1 OBJETIVO

Estabelecer diretrizes de orientação para o tratamento da informação em relação à privacidade dos dados pessoais dentro da organização, em conformidade com os princípios e fundamentos da 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

2 ESCOPO

Toda informação privada relacionada ao tratamento dos dados pessoais dentro da organização.

3 DEFINIÇÕES

- **Bases legais:** são as hipóteses previstas na LGPD que permitem a PREVIG a realizar o tratamento dos dados pessoais, tais como, consentimento, obrigação legal ou regulatória, execução de contrato, dentre outras.
- **Controlador (PREVIG):** pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dado pessoal;
- **Dado pessoal (DP):** informação relacionada a pessoa natural identificada ou identificável;
- **Dado pessoal de criança e adolescente:** dado referente a pessoa de até 12 anos incompletos (criança) e pessoa entre doze e 18 anos de idade (adolescente).
- **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;
- **Encarregado de proteção de dados:** pessoa física ou jurídica nomeada 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);
- **Lei Geral de Proteção de Dados Pessoais (LGPD):** lei que estabelece a proteção dos direitos fundamentais de liberdade e privacidade do titular de dados acerca do tratamento de dados pessoais por pessoa física ou jurídica, de direito público ou privado;
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais do titular, de acordo com as instruções do controlador. Ex: Fornecedores;
- **SGSI:** Sistema de gestão de segurança da informação.
- **Sub-operador:** Pessoa física ou jurídica designada pelo Operador para operar Dados Pessoais em nome do Controlador;
- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Ex: Participantes e Colaboradores;
- **Tratamento:** toda operação realizada com dado pessoal, tais como, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

4 REFERÊNCIAS

- Norma ISO 27001:2013;
- Lei 13.709/2018 (“Lei Geral de Proteção de Dados Pessoais – LGPD”);
- Lei 8.069/1990 (“Estatuto da Criança e do Adolescente – ECA”).

5 PRINCÍPIOS

Os princípios de privacidade norteiam os nossos processos de negócios, onde nossa informação e dos nossos participantes deve ser tratada com cautela, obedecendo os princípios de segurança da informação estabelecidos nos objetivos estratégicos da organização.

A Lei Geral de Proteção de Dados define os seguintes princípios para o tratamento de informações relacionadas a dados pessoais e devem ser seguidos nesta política:

- **Finalidade e adequação:** todos os processos da organização que realizarem tratamento de dados pessoais devem possuir finalidades específicas, explícitas e legítimas, não podendo a informação privada ser tratada, posteriormente, de maneira incompatível com tais finalidades. Quando houver mudança na finalidade do tratamento dos dados pessoais, o processo em questão deve ser adequado para atender as novas finalidades e o titular devidamente notificado, conforme o **FOR RH 003 – Comunicações do SGSI e Privacidade.**
- **Necessidade:** o tratamento dos dados pessoais deve se limitar ao mínimo necessário para ao atendimento da finalidade determinada, coletando e utilizando tão somente, os dados estritamente necessários. Os dados pessoais coletados de forma excessiva e sem finalidade determinada, devem ter seu tratamento interrompido, e obedecer ao processo de descarte estabelecido na **PSI 018 – Procedimento de Descarte da Informação.**
- **Livre acesso e transparência:** o Titular dos dados pessoais tem direito de acessar suas informações, de forma clara, gratuita e facilitada, sobre a forma e a duração do tratamento dos seus dados pela organização. O atendimento às solicitações do Titular será realizado através do formulário de requisição instituído no website da PREVIG.
- **Qualidade dos dados:** o uso dos dados pessoais do Titular deve ser realizado com exatidão clareza, relevância, onde os dados devem ser atualizados ou corrigidos, sempre que possível, de acordo com a necessidade e finalidade do uso das informações pela organização.
- **Segurança e prevenção:** todo o tratamento realizado com dados pessoais deve ser pautado em medidas técnicas, administrativas e preventivas adotadas pela organização para a proteção da informação de eventuais danos durante o tratamento.
- **Não discriminação:** o uso de dados pessoais deve ser feito de forma lícita e legítima, sendo vedado qualquer tipo de tratamento com o objetivo de discriminar o Titular de dados ou para realização de práticas ilícitas ou abusivas.
- **Responsabilização e prestação de contas:** deve ser observada a adoção de medidas eficazes capazes de comprovar o cumprimento das exigências da LGPD e sua eficácia no uso da informação privada. As informações sobre o uso da informação privada pela organização estão listadas na **Avaliação de impacto de privacidade**.

