Política de Privacidade e Proteção de dados

Quadro resumo

Código documento:	Processo:	Última atualização:
01/2023	Diretrizes e regras para tratamento de dados pessoais	03/07/2023

Áreas impactadas:	Objetivo:	Resumo:
Todas as áreas da empresa	Definir como, quando e para quais finalidades a empresa poderá tratar dados pessoais	Documento base sobre proteção de dados na empresa

Sumário:

1. Introdução

Este documento lança as bases para toda a estrutura de governança em privacidade e proteção de dados na FUNDAÇÃO DOM AGUIRRE. Nele, procuramos informar nossos públicos de interesse (clientes, colaboradores, parceiros e fornecedores) a respeito do assunto, bem como afirmar nosso compromisso, valores e processos internos adotados sobre privacidade e proteção de dados.

1.1. O direito à privacidade

O direito à privacidade garante aos cidadãos a não intervenção de terceiros em sua esfera privada, também chamado de "direito de estar só". É um direito fundamental e está protegido pela Constituição Federal (art. 5º, inciso X) e pelo Código Civil brasileiro (art. 21). A violação à privacidade enseja reparação por indenização, e pode ocorrer de várias formas, inclusive por uso indevido de informações pessoais.

1.2. O direito à proteção de dados pessoais

As informações pessoais podem impactar em outros direitos dos cidadãos, como a privacidade, intimidade, honra e a imagem. Porém, entendendo que os dados pessoais deveriam ter sua própria tutela, tendo em vista suas particularidades e seus impactos específicos nas relações privadas, o Brasil promulgou a Lei Geral de Proteção de Dados em 2018 e declarou a proteção de dados como um direito fundamental, inserindo-a no inciso LXXIX do art. 5º da Constituição Federal em 2022.

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 dá transparência a todos sobre quais informações, como, quando e para qual finalidade podemos vir a tratar. Nossa política estabelece, ainda, as diretrizes e padrões inegociáveis que adotamos para proteger os dados pessoais que tratamos e garantir que as pessoas que se relacionam conosco tenham segurança e confiança na forma como processamos os dados.

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 relacionadas às metas de privacidade estabelecidas pela FUNDAÇÃO DOM AGUIRRE para a atuação de todos aqueles elencados 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 modo uniforme e transparente, promovendo a implementação dessas regras como base para o desenvolvimento da empresa, garantindo não somente 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 a respeito de nossa busca pela conformidade com a privacidade e proteção de dados pessoais e como podem exercer direitos estabelecidos 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 de pessoas, independentemente do tipo de relação mantida entre as partes. Portanto, essa Política se aplica a você:

- Diretores
- Parceiros
- Prestadores de Serviços
- Representantes
- Sócios
- Fornecedores
- 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;
- Treinamentos.

2.3. Nossa Visão de Privacidade e Proteção de Dados

A Fundação Dom Aguirre é uma pessoa jurídica de direito privado, sem fins lucrativos, de caráter educacional, de assistência social e filantrópica, conforme certificado em 29 de setembro de 1972, cujo certificado definitivo foi concedido em 28 de abril de 1982, declarada de utilidade pública federal pelo decreto 86.668, de 30 de novembro de 1981, publicado no DOU de 02/12/1981, declarada de utilidade pública estadual pela Lei 8.064 de 19 de outubro de 1992, publicada no DOE de 20/10/1992, e de declarada de utilidade pública municipal pela Lei 1.397 de 1º de abril de 1966, publicada pela imprensa local em 02/04/1966, detentora do Certificado de Entidade Beneficente de Assistência Social – CEBAS, mantenedora da Universidade de Sorocaba – UNISO, do ICT Uniso Tech e do Colégio Dom Aguirre.

Nossa política de privacidade foi desenvolvida com o intuito de que você possa compreender as formas de tratamento de dados utilizadas pela Fundação Dom Aguirre e suas mantidas, explicando como utilizamos e protegemos os dados coletados, cumprindo com o princípio da privacidade.

Ressalta-se que esta política de privacidade é aplicada a todas as operações institucionais, especialmente as que ocorrem em plataformas digitais, para a consecução de seus serviços educacionais, decorrentes das atividades desenvolvidas, demonstrando seu compromisso e respeito no tocante à privacidade dos titulares e proteção de seus dados pessoais, expondo as razões pelas quais poderá realizar a coleta de dados.

A Fundação Dom Aguirre e suas mantidas na condição de instituição de ensino, tem acesso diário a dados pessoais de discentes, docentes, funcionários ou terceiros envolvidos em suas relações obrigacionais, mas está comprometida com as obrigações legais impostas para proteção da privacidade e de dados pessoais, especialmente quanto ao tratamento de dados, regularizado pela Lei Geral de Proteção de Dados.

