

POLÍTICA DE GESTÃO DE DADOS PESSOAIS

REGISTRO DAS REVISÕES		
REVISÃO Nº	DATA	MOTIVO

ELABORAÇÃO	REVISÃO	APROVAÇÃO
Diretoria Executiva	Gerência de Jurídica, Gerência Compliance e Governança e Coordenação de Risco	Conselho Deliberativo

Este documento foi aprovado na Reunião Extraordinária do Conselho Deliberativo nº 146ª no dia 13/08/2020 e entrará em vigor na data de 13/08/2020. O documento estará disponível no site da Previdência Usiminas.

ÍNDICE

1. OBJETIVOS.....	4
2. APLICAÇÃO	4
3. PRINCÍPIOS	4
4. CICLO DE VIDA DO DADO PESSOAL	5
5. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS.....	12
6. DIRETRIZES DE RESPOSTA A SOLICITAÇÕES E REQUISIÇÕES	14
7. VIOLAÇÃO DE DADOS PESSOAIS	16
8. SEGURANÇA DA INFORMAÇÃO.....	16
9. DADOS PESSOAIS SENSÍVEIS	17
10. DADOS DE SAÚDE	18
11. DECISÕES AUTOMATIZADAS.....	18
12. CONTRATOS.....	18
13. ATRIBUIÇÕES E RESPONSABILIDADES	21
14. DAS DISPOSIÇÕES FINAIS.....	26
15. DEFINIÇÕES.....	26

1. OBJETIVOS

Esta Política de Gestão de Dados Pessoais têm os seguintes objetivos:

- Apresentar aos Colaboradores, prestadores de serviços, parceiros e fornecedores da PREVIDÊNCIA USIMINAS as diretrizes da proteção aos Dados Pessoais e a importância da adoção das melhores práticas;
- Estabelecer as responsabilidades e os limites de atuação dos Colaboradores, prestadores de serviços, parceiros e fornecedores da PREVIDÊNCIA USIMINAS na proteção aos Dados Pessoais, reforçando a cultura interna e priorizando as ações necessárias conforme o negócio;
- Formalizar o comprometimento da PREVIDÊNCIA USIMINAS em adequar-se às leis aplicáveis, fortalecendo os negócios, as parcerias e as relações com os Titulares dos Dados Pessoais.

A Diretoria está comprometida e apoia as diretrizes estabelecidas nesta Política bem como na proteção dos Ativos Tangíveis e Intangíveis da PREVIDÊNCIA USIMINAS de acordo com as necessidades de negócio e em conformidade legal, garantindo a sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade no Tratamento dos Dados Pessoais.

2. APLICAÇÃO

Esta Política é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, aos Colaboradores, prestadores de serviços, parceiros e fornecedores.

3. PRINCÍPIOS

O Tratamento de Dados Pessoais deve ser regido pelos seguintes princípios:

- **Licitude:** O Tratamento dos Dados Pessoais deve ser realizado de modo lícito, justo e transparente com relação ao Titular dos Dados Pessoais.
- **Finalidade:** Os Dados Pessoais devem ser tratados apenas para as finalidades determinadas, explícitas, legítimas e informadas antes do Tratamento, não podendo ser tratados posteriormente para finalidades incompatíveis.
- **Adequação:** Os Dados Pessoais devem ser tratados de modo adequado e pertinente às suas finalidades de uso.
- **Proporcionalidade e Necessidade:** O Tratamento dos Dados Pessoais deve ser proporcional aos objetivos do negócio, não sendo feito Tratamento de tipos de Dados Pessoais que não sejam necessários e proporcionais aos objetivos de negócio.

- **Livre acesso:** assegurar aos Titulares a consulta facilitada e gratuita sobre a forma e a duração do Tratamento de seus Dados Pessoais.
- **Qualidade dos Dados:** assegurar aos Titulares, a exatidão, clareza, relevância e atualização dos Dados Pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu Tratamento.
- **Transparência:** assegurar que os Titulares tenham informações claras, precisas e facilmente acessíveis sobre o Tratamento de seus Dados Pessoais, observados os segredos comercial e industrial.
- **Segurança:** O Tratamento deve ser realizado de modo a assegurar a proteção e segurança dos Dados Pessoais, incluindo a proteção contra o Tratamento não autorizado ou ilícito, perda, destruição ou dano acidental, devendo a PREVIDÊNCIA USIMINAS adotar medidas técnicas e organizacionais para salvaguardar a integridade, confidencialidade e disponibilidade dos Dados Pessoais.
- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais.
- **Não discriminação:** impossibilidade de realização do Tratamento para fins discriminatórios ilícitos ou abusivos.
- **Responsabilização e prestação de contas:** demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.
- **Subsidiariedade:** Deve-se sempre buscar formas alternativas (subsidiárias) de se atingir as mesmas finalidades por meios menos invasivos à privacidade do Titular dos Dados Pessoais.
- **Limitação de armazenamento:** Os Dados Pessoais e registros devem ser armazenados apenas durante o período estritamente necessário de acordo com sua finalidade, com os padrões a serem estabelecidos pela Autoridade Nacional de Proteção de Dados (ANPD) e de acordo com a legislação aplicável.

