6º, X da LGPD), ou, do termo em inglês *accountability*, cujo objetivo é demonstrar a efetividade do programa de conformidade em privacidade e proteção de dados pessoais, bem como a observância das leis vigentes.

Para demonstrar a eficácia das medidas tomadas para a conformidade com as regras de proteção de dados, a FUNDAÇÃO DOM AGUIRRE mantém um rigoroso e estruturado processo de registro de evidências sobre o funcionamento do seu programa de conformidade.

Assim, não basta que a nossa organização esteja em conformidade com a lei, mas também deve ser capaz de demostrar conformidade. Por isso, estabelece-se um conjunto de medidas aptas para a geração de evidências, dentre as quais, cita-se:

1. Registrar as atividades de tratamento de dados, considerando as bases legais aptas e seus procedimentos específicos (e.g., Termo de Consentimento; Avaliação de Legítimo Interesse);
2. Elaborar e atualizar relatórios de impacto à proteção de dados (RIPD);
3. Manter estruturas de governança para aplicação e fiscalização de códigos e manuais de boas condutas, treinamentos e conscientização para fomento de cultura de proteção de dados e privacidade;
4. Medidas de incentivo para comportamentos de conformidade à lei e medidas de repressão em casos de descumprimentos.

3.5. Gestão de riscos em privacidade e proteção de dados

Por sermos uma organização que se utiliza de dados pessoais, a presença de riscos relacionados a atividade de tratamento, como a coleta, armazenamento e descarte, é uma situação inerente ao negócio.

A partir das circunstâncias particulares de cada processamento de dados, compreenderemos quais são os riscos de cada atividade e quais as medidas mais adequadas para saná-los ou mitigá-los. Em situações de risco elevado, por exemplo, a adoção de medidas de privacidade e segurança é imprescindível para o cumprimento da legislação.

Por isso, a FUNDAÇÃO DOM AGUIRRE compromete-se a identificar, mensurar e gerir os potenciais riscos das atividades de tratamento de dados, a fim de impedir a ocorrência de danos aos direitos de titulares de dados, bem como definir a intensidade das medidas de mitigação aplicáveis a cada caso.

4. Ciclo de vida do dado pessoal

Em todo o processo de tratamento de dados pessoais, desde a sua coleta até sua eliminação, existe um **ciclo de vida do dado pessoal a ser considerado**, o qual deve ser acompanhado por nós.

1. **Coleta dos dados**, que deve obedecer aos princípios da finalidade, adequação e necessidade
2. **Utilização do dado pessoal**, fundamentada em uma das hipóteses legais
3. Após a utilização, os dados devem ser **guardados pelos prazos estabelecidos** por leis aplicáveis em cada caso
4. Com o fim dos prazos legais, os **dados pessoais** devem ser eliminados de modo seguro e permanente

O tratamento dos dados pessoais devem obedecer as hipóteses permitidas pela LGPD e não devem ser processados em casos de ofensa as legislações.

Além disso, com o fim do tratamento de dados, os dados pessoais armazenados nos sistemas e ambientes da organização, devem ser revistos e higienizados periodicamente e, não existindo prazos legais que autorizem a sua retenção, devem ser, descartados com a devida segurança, em consonância com a Política de Guarda e Descarte.

Em caso de dúvida sobre a legitimidade de uma determinada situação ou projeto que envolva tratamento de dados pessoais, consulte o Comitê de Proteção de Dados, pelo e-mail: **cpd@fda.com.br**

5. *Privacy by design* e *Privacy by default*

Dois conceitos muito importantes sobre privacidade incorporados pela Lei Geral de Proteção de Dados são: *privacy by design* (privacidade por concepção) e *privacy by default* (privacidade por padrão), a aplicação desses conceitos em processos e rotinas envolvendo tratamentos de dados pessoais podem reduzir ou eliminar riscos à violação da proteção dos dados ou incidentes de segurança.

