POLÍTICA DE GOVERNANÇA DE DADOS PESSOAIS

Sumário

1 Introdução

Este documento dispõe sobre a Política de Governança de Dados Pessoais do **HOSPITAL SANTA TERESINHA**, estabelecendo princípios, diretrizes, atribuições e responsabilidades para a gestão de dados, em observância aos preceitos do art. 50 da Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (“LGPD”).

2 Escopo

Os termos dispostos neste documento abrange as ações de boas práticas e de governança na gestão de dados pessoais estruturadas pelo **HOSPITAL SANTA TERESINHA**, na difusão e aprimoramento da cultura de privacidade e proteção de dados pessoais pelos funcionários e/ou profissionais que agem em seu nome.

A presente Política é aplicável e deve ser observada por todos aqueles que atuem em nome do **HOSPITAL SANTA TERESINHA** nas atividades e funções que envolvam dados pessoais.

3 Definições

Para efeitos desta Política, são considerados os seguintes termos e seus respectivos significados:

- **Dado Pessoal**: informação relacionada a pessoa natural identificada ou identificável, ou seja, quaisquer dados que possam identificar uma pessoa;
- **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 referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **Tratamento de dados**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, tratamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- **Agentes de Tratamento**: Controlador e Operador;

- **Encarregado dos Dados** (sigla **DPO** – Data Protection Officer): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- **Autoridade Nacional de Proteção de Dados (ANPD)**: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD;
- **LGPD**: Lei Geral de Proteção de Dados Pessoais, lei nº 13709/2018;
- **Dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- **Anonimizaçã**o: 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;
- **Uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

4 Diretrizes

Esta Política busca garantir a proteção dos dados pessoais acessíveis no âmbito das operações do **HOSPITAL SANTA TERESINHA**, assegurando que sejam sempre tratados em observância aos princípios da boa-fé, finalidade, adequação e necessidade, bem como livre acesso, segurança, prevenção e não discriminação, de modo a preservar a qualidade dos dados e transparência ao titular dos dados sobre o tratamento de seus dados pessoais, conforme as melhores práticas de governança e segurança.

Pautado nos princípios estabelecidos pela LGPD, especialmente em observância aos princípios de segurança e prevenção, as diretrizes e ações constantes nesta Política visam assegurar a proteção de dados e mitigação dos riscos.

4.1 Premissa

Esta política tem como premissa que dados e informações bem organizados, documentados, acessíveis e verificados quanto a sua exatidão e validade proporciona as seguintes vantagens:

a) ampliação da visibilidade;

b) maior rapidez na descoberta do conhecimento e inovação;

c) prevenção de fraudes;

d) redução da replicação de esforços e de custos associados;

e) mitigação do risco de contradição entre as diversas áreas e gestores da organização na divulgação de informações relevantes;

f) garantia do sigilo e da integridade, autenticidade, disponibilidade, conformidade e segurança de dados e informações.

5 Funções e Responsabilidades

O **HOSPITAL SANTA TERESINHA** trata a segurança dos dados pessoais com muita seriedade. Uma das principais características de uma abordagem eficaz à proteção de dados é a definição de funções, cada uma com responsabilidades determinadas. Cada uma dessas funções precisa ser direcionada para indivíduos ou grupos específicos dentro da organização.

Ao garantir que os papéis e responsabilidades estejam claramente definidos, podemos evitar incidentes de proteção de dados ou caso ocorra alguma situação, estamos capacitados para uma atuação efetiva e adequada.

5.1 Funções

Dentro da estrutura de proteção de dados, as seguintes funções principais precisam ser definidas e atribuídas:

- Controlador de Dados
- Operador de Dados
- Encarregado da Proteção de Dados

Há também funções específicas de proteção de dados que devem ser desempenhadas por colaboradores internos. Essas funções são:

- Gestor de Segurança da Informação
- Gestores de Departamento e/ou Setores
- Funcionários e prestadores de serviços

5.2 Responsabilidades

Este tópico detalha as responsabilidades específicas, no âmbito da proteção de dados pessoais, de cada função dentro da estrutura do **HOSPITAL SANTA TERESINHA**.

5.2.1 Controlador de Dados

A LGPD define como Controlador a "*pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais*". Assim, as responsabilidades descritas abaixo podem ser atribuídas a um Controlador ou podem ser aplicadas à organização como um todo.