4. CICLO DE VIDA DO DADO PESSOAL

4.1. DIRETRIZES GERAIS PARA TRATAMENTO DOS DADOS PESSOAIS

O Tratamento de Dados Pessoais significa toda e qualquer operação realizada pela PREVIDÊNCIA USIMINAS com Dados Pessoais, a exemplo de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração entre outras operações possíveis.

A coleta do Dado Pessoal significa a entrada do Dado Pessoal na PREVIDÊNCIA USIMINAS, podendo ser feita por meio de sistemas da informação ligados a sites, aplicativos, recebimento de arquivos, aquisição de base de Dados bem como no ambiente físico como pelo preenchimento de formulários, listas ou pelo registro de uma conversa presencial, por chat, troca de mensagens, e-mails ou por telefone, por exemplo.

O Tratamento de Dados Pessoais deve ser realizado de acordo com os seguintes pontos de conformidade:

- **Transparência:** Antes de realizar o Tratamento de Dados Pessoais, o Titular dos Dados Pessoais deve receber informação clara, concisa, inteligível, de fácil acesso e de fácil compreensão sobre a coleta, finalidade, armazenamento, compartilhamento e descarte de seus Dados Pessoais. Devem ser apresentadas, no mínimo, as seguintes informações quando o Tratamento for realizado:
 - a) A qualificação da PREVIDÊNCIA USIMINAS e seus Dados de contato;
 - b) O canal de contato com o Encarregado pelo Tratamento de Dados Pessoais da PREVIDÊNCIA USIMINAS;
 - c) As finalidades específicas e forma de Tratamento;
 - d) O Tempo de retenção dos Dados Pessoais, levando em consideração a finalidade do Tratamento (devendo estar de acordo com a lei e a tabela de temporalidade);
 - e) Demais Controladores com as quais a PREVIDÊNCIA USIMINAS realiza o uso compartilhado de Dados Pessoais, tanto entidades públicas como privadas;
 - f) Se o Tratamento dos Dados Pessoais se baseia em interesse legítimo da PREVIDÊNCIA USIMINAS ou de terceiros;
 - g) Se ocorrerá a transferência de Dados Pessoais para outro país (incluindo-se por meio do armazenamento em nuvem ou se o hardware se localiza em outro país) e, neste caso, se há salvaguardas adequadas para a transferência internacional;
 - h) Se a comunicação de Dados Pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato;
 - i) Quando o Consentimento do Titular dos Dados Pessoais for necessário, dispor acerca da possibilidade de não fornecimento de Consentimento e sobre as consequências que a negativa pode ocasionar, bem como possibilitar que o Titular revogue o Consentimento, nos termos da legislação aplicável.

- j) A existência de decisões automatizadas, incluindo a definição de perfis, além de informações úteis relativas à lógica utilizada, a importância e as consequências previstas de tal Tratamento para o Titular dos Dados Pessoais;
 - k) Os direitos do Titular dos Dados Pessoais, como a confirmação da existência do Tratamento, acesso aos Dados Pessoais, correção de Dados Pessoais incompletos, inexatos ou desatualizados, portabilidade dos Dados Pessoais, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a legislação aplicável;
 - l) Os riscos, regras e garantias associadas ao Tratamento dos Dados Pessoais, bem como os meios que o Titular dos Dados Pessoais dispõe para exercer os seus direitos relativamente a esse Tratamento;
 - m) Quando o Tratamento de Dados Pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direitos, o Titular dos Dados Pessoais será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os seus direitos.
- **Proporcionalidade:** As Áreas que realizam o Tratamento dos Dados Pessoais devem buscar tratar o menor volume possível de Dados Pessoais, devendo esse volume ser proporcional aos objetivos do negócio.
 - **Minimização:** Os Dados Pessoais tratados pela PREVIDÊNCIA USIMINAS devem ser limitados ao mínimo necessário para execução das finalidades de Tratamento informadas. Não se deve coletar Dados Pessoais que não têm uma finalidade definida.
 - **Subsidiariedade:** Devem ser cogitados métodos alternativos ou subsidiários que levem em consideração os direitos dos Titulares dos Dados para o cumprimento das finalidades de Tratamento.
 - **Limitação do armazenamento:** Os Dados Pessoais devem ser armazenados por período limitado, sendo que o período (ou critério) estabelecido deve ser informado ao Titular dos Dados Pessoais antes do Tratamento, excetuando-se hipóteses legais nas quais seja permitido o armazenamento por maior período de tempo. O período para a guarda dos Dados Pessoais deve ser definido em tabela de temporalidade.
 - **Licitude:** O Tratamento de Dados Pessoais somente é permitido e, portanto, está legitimado:
 - a) Com o Consentimento do Titular dos Dados Pessoais, conforme detalhado nos itens 4.2 e 4.3. É vedado o Tratamento de Dados Pessoais mediante vício de Consentimento:
 - b) Em caso do cumprimento de uma obrigação legal ou regulatória pela PREVIDÊNCIA

