S.P.A. Saúde

O Plano de Saúde do Produtor Rural

POLÍTICA GERAL DE PRIVACIDADE E PROTEÇÃO DE DADOS

INTERNA

Controle e Aprovação

RESPONSÁVEL		VER	CARGO
ELABORADO	Toro e Advogados Associados CNPJ 03.777.369/0001-01	00	Assessoria Jurídica
REVISADO	Comitê Executivo Interno	00	Diversos
APROVADO	Denilson Luciano – Encarregado de Dados	00	Gerente Técnico Operacional

Sumário

1. Introdução

Esta Política é destinada a todos os colaboradores, associadas e prestadores de serviços do S.P.A. Saúde, e tem por objetivo orientar nossos departamentos internos e parceiros de negócio quanto aos procedimentos e controles adotados pela Entidade para proteção dos dados pessoais que tratamos em decorrência da nossa atividade, na qualidade de Controlador de Dados Pessoais e de Dados Pessoais Sensíveis, para assegurar que o tratamento desses dados seja realizado em conformidade com à LGPD.

Destacamos que é nosso compromisso indelegável a privacidade e proteção dos dados pessoais que tratamos em respeito ao titular dos dados, de modo que, qualquer tratamento realizado pela Entidade respeitará a finalidade a que se destina e estará fundamentado em uma base legal legítima.

2. Sua Privacidade

Em razão da atividade que exercemos como Plano de Saúde, somos submetidos às disposições existentes na Lei nº. 9.656, de 1998, que rege os planos e seguros privados de assistência à saúde, e demais legislações correlatas, como por exemplo, as Resoluções Normativas editadas pela Agência Nacional de Saúde Suplementar – ANS, especificamente no que concerne à proteção de suas informações. Temos que observar, dentre outras, as Resoluções Normativas nº. 117, de 2005, a nº. 305, de 2012 e a nº. 389, de 2015, pois são instrumentos de regulação utilizados pela ANS e que afetam diretamente forma como tratamos seus dados pessoais.

Vale dizer que, existem diversas outras normas voltadas às áreas trabalhista, empresarial, tributária, e sanitária, por exemplo, que podem vir a fundamentar o objeto principal da nossa relação com nossos colaboradores(as) e outros profissionais que estão vinculados de alguma maneira ao S.P.A. Saúde.

3. Coleta e Tratamento de Dados de Colaboradores e Profissionais terceirizados e/ou autônomos

Com relação a nossos colaboradores, nossa Entidade só coleta os dados necessários para fins de viabilizar nossa relação junto a você, sendo que, na maior parte das vezes, o processamento de dados está atrelado a relação contratual estabelecida e as obrigações legais dela decorrentes.
Pode ser necessário o fornecimento ou acesso desses dados por colaboradores ou prestadores terceirizados, entretanto, se o caso, será feito dentro da finalidade supracitada.

No caso dos profissionais terceirizados e ainda, aqueles contratados de modo autônomo para prestação de serviços junto a Entidade, o contrato existente entre as partes ajustará a responsabilidade das partes à LGPD.

4. Governança de Privacidade

4.1. Programa de Privacidade

O S.P.A. Saúde adota um Programa de Privacidade administrado pela Equipe de Privacidade e liderada pelo Encarregado de Proteção de Dados, para gerir os procedimentos e controles de privacidade.
Para uma governança adequada do Programa de Privacidade, são realizadas as seguintes ações:

a) Definição da estratégia e diretrizes da Entidade com relação ao tema privacidade.
b) Adoção de uma estrutura de governança e forma de atuação para o Encarregado de Dados e Comitê de Privacidade, considerando independência suficiente de maneira que as tomadas de decisão não sejam afetadas por outras questões da organização.
c) Reunião do Comitê de Privacidade para analisar as necessidades do S.P.A. Saúde e quais iniciativas relacionadas a atividades de tratamento de dados devem ser tomadas, bem como

coordenar a implementação de diretrizes definidas pela Diretoria da Entidade, reportando temas relevantes periodicamente.

d) Revisões periódicas dos controles relacionados ao risco de descumprimento das obrigações pertinentes à proteção de dados, cujos reportes periódicos são feitos ao Encarregado, que é responsável por comunicar a Diretoria da Entidade.

e) Realização de auditorias de conformidade.

Destacamos que você, enquanto colaborador, associado e/ou parceiro de negócio do S.P.A. Saúde, tem a obrigação de adotar medidas básicas de proteção contra acessos não autorizados às suas senhas e aparelhos eletrônicos.