6 RESPONSABILIDADES

O Gestor de Tecnologia tem a responsabilidade do pleno suporte para planejamento, execução e melhoria contínua do sistema de gestão de segurança e privacidade da informação. Ele é o guardião das políticas que orientam os processos da organização e deve patrocinar o seu desenvolvimento. Em caso de denúncia de incidentes de segurança e/ou privacidade da informação, o Gestor de Tecnologia deve avaliar as mudanças do SGSI que mitiguem os riscos apresentados pela denúncia.

7 TRATAMENTO DE DADOS PESSOAIS

7.1 Uso de Dados Pessoais:

A utilização dos dados pessoais dentro dos processos organizacionais deve ser pautada por ao menos uma das bases legais abaixo informadas:

- **Consentimento** – O uso dos dados pessoais deve ser precedido de um consentimento explicito e específico, e/ou da ciência do Titular de dados nos acordos estabelecidos. Ex: contratos de trabalho de colaboradores, termo de adesão de participantes, formulários de contato no website da organização etc.
- **Obrigação legal** – O uso dos dados pessoais pode estar fundamentado em legislação ou normas regulatórias que exigem o tratamento de dados pela organização, independente de consentimento do Titular de dados. Essas exigências podem incidir em sanções administrativas e judiciais quando não cumpridas. Ex: leis trabalhistas, previdenciárias, tributárias, normas de órgãos regulatórios (PREVIC, Receita Federal, Ministério do Trabalho, Previdência Social etc.);
- **Execução de Contrato** – O uso de dados pessoais pode ser realizado em razão do cumprimento de obrigações estabelecidas nos contratos firmados pela organização, dos quais o Titular de dados seja parte. Ex: contrato de trabalho, termo de adesão de plano previdenciário.
- **Exercício regular de direitos** – Nos casos em que houver determinação advinda de processo judicial, administrativo ou arbitral emitida por autoridade judicial ou por qualquer autoridade competente ligada à órgãos da administração pública (INSS, PREVIC, Receita Federal, Ministério do Trabalho, Previdência Social etc.), que exija o tratamento dos dados pessoais pela organização, o uso dos dados pode ser realizado, independente de consentimento do Titular de dados. Ex: intimações, mandados, decisões judiciais ou de órgãos da administração pública.
- **Legítimo interesse** – O uso dos dados pessoais pode ser realizado para apoio e promoção das atividades da empresa, tais como, o oferecimento de serviços/produtos e prospecção de clientes, desde que coletados os dados estritamente necessários para o cumprimento das finalidades as quais se propôs sua utilização. Ex: oferecimento de plano previdenciário para não participantes, disponibilização de formulários de contato no website da organização etc.

Toda a forma de tratamento de dados pessoais nos processos da organização deve ser justificada de acordo com as finalidades determinadas e informadas ao Titular nos acordos firmados, independente da base legal da base legal que justifica o seu tratamento.

7.2 Acesso a Dados Pessoais:

Todos as informações privadas devem ser tratadas com segurança, a fim de garantir que nos acordos estabelecidos, sejam observados os princípios legais, aos quais a organização está sujeita.

O acesso aos dados pessoais deve obedecer aos princípios indicados na política de segurança da informação, onde se determina o conceito de **"CONCESSÃO DE ACESSO"**, com o objetivo de estabelecer que cada processo obtenha as informações necessárias para suas atividades.