O Controlador de dados tem as seguintes responsabilidades:

- Assegurar que os princípios relativos ao processamento de dados pessoais descritos na LGPD sejam cumpridos e possam ser demonstrados. Em resumo, garantir que os dados pessoais sejam:
  - tratado de forma legal, justa e transparente;
  - coletado para fins específicos, explícitos e legítimos;
  - adequado, relevante e limitado ao necessário;
  - precisos e, quando necessário, atualizados; e
  - tratados com garantia de segurança apropriada.
- Garantir que o consentimento dos dados sujeitos ao tratamento seja obtido de forma apropriada, incluindo o consentimento dos pais para crianças e adolescentes;
- Fornecer toda informação necessária ao titular dos dados de forma concisa, transparente e de fácil acesso, usando linguagem clara e simples;
- Facilitar o exercício dos direitos dos titulares dos dados e mantê-los informados sobre seus pedidos;
- Implementar medidas técnicas e organizacionais apropriadas para garantir e demonstrar que o tratamento é realizado de acordo com a LGPD;
- Garantir que os operadores forneçam garantias suficientes para implementar medidas técnicas e organizacionais apropriadas para atender a LGPD e proteger os dados pessoais usados;
- Manter registro das atividades de tratamento relacionadas aos dados pessoais que são de responsabilidade do controlador;
- Cooperar com a autoridade fiscalizadora no desempenho de suas atividades;
- Notificar eventual violação aos dados pessoais para a autoridade fiscalizadora e o titular, exceto nos casos que não há risco aos direitos e liberdades das pessoas naturais, de acordo com os procedimentos internos;
- Documentar quaisquer violações aos dados pessoais, incluindo os fatos, seus efeitos e as ações corretivas aplicadas;
- Quando apropriado, comunicar a violação de dados pessoais ao titular conforme procedimento interno;
- Realizar avaliações do impacto da proteção de dados, conforme os procedimentos internos;
- Designar um encarregado na proteção de dados (DPO) e disponibilizar os dados de contato;
- Apoiar o encarregado da proteção de dados no desempenho de suas responsabilidades, fornecendo recursos necessários para que ele realize suas tarefas;

- Transferir dados pessoais para um país terceiro ou uma organização internacional, apenas se o responsável pelo tratamento ou o operador tiver fornecido as garantias adequadas e sob a condição de que os direitos do titular estarão protegidos.

5.2.2 Operador de Dados

A LGPD define como Operador a *"pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"*.

O Operador de dados tem as seguintes responsabilidades:

- Garantir que todo o tratamento de dados pessoais seja regido por um contrato que especifique o objeto, a duração, a natureza e a finalidade do tratamento, o tipo de dados pessoais e categorias de titulares dos dados e as obrigações do responsável controlador;
- Processar os dados pessoais apenas com instruções documentadas do responsável controlador, incluindo o que diz respeito a transferências de dados pessoais para um país terceiro ou uma organização internacional;
- Assegurar que as pessoas autorizadas a realizar o tratamento dos dados pessoais se comprometeram com a confidencialidade;
- Implementar medidas técnicas e organizacionais para garantir um nível de segurança adequado ao risco do tratamento de dados pessoais;
- Eliminar ou devolver todos os dados pessoais ao controlador após o final da prestação de serviços relacionados com tratamento de dados;
- Disponibilizar ao controlador todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas na LGPD, permitindo verificações, conduzidas pelo controlador ou por auditor contratado pelo controlador;
- Manter registro das atividades de tratamento realizadas em nome do controlador;
- Cooperar com a autoridade fiscalizadora no desempenho de suas funções;
- Assegurar que qualquer colaborador atuando em nome do operador e tenha acesso a dados pessoais realize o tratamento conforme as instruções do controlador;
- Notificar o controlador, logo que tomar conhecimento, de qualquer violação de dados pessoais;
- Designar um encarregado na proteção de dados (DPO) e disponibilizar os dados de contato;
- Apoiar o encarregado na proteção de dados no desempenho de suas tarefas, fornecendo recursos necessários e acesso a dados pessoais e operações de tratamento.

5.2.3 Encarregado de Dados (DPO)

O encarregado da proteção de dados é uma função descrita na LGPD e tem responsabilidades específicas.