5.1. Privacidade por concepção

O conceito de privacidade por concepção propõe que as medidas de privacidade sejam consideradas desde a etapa de desenvolvimento de um produto ou serviço, isto é, desde criação e projeto a privacidade deve ser implementada de modo a garantir a sua efetividade no produto ou serviço final.

O conceito ainda traz sete princípios:

- Proativo e não reativo - preventivo e não corretivo;
- Privacidade como padrão (*Privacy by Default*);
- Privacidade incorporada ao design;
- Funcionalidade total (soma positiva, não soma-zero);
- Segurança de ponta a ponta;
- Visibilidade e transparência;
- Respeito pela privacidade do usuário.

5.2. Privacidade por padrão

O conceito de privacidade por padrão, inserido no conceito acima, estabelece que durante o desenvolvimento e a execução de um produto ou serviço a privacidade deve ser tratada como prioridade, portanto, devem ser implementadas as melhores medidas técnicas e administrativas para garantir a segurança das informações e o respeito à legislação. Para isso, deve ser realizado um monitoramento contínuo dos processos de tratamento de dados, das pessoas e dos ativos de informação envolvidos.

6. Relacionamento com parceiros e fornecedores

6.1. Requisitos pré-contratuais

Avaliação do nível de conformidade dos parceiros e fornecedores

Será aplicado um questionário a todos os parceiros e fornecedores, de modo a avaliar sua adequação às normas de proteção de dados, de acordo com as particularidades dos tratamentos de dados realizados entre as empresas.

Gestão de evidências da regularidade do parceiro

As respostas do fornecedores devem ser armazenadas durante a vigência do contrato e, por período específico após o fim da relação.

Elaboração de termos ou disposições de proteção de dados

A depender da complexidade dos tratamentos de dados realizados entre as empresas, serão aplicados termos de compromisso e confidencialidade e/ou inseridas cláusulas de proteção de dados nos contratos.

Avaliação do Encarregado (DPO)

Antes de formalizar a contratação do parceiro ou fornecedor, a FUNDAÇÃO DOM AGUIRRE deve comunicar o Encarregado de Proteção de Dados (DPO) e apresentar os documentos necessários para a avaliação desta nova contratação.

Formalização do Contrato

Com o aval formalizado pelo Encarregado de Proteção de Dados (DPO) e ciência do Comitê de Proteção de Dados da FUNDAÇÃO DOM AGUIRRE, o contrato poderá ser assinado pelas partes.

6.2. Requisitos durante a execução do contrato

Monitoramento contínuo

Durante toda a relação contratual, nós iremos realizar um monitoramento da conformidade dos nossos parceiros e fornecedores com as normas de proteção de dados e segurança da informação, inclusive com possibilidade de solicitação de auditoria interna para apurar eventuais irregularidades.

Gestão de evidências da regularidade dos parceiros

Para atender ao princípio da responsabilização e prestação de contas (art. 7º, inciso X da LGPD), iremos solicitar e manter continuamente registros da conformidade dos nossos parceiros e fornecedores, para o caso de eventuais fiscalizações e solicitações pelas autoridades competentes e os titulares de dados.

7. Respostas a incidentes de segurança

Um incidente de segurança da informação é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita, passível de impactar a **disponibilidade**, **integridade**, **confidencialidade** ou **autenticidade** de um ativo de informação, que são os pilares que estruturam a segurança da informação.

Se uma determinada violação de segurança envolver informações pessoais, o incidente deve ser tratado em observância a Lei Geral de Proteção de Dados (LGPD).

7.1. Como identificar um incidente de segurança com dados pessoais?

Para identificação de um incidente de segurança com dados pessoais, é necessário consultar se a situação se enquadra ao conceito de incidente apresentado pela **Autoridade Nacional de Proteção de Dados (ANPD)**:

"Um incidente de segurança com violação de dados pessoais é entendido como violação da segurança, capaz de provocar de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento."