O Titular de dados deve ter acesso aos seus dados pessoais, através do seu cadastro na área do participante ou por meio de solicitação no formulário de requisição no website da PREVIG, devendo o atendimento a sua solicitação ser devidamente documentada.

7.3 Dados pessoais sensíveis

O tratamento de dados pessoais considerados sensíveis pela organização, tais como dados referentes a saúde, dados biométricos e demais situações previstas no **Art. 5º, II da LGPD**, deve observar uma das bases legais abaixo informadas:

- **Consentimento –** o uso de dados pessoais sensíveis deve ser precedido de consentimento do titular de dados, com finalidades específica e destacada nos acordos realizados pela organização. Ex: Termo de adesão de participantes, contratos com colaboradores.
- **Obrigação legal –** o uso de dados pessoais sensíveis pode ser fundamento em leis ou normas regulatórias que exigem o tratamento de tais dados pela organização, independente de consentimento. As exigências podem incidir em sanções judiciais ou administrativas, se não cumpridas. Ex: leis trabalhistas, previdenciárias, normas de órgãos regulatórios etc.
- **Execução de contrato –** o uso de dados pessoais sensíveis pode ser realizado em razão da execução das obrigações previstas em contrato do qual o titular de dados seja parte, independente de consentimento do Titular. Ex: Termo de adesão de plano previdenciário, contrato de trabalho etc.
- **Exercício regular de direitos -** nos casos em que houver determinação advinda de processo judicial, administrativo ou arbitral emitida por autoridade judicial ou por qualquer autoridade competente ligada à órgãos da administração pública (INSS, PREVIC, Receita Federal, Ministério do Trabalho, Previdência Social etc.), que exija o tratamento dos dados pessoais sensíveis pela organização, o uso dos dados pode ser realizado, independente de consentimento do Titular de dados. Ex: intimações, mandados ou decisões judiciais ou de órgãos da administração pública.

Todo uso de dado pessoal sensível pela organização deve ter finalidade específica e devidamente informada ao Titular de dados nos acordos estabelecidos, independente da base legal de tratamento que justifica o seu tratamento.

É vedada a utilização de dados pessoais sensíveis, fundamentado apenas no **legítimo interesse** da organização.

7.4 Dados pessoais de criança ou adolescente:

O uso de dados pessoais de menores de 18 anos pela organização deve seguir os seguintes critérios:

- **Autorização dos pais ou representante legal –** o tratamento de dados pessoais de menores deve ser precedido de autorização específica e destaca por pelo menos um dos pais ou pelo responsável legal do menor, nos termos do § 1º do artigo 14 da LGPD.
- **Obrigação legal ou execução de contrato –** o uso dos dados pessoais de menores deve estar fundamento em legislação ou normas regulatórias que exijam a coleta de tais dados pela organização ou em razão do cumprimento de obrigações estabelecidas nos contratos firmados. Ex: lei trabalhistas, fiscais, previdenciárias, normas de órgãos regulatórios ou obrigações estipuladas em contratos de trabalho e/ou termo de adesão de plano previdenciário.

Todo uso de dados pessoais de menores de 18 anos deve possuir finalidade determinada e informada a um dos pais ou ao representante legal nos acordos estabelecidos.

7.5 Controles utilizados

Todo o tratamento de dados pessoais privada deve ser controlado para mitigar os riscos de vazamento de informação e uso indevido. Os controles devem atender os requisitos:

- **Segregação** – O dado pessoal deve ser segregado pelo processo sistêmico da organização levando em consideração os princípios da política de segurança da informação. A segregação deve ser obtida por controle de acesso ao processo. Esse controle deve ser capaz de dividir em grupos específicos para organizá-los em departamentos/unidades/pastas/módulos entre outros, que contenham necessidades de separação entre um grupo e outro.
- **Auditoria** – Os sistemas/processos que contêm dados pessoais devem ser auditados regularmente para aferir a qualidade de seus controles.
- **Inventário** – Deve-se manter inventário de uso de dados pessoais dentro da organização que mapeiam todos os sistemas e processos que tratam da informação. Os itens a serem observados identificam claramente o uso da informação na empresa. Esse inventário deve ser atualizado regularmente.
- **Cópias de segurança** – Todos os dados devem ser protegidos de perdas lógicas dos sistemas, desta forma deve ser possível recuperar todos os dados pessoais dentro do seu ciclo de vida através de processo de recuperação de arquivos.
- **Riscos** – Com base no inventário de dados pessoais, deve-se executar uma avaliação dos riscos de cada processo no manuseio da informação privada. Essa avaliação deve contemplar a priorização e tratamento dos riscos identificados que tenham maior impacto na organização.
- **Ações de tratamento dos riscos** – Devem ser desenvolvidas ações de tratamento capazes de mitigar e/ou eliminar os riscos identificados na avaliação dos processos que tratam dados pessoais.

7.6 Acordos formais

O acordo é a formalização de um relacionamento para utilização de dados pessoais. A relação entre as partes e utilização da informação pelas mesmas deve estar claramente definida, como:

- A definição das partes como Operador, Controlador, Suboperador, e/ou Titular de dados;
- Os motivos da utilização da informação no tratamento de dados (Finalidade);
- As responsabilidades das partes com relação ao controle da informação;
- As medidas de segurança e as boas práticas adotadas;
- A determinação clara de quais informações (dados pessoais) está sendo tratadas.

8 DIREITOS DO TITULAR

O Titular de dados tem direito a solicitar informações acerca da forma como a organização realiza o tratamento dos seus dados pessoais e também requerer ações relacionadas aos seus dados, tais como, acesso e confirmação, eliminação, revogação do consentimento, bloqueio e demais informações previstas na Política de Privacidade disponibilizada no website da PREVIG: https://www.previg.org.br/politica-de-privacidade.

Todas as solicitações do Titular devem ser atendidas pela organização seguindo o processo de comunicação da empresa previsto no **FOR RH 003 – Comunicações do SGSI e Privacidade**.

9 ENCARREGADO DE PROTEÇÃO DE DADOS

O Encarregado de proteção de dados, é o profissional nomeado pela organização para realizar as comunicações internas e externas relacionadas a privacidade dos dados pessoais representado pelo(a) Gerente de Sistemas de Informação (GSI).

9.1 Atribuições:

- Atender às requisições dos titulares de dados realizadas através no canal de ouvidoria no site da empresa: https://www.previg.org.br/politica-de-privacidade;
- Atender e tomar providências referente a solicitação da ANPD;
- Orientar os colaboradores e demais contratados acerca das melhores práticas a serem adotadas para a proteção dos dados pessoais;

9.2 Contato

As solicitações referentes a privacidade de dados pessoais nas atividades da empresa, devem ser encaminhadas para o e-mail privacidade@previg.org.br.

10 TRANSFERÊNCIA DE DADOS PESSOAIS

Todo dado pessoal que for transferido para outra organização deve constituir formalmente um acordo de tratamento de dados pessoais com o pleno entendimento da forma de utilização da informação, obedecendo as orientações previstas na **PSI 015 – Procedimento de Gestão de Fornecedores**.

10.1 Transferência para Operador de dados:

A organização a qual a PREVIG realiza transferência de dados pessoais, deve ser considerada como Operador dos dados, devendo tal Operador obedecer aos princípios de segurança da informação instituídos pela PREVIG. As responsabilidades do Operador quanto ao tratamento dos dados pessoais, devem estar formalmente identificadas no acordo estabelecido.

O Titular deve ser cientificado sobre a transferência dos seus dados pessoais, bem como sobre a finalidade do tratamento dos seus dados pelo Operador.