USIMINAS;

- c) Quando o Titular dos Dados Pessoais é parte em contrato ou os seus Dados Pessoais são necessários para execução de procedimentos preliminares para se firmar o contrato;
- d) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, prezando sempre pelo pedido de sigilo de justiça quando envolver Dado Pessoal;
- e) Para a proteção da vida ou da segurança física da pessoa a quem os Dados Pessoais se referem;
- f) Para proteção da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- g) Por interesse legítimo da PREVIDÊNCIA USIMINAS ou de terceiros, sendo obrigatória a confecção de relatório de impacto à proteção de Dados Pessoais;
- h) Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

4.2. CONSENTIMENTO

Quando o Tratamento dos Dados Pessoais se basear no Consentimento do Titular, este deve ser Dado mediante manifestação de vontade livre de que o Titular concorda com o Tratamento de Dados Pessoais da forma declarada.

O Consentimento pode ser Dado de modo escrito, digital ou oral, sendo fundamental que a PREVIDÊNCIA USIMINAS registre e comprove o Consentimento do Titular (neste caso o ônus da prova pertence ao Agente de Tratamento de Dados Pessoais).

O Consentimento para Tratamento de Dados Pessoais Sensíveis deve ser possível de ser coletado de forma específica e destacada, para finalidades específicas.

O silêncio, opções pré-validadas, generalistas ou a omissão NÃO são consideradas manifestações de Consentimento.

A Área responsável pelo tratamento dos dados da PREVIDÊNCIA USIMINAS deve realizar a gestão do Consentimento nos casos em que o Tratamento ocorra sob a hipótese legal do Consentimento do Titular.

Se o Consentimento do Titular dos Dados Pessoais for Dado no contexto de uma declaração escrita que diga também respeito a outras finalidades de Tratamento, o pedido de Consentimento deve ser apresentado de uma forma que o diferencie claramente das demais finalidades de modo inteligível, destacado, de fácil acesso e em linguagem clara e simples.

O Titular dos Dados Pessoais deve ser informado previamente sobre o seu direito de revogar o

Consentimento a qualquer momento. A revogação do Consentimento deve ser oferecida de maneira simples, clara e facilitada, de preferência pela mesma via de coleta do Consentimento.

O Titular dos Dados Pessoais deve ser informado previamente das consequências da revogação do Consentimento.

A revogação do Consentimento não compromete a licitude do Tratamento já efetuado com base no Consentimento previamente Dado e deverá ser realizado por procedimento gratuito e facilitado.

4.3. CONSENTIMENTO DE MENORES DE IDADE

O Tratamento de Dados Pessoais de crianças deve ocorrer somente se o Consentimento for Dado por pelo menos um dos pais ou pelo responsável legal.

Cada Área responsável por este Tratamento deve coletar a evidência de cumprimento do disposto acima para fins de formação de prova.

4.4. ARMAZENAMENTO

O armazenamento dos Dados Pessoais pode ser feito de modo físico (guarda de crachás, cartões, fichas, papéis com anotações à mão, formulários, notas fiscais, contratos e outros documentos em papel, por exemplo) ou digital (em mídias como CD, DVD, Blu-Ray, HD externo, pendrive, cartão de memória SD, nas plataformas digitais da PREVIDÊNCIA USIMINAS ou em serviço contratado para esta finalidade).