Veja alguns exemplos de incidentes de segurança com dados pessoais:
Exemplo 1: Encaminhar arquivo ou planilha para destinatário não autorizado via e-mail;
Exemplo 2: Acesso não autorizado por meio de ataque cibernético/*hacker* aos sistemas da empresa;
Exemplo 3: Roubo ou furto de equipamentos, dispositivos ou mídias de armazenamentos (pen-drive, notebooks, celulares, HD externos) com arquivos e documentos pessoais;
Exemplo 4: Perda ou eliminação acidental de equipamentos, dispositivos ou documentos durante o seu transporte;
Exemplo 5: Alteração não autorizada de dados cadastrais de um Titular de Dados, que torne as informações inverídicas ou incorretas;

7.2. O que fazer em caso de identificação de um incidente?

Caso você, **colaborador**, **prestador de serviços** ou **terceiro**, identifique qualquer situação ou evento que esteja relacionado a uma violação de segurança em nossos ambientes, permaneça em sigilo e comunique imediatamente o responsável pelo Comitê de Proteção de Dados através do e-mail: cpd@fda.com.br

7.3. Quem é responsável por conduzir o incidente de segurança?

Em caso de incidente de segurança com dados pessoais, é o **Comitê de Proteção de Dados da FUNDAÇÃO DOM AGUIRRE** que será responsável pela condução e tratativas necessárias, sendo apoiado pelo Encarregado de Proteção de Dados (DPO).

A Administração da Fundação Dom Aguirre será comunicada formalmente e por escrito sobre cada uma das etapas conduzidas pelo Comitê e pelo Encarregado de Proteção de Dados e ficará responsável pela tomada de decisões financeiras e administrativas .

8. Treinamentos e Conscientização

As falhas humanas são um dos principais fatores que podem causar tratamentos de dados pessoais em desconformidade com as legislações.

Por isso, como medida de prevenção para ocorrência de irregularidades ou ilicitudes, a FUNDAÇÃO DOM AGUIRRE promove a conscientização contínua de seus colaboradores sobre a importância da proteção de dados, bem como deve fomenta as boas práticas.

8.1. Obrigatoriedade

De acordo com as regras impostas pela LGPD, a promoção de treinamentos e conscientização sobre a proteção de dados e privacidade passa a ser obrigatória e deve ocorrer periodicamente e de modo permanente em nossa Instituição.

Para garantir a sua efetividade, os treinamentos e conscientizações devem ocorrer por meio de linguagem acessível ao público-alvo e condizente com as especificidades da nossa organização.

Os materiais, cursos e sessões são atualizados periodicamente, a fim de garantir a conformidade com a proteção de dados deve ser algo permanente e a participação de todos os colaboradores ou prestadores convocados é **obrigatória, independentemente do nível hierárquico.**

8.2. Evidências

Treinamentos, cursos, palestras e workshops relacionados ao programa de conformidade em privacidade e proteção de dados deverão ser registrados mediante gravação, filmagem, lista de presença devidamente assinada por todos os participantes e/ou qualquer outro meio que evidencie, os quais devem ser armazenadas em local seguro e com restrição de acesso, a fim de atestar o nosso compromisso com a adequação às leis, a adequada capacitação de nossos funcionários e para comprovação e evidência junto as autoridades competentes.

9. Em caso de descumprimento desta Política

Todas as pessoas vinculadas com a FUNDAÇÃO DOM AGUIRRE e suas mantidas têm o dever de cumprir e aplicar as disposições e diretrizes desta Política. No entanto, a suprema vigilância e aplicação das sanções estabelecidas nesta Política serão adotadas com base no mérito e gravidade da situação. Para avaliar ocorrências, realizar investigações, aplicar as sanções e disseminar a cultura de proteção de dados em nossa organização, foi criado um Comitê de Proteção de Dados. (cpd@fda.com.br).