O encarregado da proteção de dados tem as seguintes responsabilidades:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da autoridade nacional e adotar providências;
- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

5.2.4 Gestor de Segurança da Informação

O Gestor de Segurança da Informação tem as seguintes responsabilidades:

- Reportar para a diretoria e/ou administração todos os assuntos relacionados à segurança;
- Comunicar sobre política de segurança da informação a todas as partes interessadas, quando apropriado, incluindo clientes;
- Implementar os requisitos da política de segurança da informação;
- Garantir que os controles de segurança estejam corretos e documentados;
- Quantificar e monitorar os tipos, volumes e impactos de incidentes de segurança;
- Definir planos e metas de melhoria;
- Identificar e gerenciar incidentes de segurança da informação conforme procedimento específico.

5.2.5 Gestores de Departamento e/ ou Setor

Os gestores de departamento podem ser chefes ou supervisores de unidades operacionais dentro da organização.

Um gestor de departamento tem as seguintes responsabilidades:

- Revisar e gerenciar as competências dos funcionários e as necessidades de treinamento para permitir que desempenhem efetivamente suas funções na área de proteção de dados;
- Garantir que os funcionários estejam cientes da relevância e importância de suas atividades e de como eles contribuem para o alcance dos objetivos de proteção de dados;
- Participar e contribuir para as avaliações de impacto de proteção de dados que afetam sua área de negócios.

5.2.6 Funcionários e prestadores de serviços

As responsabilidades dos funcionários e prestadores de serviços são definidas em políticas internas. Resumidamente, possuem as seguintes responsabilidades principais:

- Cumprir todas as políticas de proteção de dados na sua atividade laborativa;

- Relatar qualquer violação de dados ou riscos de segurança da informação;
- Contribuir para a avaliação do impacto da proteção de dados quando necessário.

5.3 Responsabilidade Solidária

- O Controlador ou o Operador que, em razão do exercício de atividade de tratamento de informações pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de informações pessoais, é obrigado a repará-lo;
- O Operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o Operador se equipara ao Controlador;
- Os Controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente. Salvo, nos seguintes casos de exclusão, quando os agentes de tratamento só não serão responsabilizados quando provarem, conforme o Artigo 43 da LGPD:
    - Que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
    - Que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

6 Estruturação do Programa de Privacidade e Proteção de Dados Pessoais

Corresponde à criação e implementação da base para difusão de conhecimentos relacionados à cultura da privacidade e proteção de dados no **HOSPITAL SANTA TERESINHA**, com a elaboração, atualização e constante monitoramento da efetividade dos normativos que abordem o tema.

6.1 Nomeação do Encarregado de Dados Pessoais

O Encarregado de Dados Pessoais (DPO) é o responsável por orientar o **HOSPITAL SANTA TERESINHA** em suas operações de Tratamento de Dados Pessoais e por atuar como canal de comunicação entre o **HOSPITAL SANTA TERESINHA**, os Titulares e a ANPD.

O Encarregado poderá ser um funcionário (dedicado ou não), um terceiro contratado (seja pessoa física ou jurídica). Este profissional deverá ter uma visão ampla do risco associado às operações de Tratamento de Dados Pessoais considerando sua natureza, o contexto no qual está inserido e suas finalidades. Ainda, o Encarregado deverá manter o compromisso de sigilo e a confidencialidade em relação ao desempenho de suas atividades profissionais. O contato do Encarregado deve ser divulgado publicamente, de forma clara e objetiva, no facebook, instagram e site do **HOSPITAL SANTA TERESINHA**.

É dever do **HOSPITAL SANTA TERESINHA** registrar a nomeação do Encarregado, como no modelo em Anexo, e manter os dados do Encarregado sempre atualizados.

6.2 Treinamento e Conscientização

Todos os colaboradores e terceiros que atuam em nome do **HOSPITAL SANTA TERESINHA** receberão treinamento inicial sobre as diretrizes previstas na presente política e orientações constantes com atualizações e revisões, caso necessário.

A disseminação do assunto se dará por meio de ações de comunicação e campanhas institucionais, bem como treinamentos, cursos de capacitação, eventos e ferramentas de atualização periódica.