No caso de armazenamento fora do Brasil, a Área responsável pelo tratamento de dados da Previdência Usiminas por garantir o Tratamento dos Dados Pessoais deve estar atenta para o país em que o hardware se localiza e, localizando-se no exterior, deve-se acionar a Área Jurídica da PREVIDÊNCIA USIMINAS para verificar se há amparo legal e contratual para que os Dados Pessoais estejam armazenados nesse país.

Os meios físicos e digitais de armazenamento dos Dados Pessoais devem assegurar a sua qualidade, devendo ser mantidos exatos e atualizados, de acordo com a necessidade para o cumprimento da finalidade de Tratamento.

Quando o Titular dos Dados Pessoais solicitar a correção ou atualização de seus Dados Pessoais, o Encarregado pelo Tratamento de Dados Pessoais, após análise da requisição, deve acionar as Áreas Responsáveis para assegurar que os meios físicos e digitais onde esses Dados Pessoais foram replicados e armazenados sejam também atualizados.

4.5. USO

O uso dos Dados Pessoais deve ser realizado dentro dos limites das finalidades legitimadas na coleta. Caso haja a necessidade de realizar o Tratamento do Dado Pessoal para outra finalidade diversa da informada no momento da coleta, é necessário verificar:

- Qualquer ligação entre a finalidade para a qual os Dados Pessoais foram coletados e a finalidade do novo Tratamento;
- O contexto em que os Dados Pessoais foram tratados (a relação entre o Titular dos Dados Pessoais e a PREVIDÊNCIA USIMINAS);
- Se o Dado coletado está sendo compartilhado com demais Agentes de Tratamento;
- A natureza dos Dados Pessoais (se há Dados Pessoais Sensíveis envolvidos);
- As consequências do novo Tratamento para o Titular dos Dados Pessoais, e
- A existência de medidas de proteção adequada, como Anonimização.

Essas informações devem ser encaminhadas ao Encarregado pelo Tratamento de Dados Pessoais para que defina se o novo Tratamento já está ou não legitimado, e, caso não esteja, ele deve propor as estratégias de como este Tratamento pode ser legitimado antes de ser realizado.

O Titular dos Dados Pessoais deve ser informado sobre esse novo Tratamento antes de ser realizado.

O legítimo interesse deverá ser previamente analisado pelo Encarregado pelo Tratamento de Dados Pessoais conforme procedimento específico.

4.6. COMPARTILHAMENTO

O compartilhamento de Dados Pessoais ou de documentos/arquivos com Dados Pessoais em território nacional pode ser feito para Agentes de Tratamento autorizados, com as medidas de segurança indicadas pela Área de Tecnologia da Informação e somente para as finalidades de uso ou Tratamento prévia e devidamente informadas e legitimadas junto ao Titular dos Dados Pessoais.

O compartilhamento de Dados Pessoais com demais Agentes de Tratamento, excetuando-se o compartilhamento realizado para cumprimento de obrigações legais, somente poderá ocorrer caso estes tenham firmado contratos com cláusulas referentes à Proteção de Dados Pessoais, conforme disposto no item 12 – CONTRATOS desta Política.

No caso de impossibilidade de celebração de Contrato ou Aditivo com a parte em questão, devem ser adotados controles mitigatórios em relação à segurança e proteção do Tratamento dos Dados Pessoais.

O compartilhamento de Dados Pessoais cujo Tratamento tenha como hipótese legal o Consentimento somente poderá ocorrer com o Consentimento do Titular dos Dados Pessoais que esteja ciente deste compartilhamento, sendo que o Consentimento deve ser coletado anteriormente ao início do

Tratamento dos Dados Pessoais.

Os Dados Pessoais anonimizados podem ser transferidos para terceiros, desde que respeitados os requisitos de Tratamento disposto na legislação aplicável.

O compartilhamento de Dados Pessoais deve ocorrer somente por canais com medidas de segurança aplicadas.

4.7. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

Caso os Dados Pessoais tenham a previsão de serem transferidos para outro país, a possibilidade de compartilhamento com outro Controlador deverá ser submetida à análise do Encarregado pelo Tratamento de Dados Pessoais, pela Área de Tecnologia da Informação e a Área Jurídica, de modo que possam avaliar se o país de destino possui grau de proteção de Dados que esteja adequado ao ordenamento jurídico brasileiro.

Se o Controlador-Receptor oferecer e comprovar garantias de cumprimento dos direitos do Titular, a transferência internacional de Dados também poderá ser possível na forma de (i) cláusulas contratuais específicas para determinada transferência; (ii) cláusulas-padrão contratuais; (iii) normas corporativas globais; e (iv) selos, certificados e códigos de conduta emitidos pela Autoridade Nacional de Proteção de Dados.