Após a apuração de uma situação ou violação mediante processo administrativo interno, caso haja identificação de atuação indevida, proposital ou não, de um de nossos colaboradores, sócios, diretores, prestadores de serviços ou fornecedores, o infrator será responsabilizado dentro dos limites estabelecidos na legislação vigente.

O descumprimento desta Política por colaboradores em qualquer nível hierárquico e que eventualmente cause dano grave ou irreparável à FUNDAÇÃO DOM AGUIRRE, demais colaboradores ou titulares de dados pessoais, após regular processo de apuração de incidente de segurança da informação, conduzido pelo Encarregado de Proteção de Dados (*DPO*), com apoio do Comitê de Proteção de Dados (CPD), observados os direitos à ampla defesa e contraditório, poderá culminar em:

a) advertência

b) suspensão

c) demissão por justa causa

d) rescisão contratual,
no caso de fornecedores e prestadores de serviços

e) ajuizamento de ação por danos materiais ou ação criminal,
a depender da gravidade e do dano causado

f) outras providências previstas na lei vigente

10. FAQ (Perguntas frequentes)

Ainda está com dúvidas relacionadas à nossa Política de Proteção de Dados? Trouxemos alguns tópicos que podem te ajudar:

Como o Titular de Dados poderá exercer seus direitos?

O titular de dados pode exercer os seus direitos por meio do nosso canal exclusivo: cpd@fda.com.br. As solicitações serão respondidas em até 05 dias.

Caso sejam necessárias informações complementares para que possamos responder à solicitação, poderemos entrar em contato com o titular, assim atenderemos sua demanda de forma mais assertiva.

Como serão informadas alterações nesta Política?

A nossa Política de Proteção de Dados poderá passar por atualizações, por isso orientamos que o site seja periodicamente visitado para obter informações atualizadas e transparentes dessas alterações. Ressaltamos que, caso sejam necessárias mudanças substanciais e relevantes, publicaremos essa atualização e entraremos em contato com os interessados para ciência dos novos termos.

Quem são os Agentes de Tratamento?

Segundo a LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o controlador e o operador.

O **controlador** é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

O **operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, como por exemplo, pessoas jurídicas diversas daquela representada pelo controlador, que exerçam atividade de tratamento de dados em seu nome.

É necessário a coleta do consentimento para o tratamento de dados pessoais?

O consentimento é apenas uma das bases legais que autoriza o tratamento de dados pessoais. A depender do tipo de relação estabelecida, o tratamento de dados poderá estar respaldado em outras bases legais, como execução de contrato, legítimo interesse, exercício regular de direitos etc.

Como tratamos os dados de Criança e Adolescente?

O tratamento de dados pessoais de crianças e adolescentes é realizado de acordo com os parâmetros do art.14 da LGPD, sempre em seu melhor interesse.
Além disso, o tratamento de Dados Pessoais e Dados Pessoais de crianças e adolescente é realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Dado anonimizado e pseudoanonimizado são a mesma coisa?

A anonimização é a possibilidade de converter dados pessoais em dados anonimizados. É caracterizada pela utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Ou seja, para que o dado seja considerado anonimizado, não deve ser possível, por meios técnicos e razoáveis disponíveis, a reidentificação do titular do dado.

Segundo art. 12 da LGPD, tais dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Já no processo de pseudoanonimização, os dados pessoais são falsamente anonimizados, sendo possível, a qualquer momento e a partir de métodos conhecidos e disponíveis, que a empresa desfaça a anonimização e reidentifique o titular, em processo de reversão, como ocorre na criptografia e descriptografia.

Em qual situação nós não excluiremos os dados?

Em algumas situações autorizadas pela LGPD, poderemos manter os dados em nossa base, sendo elas:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei;
- uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Como atuamos em casos de Incidente de Segurança?

Em caso de incidente de segurança com os dados pessoais que gerem riscos ou danos relevantes, nos comprometemos a informar os titulares o mais breve possível com as medidas disponíveis para diminuir ou impedir que os dados sejam utilizados indevidamente por terceiros ou criminosos.