4.2. Encarregado de Proteção de Dados

O Encarregado de Proteção de Dados, nomeado pelo S.P.A. Saúde, atua como canal de comunicação entre a Entidade, os Titulares dos dados e a ANPD (Autoridade Nacional de Proteção de Dados).
As formas de contato com o Encarregado estão devidamente publicadas no site do S.P.A. Saúde (http://www.spasaude.org.br/site/), de forma clara e transparente ao público interno e externo. Suas atribuições e responsabilidades estão descritas no manual elaborado pela Entidade e disponível para consulta.

4.3. Comitê de Privacidade

O Comitê de Privacidade é estruturado por uma equipe multidisciplinar coordenada pelo Encarregado de Proteção de Dados e possui membros de áreas estratégicas do S.P.A. Saúde responsáveis por conduzir os processos de privacidade e auxiliar o Encarregado em suas demandas e atribuições. A composição do Comitê de Privacidade pode ser revista a qualquer momento, em razão do volume ou complexidade das demandas.

4.4. Auditoria Interna e Externa

O S.P.A. Saúde adota processos para avaliação do seu Programa de Privacidade, através da a realização de auditorias periódicas.

A periodicidade para realização da auditoria interna e independente observará eventuais previsões legais e os interesses da Entidade em gerir o Risco inerente ao tratamento de dados realizado.

4.5. Gestão de Riscos e mecanismos de Controle

O S.P.A. Saúde possui controles para aferir o risco de suas atividades de tratamento de dados, de modo que atrelados as atividades realizadas pela Entidade possibilitam avaliar e mitigar riscos inerentes ao tratamento de dados.

São mecanismos de controle de Riscos, respectivamente:

- Avaliação de Riscos (Relatório de Impacto a Proteção de Dados e Avaliação de Interesse Legítimo)
- Conscientização e Treinamento
- Gestão de Bases Legais
- Gestão de Consentimento
- Gestão de Controles de Segurança da Informação (análise de vulnerabilidades, gestão de incidentes, logs e registros de atividades, gestão e revisão de acessos, pseudonimização/anonimização e segregação de ambientes)
- Gestão de Retenção de Dados
- Gestão da relação com terceiros (processos de *due diligence* voltados a proteção de dados e cláusulas contratuais voltadas a proteção de dados)
- Gestão Direitos dos Titulares
- Gestão do Inventário de Processamento (ROPA)
- Gestão do programa de privacidade

- Monitoramento e Resposta a Incidentes de Segurança
- Políticas, Processos e Procedimentos de Governança
- *Privacy by Design*

5. Governança dos Processos de Privacidade

5.1. Gestão de Fluxos de Tratamento e Bases Legais

Para gestão do fluxo de tratamento de dados, o S.P.A. Saúde realiza atualização constante do inventário de processamento (ROPA) para todo novo produto, serviço, projeto que realize o tratamento de dados pessoais e sensíveis na organização.
Ainda, há um processo de revisão periódica do inventário de processamento de dados (ROPA) para avaliar se o uso do dado está adequado às finalidades propostas e se as atividades mapeadas possuíram alterações relevantes.

I. Ainda, periodicamente são revisados os tipos de dados coletados para avaliar se não excedem o tratamento necessário para a execução de determinado fluxo de tratamento de dados, visando o princípio da minimização conforme a LGPD.
II. Revisão periódica dos inventários de processamento garantindo a avaliação dos fluxos de dados para o enquadramento de bases legais com o objetivo de fundamentar os tratamentos de dados de acordo com as finalidades a que se destinam.

5.2. Gestão e Avaliação de Riscos de Privacidade

Como parte do Processo de avaliação de impacto à privacidade utilizamos o Relatório de Impacto à Proteção de Dados Pessoais, que será aplicado do seguinte modo:

I. Ao identificar um novo produto, serviço, projeto ou processo que realize o tratamento de dados pessoais os gestores responsáveis devem preencher o formulário PIA (Avaliação de Impacto a Privacidade), para avaliação de riscos de privacidade no novo produto, serviço, projeto ou processo.

II. Uma vez que, o Questionário PIA (Avaliação de Impacto de Privacidade) seja preenchido com a avaliação de riscos, qualquer processo classificado pelo Encarregado de Proteção de Dados como risco "Alto", o gestor responsável deve preencher também o questionário complementar DPIA (Avaliação de Impacto da Proteção de Dados).

III. O documento preenchido possibilitará avaliar com maior precisão os riscos inerentes a atividade pretendida, permitindo a Entidade decidir como proceder.

IV. Finalizada a avaliação, o documento permanecerá arquivado junto ao S.P.A. Saúde, podendo ser solicitado pela Autoridade Nacional de Proteção de Dados (ANPD) a qualquer momento.