A transferência internacional de Dados Pessoais também pode ocorrer a partir das finalidades elencadas abaixo:

- Quando a transferência for necessária para a proteção da vida do Titular ou de terceiros;
- Quando a Autoridade Nacional autorizar a transferência;
- Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional
- Quando o Titular tiver fornecido o seu Consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades;
- Para cumprimento de obrigação legal ou regulatória pela PREVIDÊNCIA USIMINAS;
- Quando necessária para execução de contrato e procedimentos preliminares relacionados a contrato do qual seja parte o Titular, a pedido do Titular dos Dados.

4.8. ELIMINAÇÃO DOS DADOS PESSOAIS

Os Dados Pessoais devem ser armazenados por período limitado, levando em consideração a finalidade específica do Tratamento.

Após cumprida a finalidade do Tratamento e findo o prazo de armazenamento determinado pela tabela de temporalidade, os Dados podem ser eliminados de modo seguro, sejam eles registrados em meios físicos ou digitais.

A eliminação dos Dados Pessoais poderá ser realizada também a pedido do Titular do Dado ou da Autoridade Nacional de Proteção de Dados.

Devem ser seguidas as definições indicadas no procedimento de eliminação de Dados seguro.

A conservação dos Dados Pessoais após atingida sua finalidade é possível nos caso de cumprimento de obrigação legal ou regulatória por parte da PREVIDÊNCIA USIMINAS.

A solicitação de eliminação do Dado Pessoal pelo Titular não será possível quando o Dado já tiver sido anonimizado.

A solicitação também não poderá ser realizada no caso de cumprimento de obrigação legal quanto ao armazenamento destes Dados para fins regulatórios, respeitada a tabela de temporalidade.

5. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

O Relatório de Impacto à Proteção de Dados Pessoais visa a descrição dos processos de Tratamento de Dados Pessoais e as medidas e mecanismos empregados para mitigar esses riscos pela PREVIDÊNCIA USIMINAS.

Todo Tratamento de Dados Pessoais tendo como hipótese legal o legítimo interesse deve ser precedido de relatório de impacto à proteção de Dados Pessoais.

O Relatório de Impacto à Proteção de Dados Pessoais deve ser elaborado pelo Encarregado pelo Tratamento de Dados Pessoais, com o envolvimento das Áreas necessárias para entendimento da elaboração deste relatório, conforme procedimento específico, e deve conter no mínimo:

- Descrição das operações de Tratamento que podem gerar riscos às liberdades civis e os direitos fundamentais dos Titulares dos Dados;
- Finalidade das operações de Tratamento de Dados Pessoais;
- Categorias de Dados Pessoais coletados;
- Existência ou não da coleta de Dados Pessoais Sensíveis;
- Categorias de Titulares dos Dados Pessoais
- Fontes e origens dos Dados Pessoais;
- Finalidade de Tratamento por categoria de Dado Pessoal;
- Hipótese legal de Tratamento.

- Sendo a hipótese legal o Consentimento do Titular dos Dados Pessoais, deve-se especificar forma de obtenção, armazenamento e meios de retirada do Consentimento.
- Presença de Tratamento de Dados Pessoais baseada no legítimo interesse. Havendo legítimo interesse envolvido, definir:
 - Finalidade a ser atingida com o Tratamento dos Dados Pessoais;
 - Legitimidade da finalidade a ser alcançada;
 - Situação concreta;
 - Coleta do mínimo e estritamente necessário para alcance da finalidade pretendida;
 - Existência de outras bases legais que não sejam o legítimo interesse para Tratamento dos Dados Pessoais;
 - Compatibilidade do Tratamento com a expectativa do Titular dos Dados Pessoais;
 - Compatibilidade do Tratamento com direitos e liberdades fundamentais do Titular dos Dados Pessoais;
 - Garantia de transparência do Tratamento realizado;
 - Mecanismos de oposição ao Tratamento de Dados Pessoais disponíveis ao Titular dos Dados Pessoais;
 - Medidas de mitigação de risco aplicáveis, como por exemplo, a Anonimização dos Dados Pessoais a depender da finalidade a ser alcançada.
- Descrição e avaliação de risco aos Titulares dos Dados Pessoais, estabelecendo:
 - Descrição detalhada do risco;
 - Fundamentação legal;
 - Grau do risco (alto, médio e baixo);
 - Probabilidade do risco se materializar.
- Medidas existentes para endereçar os riscos envolvidos no Tratamento dos Dados Pessoais, incluindo:
 - Ações de mitigação;
 - Medidas de segurança da informação aplicáveis;
 - Grau do risco após a implementação das ações de mitigação e medidas de segurança da informação aplicáveis.