6.3 Comunicação e Transparência

6.3.1 Aviso de Privacidade

O Aviso de Privacidade, ou Política de Privacidade Externa, é a notificação dirigida ao Titular dos Dados. Este Aviso visa garantir que o Titular esteja ciente de que seus dados estão sendo tratados e que entendem:

a) como a organização coleta e/ou recebe os dados pessoais;
b) finalidade do tratamento;
c) tempo de retenção do dado;
d) identificação do Controlador;
e) contato do Encarregado pelos dados pessoais (DPO);
f) informações acerca do compartilhamento e a finalidade;
g) responsabilidades dos agentes que realizarão o tratamento; e
h) direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

6.3.2 Formulário para o exercício de direito

O **HOSPITAL SANTA TERESINHA** terá disponível formulário específico para recebimento das solicitações dos direitos do titular. Neste formulário, constarão orientações de como proceder o envio da solicitação.

Para cada solicitação recebida, deve-se, obrigatoriamente, efetuar a verificação da identidade do Titular dos dados. Cabe à organização determinar as melhores práticas para confirmar a autenticidade das informações contidas na solicitação.

6.4 Política de Privacidade

A Política de Privacidade e Proteção de Dados Pessoais é uma norma interna da organização que tem por objetivo informar aos funcionários, terceirizados, parceiros e outros interessados, como a organização trata dados pessoais. Estabelece a legislação relevante e descreve as atitudes adotadas para garantir sua conformidade com a LGPD e proteger todos os dados pessoais que lhe é confiado em decorrência de suas atividades.

A Política de Privacidade e Proteção de Dados Pessoais contém as seguintes diretrizes:

a) Finalidade e base Legal para o tratamento dos dados pessoais;
b) Tarefas do encarregado de dados pessoais (DPO);
c) Registro das atividades de tratamento (Data Mapping);
d) Direitos do Titular; e
e) Transferência Internacional.

6.4.1 Retenção de Dados Pessoais (ciclo de vida)

Os dados pessoais serão tratados durante o período necessário para atingir os objetivos pelos quais foram coletados.

Ciclo de vida dos dados pessoais:

- tratamento necessário para a execução de contrato:
  - tratamento inicia na negociação (pré-contrato) até a data de rescisão do contrato e, em seguida, por período exigido pela legislação pertinente;
- tratamento necessário para o cumprimento de uma obrigação legal:
  - tratamento inicia quando tais obrigações forem cumpridas e permanece por período exigido pela legislação pertinente;
- tratamento baseado no consentimento explícito do titular:
  - tratamento inicia imediatamente após confirmado o consentimento e permanece até o período previsto para atingir o objetivo ou até a revogação do consentimento pelo Titular, exceto quando o tratamento tenha se enquadrado na hipótese de obrigação legal. Neste caso, permanece por período exigido pela legislação pertinente;
- tratamento necessário para o cumprimento os interesses legítimos:
  - tratamento inicia na negociação, permanece por período previsto ou até o momento em que o Titular se oponha ao tratamento. A oposição ao tratamento só não será acatada quando o tratamento for essencial e não violar os direitos fundamentais de liberdade e privacidade da pessoa natural;
- tratamento necessário para o cumprimento das demais hipóteses descritas nas Seções II e III da LGPD:

- tratamento inicia quando tais obrigações forem cumpridas e permanecem por período exigido nas regulamentações e legislações pertinentes, ou até período previsto para cumprimento de interesses legítimos, desde que tenha respaldo lícito e que não viole os direitos fundamentais de liberdade e privacidade da pessoa natural.

6.5 Termos e Contratos

6.5.1 Adequação de Contratos

Os contratos, bem como os termos de uso, devem conter cláusulas que os adequem aos princípios e regras da LGPD. As cláusulas devem dispor, de modo transparente, o que segue:

a) As responsabilidades das partes;
b) Quais dados estão sendo tratados;
c) Sensibilidade dos dados envolvidos;
d) Descrição do tratamento, bem como finalidade e temporalidade;
e) Categoria dos dados envolvidos;
f) Medidas de segurança da informação;
g) Compartilhamento; e
h) Transferência internacional de dados.

As negociações do **HOSPITAL SANTA TERESINHA**, das quais envolvam o tratamento de dados pessoais, estarão sujeitos a contrato ou acordo documentado com inclusão das informações e termos específicos exigidos pela LGPD. Para mais informações, consultar a Política de Contrato.