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 sócios, representantes, colaboradores, prestadores de serviços:

1. Cumprir as disposições legais aplicáveis à proteção de dados pessoais e privacidade, tendo como norma de origem a **Constituição Federal do Brasil e sequencialmente, 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 de informação** que garantam a integridade, confidencialidade e disponibilidade dos dados pessoais, levando como referência as boas práticas internacionais sob a matéria e, quanto seja possível, as diretrizes nas normas técnicas da ABNT ISO/IEC 27000, 27.001, 27.002 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 cada novo desenvolvimento que implique em tratamento de dados pessoais, o procedimento de ***Privacy by design*** **(privacidade desde a concepção*)* e *privacy by default* (privacidade por padrão)**

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 da nossa atividade;

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, ao menos uma vez ao ano, das análises de conformidade dos processos de tratamentos de dados e sua adequação à lei, tais como a garantia da gestão eficiente do consentimento prestado pelo titular nas hipóteses de tratamento de dados por ele autorizado na forma da lei e, na ausência do consentimento, a possibilidade de aplicação de outra base legal;
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) Obrigatoriedade da elaboração de Avaliação de Legítimo Interesse (LIA) anteriormente ao desenvolvimento de novas atividades fundamentadas na hipótese legal do legítimo interesse (art. 7, inciso IX da LGPD);

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

i) Oferta de treinamento contínuo, durante toda a jornada do colaborador e prestador de serviço 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 ao 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 ao 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 a 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, § 2°, I, do art. 50, que "o controlador poderá implementar programa de governança em privacidade".

3.1. Objetivo

A proteção de dados pessoais deve ser desenvolvida estrategicamente como um programa de *compliance* (vivo e fluido) que exige das diversas áreas da organização atenção permanente.

Nesse sentido, nosso programa de governança em proteção de dados considera **proteção de dados pessoais e o respeito à privacidade do titular como objeto de atenção primária, anterior a qualquer processo de desenvolvimento que venha a ser implementado em nossa empresa.** Trata-se de transformação cultural do modelo organizacional que atinge não apenas a FUNDAÇÃO DOM AGUIRRE, mas todas as organizações públicas e privadas.

Esta Política agrega os principais aspectos de nosso programa de governança em proteção de dados e privacidade, de modo a garantir **transparência** sobre nossas **ações** e sobre nossa busca pela **conformidade técnica e legal**, além de oferecer um meio prático e direto de **fonte de informações** a respeito do tema.

3.2.1. Comitê de Proteção de Dados

É o órgão multidisciplinar composto por representantes de áreas estratégicas da Organização (stakeholders), 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 na Organização no que diz respeito as questões atinentes a privacidade e proteção de dados.

O Comitê também tem como missão contribuir para uniformidade em relação ao registro das operações e tratamento de dados pessoais da Organização, manutenção da segurança de todo o sistema de informação e minimização de eventuais conflitos de interesses que possam surgir.

São funções do **Comitê de Proteção de Dados:**

1. Orientar os demais colaboradores no cumprimento da LGPD;
2. Adotar conclusões que visem à melhoria constante do processo de privacidade e tratamento de dados;
2. Aconselhar sobre questões relativas a privacidade e proteção de dados;
3. Incentivar a adoção de práticas transparentes e aplicação coerente de regras em matéria de privacidade e proteção de dados.

Contato: cpd@fda.com.br

Importante ressaltar que toda atuação do CPD deverá se dar nos moldes previamente validados pela DPO.

3.2.2. Encarregado de Proteção de Dados

A LGPD criou a figura do encarregado de proteção de dados para ser a pessoa indica pela FUNDAÇÃO DOM AGUIRRE para ser o elo de comunicação entre nós, os titulares de dados e a ANPD. Ele também será responsável por:

1. Aceitar reclamações e comunicações dos titulares, responder e tomar providências;
2. Receber comunicações da ANPD e adotar providências;
3. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
4. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em demais normas.

Nossa Encarregada de Proteção de Dados é a

Seusdados Consultoria em Gestão de Dados Ltda.

CNPJ n. 33.899.116/0001-63 – Contato: (11) 4040-5552

3.2.3. Administração da Fundação Dom Aguirre

As orientações do CPD e do Encarregado são submetidas para a **Administração da Fundação Dom Aguirre**, que é responsável pela tomada de decisões administrativas da empresa, 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: falecom@fda.com.br

3.2.4. 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 deveres específicos de todos os colaboradores e prestadores de serviço, no que couber, em relação à proteção de dados e 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 identifiquem ou 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 imediato ou canal de contato, qualquer ato ou omissão que julgar contrário aos princípios previstos na LGPD ou que entendam em desacordo com normas, leis, regras que a FUNDAÇÃO DOM AGUIRRE deve cumprir em suas atividades, ou quando não se considerar 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. Gestão de riscos

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.

No entanto, as informações de titulares de dados os usuários estarão seguramente armazenadas pela Universidade de Sorocaba – UNISO e serão utilizadas tão somente para finalidade específica, previamente autorizada, ressalvadas as decorrentes de obrigação legal.

A Universidade de Sorocaba – UNISO dispõe de meios tecnológicos que garantem a segurança das informações, todavia às áreas de links e acessos restritos, mediante login e senha, serão de total responsabilidade do usuário, que deve zelar pela sua correta utilização, evitando fraudes.

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.

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.