- Projetos e/ou funções de negócio nos quais o referido Tratamento de Dados Pessoais está inserido.
- Período de armazenamento e retenção dos Dados Pessoais.
- Medidas para adequar o Tratamento às legislações existentes de Tratamento de Dados Pessoais.

6. DIRETRIZES DE RESPOSTA A SOLICITAÇÕES E REQUISIÇÕES

6.1. RESPOSTA À REQUISIÇÃO DO TITULAR DOS DADOS PESSOAIS

Os procedimentos de resposta as requisições dos Titulares dos Dados Pessoais serão regidos pelo procedimento de resposta à requisição do Titular dos Dados Pessoais, disponível na intranet ou rede interna.

Todos os Colaboradores ou prestadores de serviço têm o dever de notificar o Encarregado pelo Tratamento de Dados Pessoais, imediatamente, sobre qualquer requisição recebida do Titular dos Dados Pessoais, antes de responder a requisição, buscando, sempre que possível, orientações acerca de melhores práticas na comunicação a ser estabelecida com o Titular dos Dados Pessoais.

Em casos de dúvida e situações específicas, o Colaborador ou prestador de serviço deve encaminhar a requisição ao Encarregado pelo Tratamento de Dados Pessoais, para que este responda da forma mais adequada perante à legislação específica aplicável e às boas práticas estipuladas internamente ou observadas no mercado.

6.2. ACESSO AOS DADOS PESSOAIS PELO TITULAR DOS DADOS PESSOAIS

O Titular dos Dados Pessoais pode requerer a qualquer momento o acesso aos seus Dados Pessoais, devendo o Colaborador ou prestador de serviço da Área Responsável pelo Tratamento assegurar que a identidade do Titular dos Dados Pessoais seja comprovada conforme procedimento de resposta à requisição do Titular dos Dados Pessoais.

A requisição e posterior acesso aos Dados Pessoais deve ocorrer, preferencialmente, de modo eletrônico, exceto quando o Titular dos Dados Pessoais expressamente requerer o envio dos Dados Pessoais de modo físico ou divulgação de modo oral.

Podem ser utilizados recursos visuais para tornar as informações ainda mais inteligíveis e de fácil compreensão.

6.3. APAGAMENTO E/OU BLOQUEIO DE TRATAMENTO DOS DADOS PESSOAIS POR REQUISIÇÃO DO TITULAR DOS DADOS PESSOAIS

O Titular dos Dados Pessoais pode requerer a qualquer momento o apagamento e/ou bloqueio do Tratamento de seus Dados Pessoais, devendo o Colaborador ou prestador de serviço da Área Responsável pelo Tratamento encaminhar a requisição de apagamento/bloqueio ao Encarregado pelo Tratamento de Dados Pessoais para que possam ser adotadas as medidas conforme os procedimentos indicados no procedimento de resposta à requisição do Titular dos Dados Pessoais.

Para apagamento de Dados Pessoais armazenados em backups, devem ser avaliados o custo, os recursos alocados e o esforço razoável para que seja feito este apagamento.

Na impossibilidade deste apagamento, o Titular deve ser informado sobre esta decisão, explicando os motivos pelos quais estes Dados Pessoais não poderão ser apagados.

A Área de Tecnologia da Informação deve estabelecer mecanismos quando da restauração de Dados Pessoais que impeçam que sejam restauradas ao ambiente lógico os Dados Pessoais de Titular dos Dados Pessoais que tenha solicitado seu apagamento.

6.4. RESPOSTA A AUTORIDADE FISCALIZADORA

Os Colaboradores ou prestadores de serviço têm o dever de notificar o Encarregado pelo Tratamento de Dados Pessoais e a Área Jurídica da PREVIDÊNCIA USIMINAS, imediatamente, sobre qualquer ordem ou requisição relativa à privacidade e proteção de Dados Pessoais recebida de autoridade fiscalizadora.

6.5. RESPOSTA À AUTORIDADE JUDICIAL

Os Colaboradores ou prestadores de serviço têm o dever de notificar imediatamente o Encarregado pelo Tratamento de Dados Pessoais e a Área Jurídica da PREVIDÊNCIA USIMINAS sobre qualquer ordem ou determinação de autoridade judicial relativa a Dados Pessoais de que tome conhecimento.

Quando requisitado por meio de ordem judicial, caberá à Área Jurídica fornecer quaisquer esclarecimentos e entregar as informações demandadas pela Autoridade podendo requisitar o apoio do Encarregado pelo Tratamento de Dados Pessoais caso entenda como necessário.