6.5.2 Termo de Confidencialidade

Todo indivíduo que, por qualquer função ou finalidade, coletar dados pessoais em nome do **HOSPITAL SANTA TERESINHA**, acessar, usar ou efetuar qualquer outro tratamento de dados pessoais, deverá assinar o termo de confidencialidade contendo cláusulas específicas de proteção de dados pessoais.

6.6 Código de Conduta

Todos os colaboradores e terceiros que atuam em nome do **HOSPITAL SANTA TERESINHA** deverão ter acesso ao Código de Conduta e agir conforme cultura e ética da organização.

6.7 Política de Segurança da Informação (PSI)

O **HOSPITAL SANTA TERESINHA** mantém um conjunto de padrões, normas e diretrizes para o uso correto da infraestrutura de TI (Tecnologia da Informação) da organização. Tem como objetivo garantir a proteção das informações contra eventuais ameaças que possam prejudicar sua operação.

Buscando garantir a confidencialidade, a integridade, a disponibilidade da informação e impedir o acesso não autorizado, como apoio a PSI, o **HOSPITAL SANTA TERESINHA** possui outras políticas que devem ser lidas em conjunto, das quais são, mas não se limitam a:

a) Política de Acesso à Internet;
b) Política de Uso de Dispositivos de Tecnologia;
c) Política de Mensagens Eletrônicas; e
d) Política de Gestão de Riscos.

Todas as políticas devem estar em local disponível e de fácil acesso para que todos os funcionários e prestadores de servoços possam visualizar sempre que necessário.

7 Riscos de Segurança e Privacidade

7.1 Gestão de Riscos

Para manter o controle em relação às ameaças de acessos não autorizados, o **HOSPITAL SANTA TERESINHA** utiliza a política de Gestão de Riscos, o qual consiste na identificação, avaliação, tratamento e monitoramento das vulnerabilidades e dos riscos de ocorrência de incidentes de violação de proteção de dados pessoais.

7.2 Metodologia de Gestão de Risco para Proteção de Dados Pessoais

A metodologia utilizada é baseada em elementos fundamentais de segurança da informação, riscos e privacidade de dados. De uma forma integrada, esses elementos visam identificar e avaliar os dados pessoais, os seus pontos de vazamento e os mecanismos de segurança, que são os objetos da LGPD.

7.2.1 Elementos Fundamentais

A metodologia de gestão de riscos para proteção de dados pessoais considera os seguintes elementos como fundamentais:

a) Lista de ativos da organização;
b) Quais dados são tratados pela organização e, destes, quais são dados pessoais;
c) Quem insere e quem consome os dados;
d) Quais os componentes (tecnológicos ou não) pelos quais os dados são processados, transmitidos ou armazenados;
e) Quais artefatos de base legal e regulatória estão sendo utilizados;
f) Quais os controles de segurança que estão sendo utilizados para proteger os dados pessoais;
g) Quais os pontos de potenciais vazamentos dos dados pessoais;
h) Quais as ameaças que podem levar a incidentes de segurança;
i) Quais os agentes de ameaça que podem explorar vulnerabilidades dos componentes;
j) Quais vulnerabilidades que podem ser exploradas pelos agentes de ameaça;
k) Quais os impactos relacionados à privacidade dos titulares dos dados;
l) Quais as probabilidades de vazamentos de dados pessoais.

7.3 Fases da Metodologia

A metodologia é composta por três fases principais, descritas a seguir:

a) Identificação do fluxo de dados pessoais;
b) Análise de gap e riscos, a partir do fluxo de dados pessoais;
c) Estratégia de adequação à LGPD de acordo com os resultados da análise de gap e riscos.

8 Resposta à Incidente

O **HOSPITAL SANTA TERESINHA** atuará de forma justa e proporcional, considerando as ações a serem tomadas para informar as partes afetadas com relação a violações de dados pessoais. Isso será alinhado de acordo com o Procedimento de Resposta a Incidentes de Segurança.

O Procedimento de Resposta a Incidentes de Segurança deverá conter, no mínimo, o que segue:

- descrição do incidente;
- a quem deve ser comunicado;
- medidas a serem tomadas; e
- atividade pós-incidente.