Todo Operador de dados que tratar dados pessoais em nome da PREVIG, deve seguir as seguintes orientações:

- Armazenamento seguro – Todas as informações cedidas devem ser protegidas física e logicamente.
- Confidencialidade estabelecida – Deve-se determinar formalmente um acordo de confidencialidades, entre a PREVIG e Operador, com relação as informações transferidas.
- Não divulgação – Deve-se estabelecer o princípio da não divulgação das informações recebidas, obedecendo o princípio da confidencialidade.
- Controle de acesso – O operador deve designar controles de acesso físico e lógico aos sistemas que receberão as informações transferidas. O controle deve segregar os usuários do Operador e usuários do Controlador que usam a aplicação/estrutura tecnológica para o tratamento de dados. As exceções devem ser tratadas explicitamente nos acordos estipulados.
- Segurança da informação: O Operador deve instituir uma política mínima de segurança da informação que atente para a prevenção e detecção de ataques cibernéticos. Deve-se também buscar a continuidade do serviço oferecido em caso de crise.

10.2 Transferência para Suboperador de dados:

O Operador que para a execução dos serviços contratos pela PREVIG necessitar transferir os dados pessoais para outra organização, deve garantir que a mesma obedecerá aos princípios de segurança da informação estabelecidos pela PREVIG, sendo tal organização identificada como Suboperador dos dados pessoais.

O Operador somente poderá transferir informações para os Suboperadores indicados no acordo estabelecido com a PREVIG, salvo nos casos em que a PREVIG autorizar de forma expressa e por escrito a transferência para determinado Suboperador.

O Operador deve transferir o conhecimento das políticas de segurança e de privacidade instituídas pela PREVIG para o Suboperador.

As orientações previstas no item **9.1** desta Política aplicam-se integralmente aos Suboperadores.

10.3 Término do tratamento dos dados pessoais

Após a finalização do tratamento de dados pelo Operador e Sub-operador, deve-se iniciar o processo de sanitização dos dados transferidos, ou seja, todos os dados devem ser removidos. O Operador e Suboperador devem gerar evidências de remoção dos dados para registro.

A exceção da remoção dos dados é aplicável quando for exigido legalmente a sua retenção por período definido, ou em observância de normas regulatórias, as mesmas devem ser previstas no acordo estabelecido.

11 LIMITES DO USO

As limitações de uso de DP devem ser orientadas pela necessidade da sua utilização pela organização e pelos princípios de:

- Finalidade de uso – a criação ou o desenvolvimento de processos de DP deve estar diretamente relacionado a uma razão específica e um propósito de uso, em outras palavras, se não houver razão para o uso dos dados, não deve ser executado o processo.
- Adequação legal – o uso da informação privada deve ser compatível/alinhada com a finalidade de uso e as determinações legais estipuladas.

Convém aos gestores de processo a observância destes princípios, para a adequação de contratos, tecnologias e orientação dos colaboradores envolvidos para o bom uso de DP.

12 DESCARTE DA INFORMAÇÃO

Toda informação, inclusive dados pessoais, inserida nos processos e/ou sistemas que não tem mais valia para a empresa ou não tem obrigação legal que obrigue seu armazenamento, está sujeita ao processo de descarte definido no processo de descarte da informação **PSI 018 – Procedimento de Descarte de informação.** O gestor do processo deve definir o processo de retenção da informação obedecendo os princípios legais e objetivos estratégicos do negócio para aferir os processos de backup e resposta a possíveis solicitações do titular de dados.
Todas as solicitações de descarte devem ser registradas para o devido acompanhamento do DPO da empresa.

13 DOCUMENTAÇÃO IMPRESSA

Todo documento impresso, tais como, contratos, currículos, fichas cadastrais, dentre outros, que contém dado pessoal e necessita de retenção legal deve ser armazenada em local adequado, com os devidos controles de acesso em conformidade com a Política de Segurança da Informação.

A informação que não precisa de retenção e tem seu ciclo de vida no processo finalizado deve ser descartada em conformidade com o processo de descarte da informação.