Caso se faça necessário o acesso a Dados Pessoais e informações com acesso restrito ou moderado, caberá à Área Jurídica acionar o Encarregado pelo Tratamento de Dados Pessoais e as Áreas Responsáveis para que estas forneçam acesso temporário (seguindo as diretrizes estabelecidas pelas Política de Segurança da Informação), possibilitado assim o cumprimento de ordem judicial de forma tempestiva.

Quando a Autoridade determinar a necessidade de prestação de esclarecimentos, caberá à Área Jurídica buscar junto ao Encarregado pelo Tratamento de Dados Pessoais e com os Colaboradores ou prestadores de serviço que tenham envolvimento no fluxo de Dados Pessoais, solicitando relatórios,

fazendo entrevistas, e buscando compilar o máximo de informações pertinentes para estruturar uma resposta adequada e concisa.

7. VIOLAÇÃO DE DADOS PESSOAIS

Os procedimentos relativos à violação de Dados Pessoais são regidos pelo procedimento de resposta a incidentes, disponível em intranet ou rede interna.

A Área de Tecnologia da Informação deve implementar controles técnicos de modo a capacitar a PREVIDÊNCIA USIMINAS quanto a possíveis violações de Dados Pessoais em seus ambientes lógicos, possibilitando reportar tais eventos em tempo hábil à Autoridade Fiscalizadora.

Os Colaboradores ou prestadores de serviço têm o dever de notificar ao Encarregado pelo Tratamento de Dados Pessoais sem demora injustificada, acerca de qualquer violação ou tentativa de violação de Dados Pessoais da qual tenham conhecimento.

Os Colaboradores ou prestadores de serviço devem, na medida de suas possibilidades, cooperar para a investigação e mitigação de incidentes de violação de Dados Pessoais.

Todos os procedimentos realizados nessa seção devem ser documentados pelas partes envolvidas, sob a supervisão do Encarregado pelo Tratamento de Dados Pessoais.

8. SEGURANÇA DA INFORMAÇÃO

Durante todo ciclo de vida do Dado Pessoal devem ser observadas as diretrizes de segurança existentes na Política de Segurança da Informação e Comunicação da PREVIDÊNCIA USIMINAS.

A Área de Tecnologia da Informação deve assegurar a confidencialidade, integridade e disponibilidade do Dado Pessoal em todos os meios de armazenamento e transmissão dos Dados Pessoais, a partir de:

- Controles técnicos de segurança envolvidos, como:
 - a) Firewall;
 - b) Criptografia;
 - c) Uso de VPN para acesso aos Dados fora das dependências da PREVIDÊNCIA USIMINAS;
 - d) Controles de acesso;
 - e) Autenticação em dois fatores;
 - f) Gerenciadores de senha.
- Assegurar de que somente pessoas e Agentes de Tratamento autorizados tenham acesso aos

Dados Pessoais (em observância à necessidade e relevância da concessão do acesso);

- Adoção de medidas de segurança da informação para assegurar que os Dados Pessoais se mantenham íntegros (sem alterações indevidas), exatos, completos e atualizados;
- Garantia de que os Dados Pessoais sejam acessíveis e utilizáveis pelas pessoas e entidades autorizadas sempre que sejam necessários;
- Registro de logs e trilhas de auditoria do ciclo de vida do Dado Pessoal;
- Criptografia, pseudonimização e Anonimização dos Dados Pessoais;
- Manutenção de backup e testes de restore;
- Treinamento em proteção de Dados Pessoais aos Colaboradores e supervisão da adoção das práticas ensinadas.

9. DADOS PESSOAIS SENSÍVEIS

O Tratamento de Dados Pessoais Sensíveis deve ser precedido de Relatório de Impacto à Proteção de Dados Pessoais.

O Tratamento de Dados Pessoais Sensíveis poderá ocorrer com o Consentimento Dado pelo Titular, realizado de forma específica e destacada, para finalidades específicas.

O Tratamento de Dados Pessoais Sensíveis poderá ocorrer sem o Consentimento do Titular dos Dados Pessoais, quando for indispensável o Tratamento, nas seguintes hipóteses:

- Cumprimento de obrigação legal ou regulatória pela PREVIDÊNCIA USIMINAS;
- Tratamento compartilhado de Dados Pessoais pela administração pública, necessários para execução de políticas públicas previstas em leis ou regulamentos;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Proteção da vida ou da incolumidade física do Titular ou terceiro;
- Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Garantia de prevenção à fraude e segurança do Titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (hipótese de legitimação exclusiva da Lei Geral de Proteção de Dados Pessoais brasileira, aplicável, portanto, somente no território nacional).