Realizamos a Avaliação de Interesse Legítimo como processo de avaliação para que seja possível classificar se uma determinada atividade de tratamento de Dados Pessoais pode ser classificada na base legal de legítimo interesse.

O documento utilizado para esta análise é o um formulário denominado LIA (Avaliação de Interesse Legítimo), que contempla:

- Teste da Finalidade: Descrição das operações de tratamento de Dados Pessoais e as suas finalidades;

- Teste da Necessidade: Avaliação da necessidade e da proporcionalidade do tratamento de Dados Pessoais em relação à finalidade pretendida em detrimento do ao impacto sobre o Titular dos dados pessoais;

- Teste do Balanceamento: Avaliação de relação dos interesses da Entidade ou de terceiros com os interesses, direitos e liberdades do Titular;

6. Segurança da Informação

O S.P.A. Saúde possui definida em sua Política de Segurança da Informação quais as diretrizes e procedimentos relativos à segurança da informação adotados pela Entidade e que deverão ser tidos como parâmetro de conduta dos Colaboradores.

O referido documento descreve quais são as medidas técnicas adotadas pela Entidade, no que concerne a segurança da informação, para impedir o acesso não autorizado, perda ou destruição de dados por terceiros.

7. Retenção de Dados

Para garantir a utilização dos dados pessoais de acordo com o tempo necessário e finalidade, possuímos uma Manual de Retenção e Descarte, que descreve o processo de retenção de dados instituído visando garantir a guarda e armazenamento de documentos físicos e eletrônicos pelo tempo determinado na tabela de temporalidade, obedecendo os parâmetros legais que justifiquem o tempo de armazenamento.

8. Gestão e Notificação de Incidentes

O S.P.A. Saúde possui um processo para identificação, tratamento e reporte de incidentes de segurança da informação que envolvam dados pessoais, que é coordenado pelo Encarregado de Proteção de Dados, que conjuntamente com o Comitê de Privacidade e demais setores que se fizerem necessários, avaliará a relevância do incidente para comunicação à ANPD e o Titular dos dados.

9. Gestão de Risco para Terceiros

O S.P.A. Saúde adota controles relacionados à proteção de dados pessoais em seus processos de gestão de riscos de terceiros como fornecedores e prestadores de serviço. Por meio do Questionário de Avaliação de Terceiros, onde avaliamos os controles de proteção de dados e segurança da informação adotados por terceiros que pretendemos firmar uma relação jurídica onde existirá o tratamento de dados pessoais.

10. Gestão de Consentimento.

O S.P.A. Saúde adota um processo de gestão de consentimento com o objetivo de mitigar riscos relacionados ao tratamento de Dados Pessoais e Dados Pessoais Sensíveis associados a esta base legal.

11. Direitos do Titular

A Lei Geral de Proteção de Dados estabelece ao titular dos dados pessoais, os seguintes direitos:

I - Confirmação da existência, acesso e correção de dados incompletos, inexatos ou desatualizados;
II - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
III - Portabilidade dos dados a outro fornecedor de serviço ou produto, conforme regulamentado pela Autoridade Nacional de Proteção de Dados – ANPD;
IV - Eliminação dos dados pessoais tratados com o consentimento do titular, nos moldes da lei.
V - Informação das entidades públicas e privadas com as quais realizamos uso compartilhado de dados;
VI - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

VII - Revogação do consentimento, se o caso.

Permitiremos o acesso e as alterações solicitadas, observando a forma e prazos estabelecidos, a menos que haja um motivo, de acordo com o LGPD ou outra regulação específica, para recusarmos ou alterarmos os dados solicitados.

12. Privacidade por padrão e desde a concepção

O S.P.A. Saúde possui um recurso para avaliação dos requisitos de segurança e privacidade de novos projetos, sistemas, produtos e serviços que utilizam dados pessoais seguindo os conceitos de Privacidade por padrão e desde a concepção, que determinam que as medidas acerca do tema de privacidade sejam consideradas desde a fase de concepção do produto ou serviço, até a sua execução e que tenham como conduta padrão a privacidade do titular de dados.

13. Treinamento

O programa de capacitação de colaboradores do S.P.A. Saúde leva em consideração treinamentos relacionados à segurança da informação, privacidade e proteção de dados considerando as exigências da Lei Geral de Proteção de Dados (LGPD).

Além disso, todo novo Colaborador receberá treinamento voltado a proteção de dados e privacidade e serão realizados os treinamentos de reciclagem ao menos uma vez ao ano.

Você pode solicitar mais informações e exercer seus direitos entrando em contato com nosso Encarregado de Proteção de Dados - EPD através dos seguintes canais:

- Canal de atendimento - (11) 3146-3131
- E-mail - lgpd@spasaude.org.br