14 PRIVACIDADE POR PADRÃO

A privacidade dos dados deve ser levada em consideração no desenvolvimento dos produtos e serviços desde sua concepção. O processo de desenvolvimento deve utilizar meios para definir os requisitos mínimos de segurança da informação e privacidade.

No momento de definição do projeto/serviço deve-se observar o seu risco no uso de informação privada no processo. Caso seja detectado que o risco não seja aceitável, deve-se estabelecer processos de contenção ou tratamento.

15 COMUNICAÇÃO

Os processos que utilizam DP devem constar na comunicação corporativa de segurança da informação com o titular dos dados. Essa comunicação deve ser clara e objetiva. A forma de armazenamento e capacidade de segurança deve ser comunicada nos contratos, acordos, termos de aceite de serviço.

15.1 Canal de ouvidoria

O canal de ouvidoria é uma das formas de comunicação, para centralizar as requisições de privacidade, relacionadas acerca das informações sobre dados pessoais, nos termos do artigo 18 da LGPD.

As solicitações realizadas pelo Titular devem ser atendidas de acordo com os itens de comunicações relacionadas a gestão de privacidade dos dados pessoais descritos no **FOR RH 003 – Comunicações do SGSI e Privacidade**.

As requisições dos Titulares serão realizadas através de formulário no website da empresa https://www.previg.org.br/politica-de-privacidade.

15.2 Notificação de alteração da finalidade do uso de dado pessoal

O titular de dados pessoais deve ser notificado nos casos em que houver alteração da finalidade que lhe foi inicialmente informada, para o uso de seus dados pessoais pela organização. Quando houver mudança nos objetivos do uso do dado privado, o Titular deve ser informado e essa notificação deve enviada em conformidade com o Plano de Comunicação descrito no **FOR RH 003 – Comunicações do SGSI e Privacidade**.

15.3 Notificação de incidente de segurança de dados pessoais

Os incidentes de segurança relacionados a dados pessoais, tais como, acessos não autorizados, vazamento de informações, situações acidentais e ilícitas que possam resultar em dano relevante para o Titular de dados ou terceiro, devem ser avaliados, registrados e comunicados, na forma do **PROC TI 007 – Procedimento de Gestão de incidentes.**

16 MELHORIA CONTÍNUA

Convém que o sistema de gestão de privacidade da informação deve ter seus controles avaliados continuamente através de auditorias internas de gestão, onde devemos buscar a plena eficácia dos controles utilizados.

16.1 Riscos

Avaliar regularmente os riscos do tratamento de dados pessoais na organização para identificar as ameaças e tratar os riscos de privacidade identificados.

16.2 Auditoria interna
Auditar regulamente os processos/sistemas da organização que tratam dados pessoais, promovendo a melhoria contínua do sistema de gestão de privacidade dos dados.

16.3 Monitoramento
Estabelecer um monitoramento das atividades de tratamento de dados pessoais, identificando eventuais riscos e sugerindo ações de tratamento.

16.4 Análise crítica
Analisar criticamente o sistema de gestão de privacidade dos dados e desenvolver controles que promovam a melhoria dos processos da empresa

16.5 Conformidade
Acompanhar as alterações e mudanças legislativas e regulatórias que versarem sobre a proteção de dados pessoais e promover as adequações necessárias nos processos da organização, mantendo a conformidade com as regras de tratamento de dados pessoais.

17 CONTROLE DE VERSÕES

Versão	Autor (es)	Data	Descrição
0.1	Ana Beatriz	19/05/2021	Criação do documento
1.0	Diretoria Executiva	25/06/2021	Análise crítica e aprovação
1.1	Conselho Deliberativo	07/07/2021	Análise crítica e aprovação
1.2	Ana Beatriz	08/07/2021	Revisão e ajustes de texto.
1.3	Odair Kawka	13/07/2021	Revisão e ajustes de texto.