8.1 Ocorrência de Incidente

Quando detectado incidente envolvendo dados pessoais, o **HOSPITAL SANTA TERESINHA** deverá:

- avaliar o incidente (natureza do dado, categoria e quantidade de titulares afetados, local de armazenamento);
- avaliar as consequências concretas e prováveis;
- comunicar o encarregado de dados pessoais (DPO);
- quando estiver agindo como Operador, comunicar o Controlador; e
- relatar as medidas tomadas juntamente com a análise de risco.

Na ocorrência de uma violação que possa **resultar em um risco para os direitos e liberdades dos indivíduos**, o titular receberá o comunicado conforme Procedimento de Resposta a Incidentes de Segurança e a autoridade fiscalizadora (ANPD) será informada, em **até 2 dias úteis**, mediante instruções disponibilizadas no link https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

8.2 Relatório de Impacto à Proteção de Dados pessoais

Quando detectado tratamento que possa **impactar fortemente os direitos e liberdades dos indivíduos**, especialmente quando **embasado no interesse legítimo**, será realizada uma avaliação do impacto da proteção de dados (Data Protection Impact Assessment - DPIA).

A construção do relatório parte do detalhamento de todos os processos de tratamento pelos quais os dados pessoais passam durante o seu ciclo de vida nas operações realizada pelo **HOSPITAL SANTA TERESINHA**, assim como, das bases legais necessárias e as medidas de segurança adotadas. Essas informações estarão identificadas no data mapping e, após análise, permitirá identificar os pontos de fragilidade da operação que podem representar algum risco aos direitos dos titulares dos dados. Tão logo efetuada a avaliação dos riscos, serão identificadas as medidas necessárias para a sua contenção, que deverão ser implementadas e testadas.

O **HOSPITAL SANTA TERESINHA** utiliza o DPIA para melhor visualizar e compreender sua operação, de modo a evitar excessos e adotar as soluções e medidas mais apropriadas no contexto de privacidade e de proteção de dados. Elaborá-lo concomitantemente com a estruturação da operação, ou mesmo antes dela, assegurará desde cedo que todos os requisitos legais serão cumpridos, o que colabora com o cumprimento de um importante dever estabelecido pela LGPD: a adoção de medidas protetivas à privacidade e segurança dos dados desde a concepção do produto ou serviço, conceito conhecido como Privacy by Design.

8.3 Privacy by Design

O **HOSPITAL SANTA TERESINHA** adota os princípios do Privacy by Desing, os quais consistem na proteção da privacidade e dos dados pessoais, em todos os projetos desenvolvidos. Não é permitido desenvolver nenhum projeto, produto ou serviço, sem que a proteção da privacidade esteja no

centro desse desenvolvimento, incluindo a realização de uma ou mais avaliações de impacto da proteção de dados.

A avaliação do impacto na proteção de dados incluirá:

- Consideração de como os dados pessoais serão processados e com quais objetivos;
- Avaliação se o tratamento de dados pessoais proposto é necessário e proporcional ao(s) objetivo(s);
- Avaliação dos riscos para os indivíduos no tratamento de dados pessoais;
- Quais são os controles necessários para abordar os riscos identificados e demonstrar conformidade com a legislação.

Esta política deverá ser revisada periodicamente e atualizada mediante mudanças dos processos internos do **HOSPITAL SANTA TERESINHA**.

ANEXO

Braço do Norte, __ de _____ de 2021

Nomeação do Encarregado de Proteção de Dados Pessoais

Na presente data, designamos o(a) _____ como Encarregado(a) pelo Tratamento de Dados Pessoais (DPO) do **HOSPITAL SANTA TERESINHA**. Com vigência imediata, o DPO atuará como canal de comunicação com os Titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), nos termos do Art 5º, VIII, da LGPD.

O DPO tem como principal função orientar o **HOSPITAL SANTA TERESINHA** em suas operações de Tratamento de Dados Pessoais, além de auxiliar no aprimoramento da nossa Política de Privacidade. Entre as principais atividades a serem desempenhadas pelo Encarregado, deverá:

(i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
(ii) receber comunicações da autoridade nacional e adotar providências;
(iii) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
(iv) executar as demais atribuições determinadas pelo hospital ou estabelecidas em normas complementares.

Atenciosamente,

Responsável Legal do Hospital

Carimbo e Assinatura