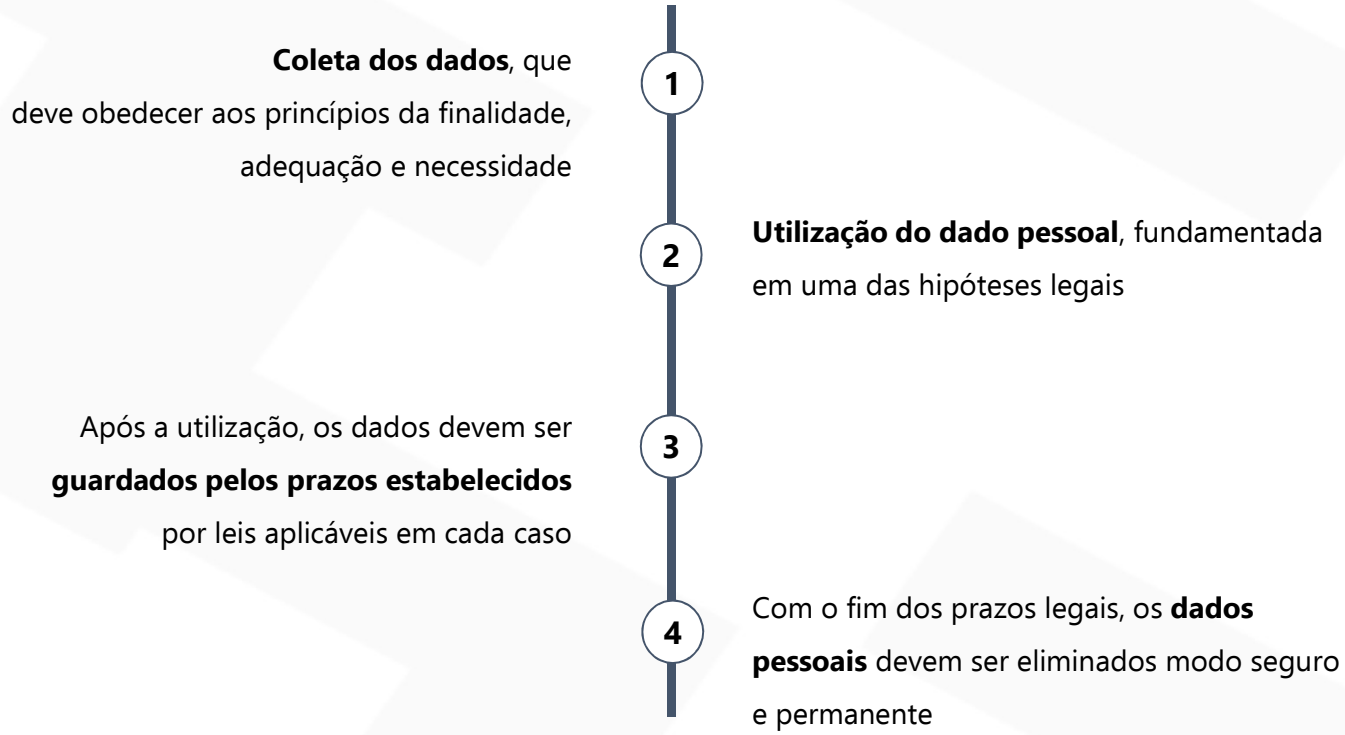
Para demonstrar a eficácia das medidas tomadas para a conformidade com as regras de proteção de dados, a FUNDAÇÃO DOM AGUIRRE deve manter um rigoroso e estruturado processo de registro de evidências sobre o funcionamento do seu programa de conformidade.

Assim, não basta que a nossa organização esteja em conformidade com a lei, mas também deve ser capaz de demostrar o seu *compliance*. Por isso, deve-se estabelecer 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 sanções em caso de descumprimento.

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.



O tratamento dos dados pessoais devem obedecer as hipóteses permitidas pela LGPD e não devem ser processados em casos de desrespeito 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 da FUNDAÇÃO DOM AGUIRRE.

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 (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 o *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. Ou seja, 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 para Contratos e/ou Convênios que envolvam tratamento de dados

Avaliação do nível de conformidade dos parceiros e fornecedores

Será aplicado um questionário inicial aos 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 solicitará parecer do Encarregado de Proteção de Dados (DPO) para avaliação em relação à LGPD.

Formalização do Contrato

Com a devolutiva do Encarregado de Proteção de Dados (DPO) e ciência do Comitê de Proteção de Dados da FUNDAÇÃO DOM AGUIRRE, o contrato será encaminhado à administração da Fundação para posterior deliberação e assinatura.

6.2. Requisitos durante a execução do contrato

Monitoramento contínuo

Durante toda a relação contratual, haverá 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** 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 seguinte 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** quem 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 .

Em caso de incidente de segurança solicite o Plano de Respostas a Incidentes junto ao Comitê de Proteção de Dados ou da Administração (cpd@fda.com.br)

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 deve promover continuadamente a conscientização sobre a importância da proteção de dados, bem como deve fomentar as boas práticas e condutas a serem adotadas em nossa organização.

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 devem ser 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 outra 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.

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 destinado ao Titular de Dados, através do link https://app.meresponda.com/privacidade/seusdados\.

As solicitações serão respondidas em até 15 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 está respaldado e 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.