10. DADOS DE SAÚDE

Os Dados de saúde poderão ser compartilhados entre Controladores, levando em consideração o benefício dos interesses dos Titulares e, se for realizado, exclusivamente, para:

- prestação de serviços de saúde;
- assistência farmacêutica;
- assistência à saúde;
- serviços auxiliares de diagnose;
- serviços de terapia.

O Tratamento de Dados de saúde deverá, obrigatoriamente, permitir ao Titular o direito a portabilidade dos seus Dados, quando solicitada ou as transações financeiras e administrativas resultantes do uso e da prestação dos serviços.

11. DECISÕES AUTOMATIZADAS

As Áreas da Previdência Usiminas devem listar os processos sob sua responsabilidade que envolvem decisões automatizadas baseada no Tratamento de Dados Pessoais que ocorrem em sua área.

Toda decisão automatizada que envolve o Tratamento de Dados Pessoais deve ter formalizada informações claras e adequadas, disponíveis aos Titulares dos Dados Pessoais, quanto aos:

- Critérios utilizados para tomada de decisão automatizada;
- Procedimentos utilizados para tomada de decisão automatiza;

O Titular dos Dados Pessoais tem o direito de solicitar a revisão de tomada de decisão baseada em Tratamento automatizado dos Dados Pessoais, tendo o acesso aos critérios e procedimentos, não sendo exigido que esta revisão seja por pessoa natural.

12. CONTRATOS

A PREVIDÊNCIA USIMINAS na figura de Controladora, sempre que fizer uso de um Operador, deve estabelecer contrato tendo em vista as regulamentações relacionadas à privacidade e proteção de Dados Pessoais vigentes no país onde ocorrerá o Tratamento dos Dados Pessoais.

A PREVIDÊNCIA USIMINAS na figura de Controladora, deve assegurar que todos os contratos que envolvam serviços e/ou sistemas nos quais haja Tratamento e/ou armazenamento de Dados Pessoais por Operador contenham, no mínimo, os seguintes itens:

- Obrigatoriedade legal de atuar respeitando legislação vigente no local de Tratamento e/ou

armazenamento dos Dados Pessoais, em especial a Lei 13.709 (“Lei Geral de Proteção de Dados Pessoais”).

- Diretrizes de Tratamento:
 - Assunto do Tratamento;
 - Duração do Tratamento;
 - Natureza e propósito do Tratamento;
 - Tipos de Dados Pessoais envolvidos;
 - Categorias de Dados Pessoais envolvidos;
 - Forma de coleta dos Dados Pessoais;
 - Forma de armazenamento dos Dados Pessoais;
 - Qualquer tipo de Tratamento fora do especificado acima será considerado descumprimento do contrato.
- Procedimentos a serem tomados no caso de requisições de Titulares dos Dados Pessoais;
- Obrigatoriedade acerca de manutenção de confidencialidade dos Dados Pessoais;
- Adoção de medidas de segurança técnicas e organizacionais para garantir a confidencialidade, integridade e disponibilidade dos Dados Pessoais que passem por Tratamento;
- Adoção de medidas de Anonimização, pseudonimização (quando aplicável) e criptografia dos Dados Pessoais conforme a necessidade do Tratamento em questão;
- Obrigatoriedade de registro das operações de Tratamento de Dados Pessoais, conforme serviço ou contrato em questão. A exemplo de registro de Tratamento de Dados Pessoais, devem ser armazenados, quando possível, no mínimo, as seguintes informações:
 - Ação realizada;
 - Identificação de usuários do sistema;
 - Dados de IP no momento da ação;
 - Data/hora da ação, com referência UTC (Universal Time Coordinated), sendo que os relógios de seus sistemas estão sincronizados com a hora legal brasileira e de acordo com o protocolo NTP (ntp.br) de sincronização dos relógios; e,
 - Identificador de sessão da conexão utilizada, quando possível.
- Adoção de medidas técnicas e organizacionais contra destruição, acidental ou ilícita, perda,

alteração indevida, comunicação ou difusão não autorizada, acesso não autorizado em relação aos Dados Pessoais que passem por Tratamento;

- Necessidade de autorização da PREVIDÊNCIA USIMINAS quanto à subcontratação de Operadores;
- Envio de relatórios sobre o monitoramento do Tratamento de Dados Pessoais, a incluir, mas não limitado, as seguintes informações:
 - O status dos sistemas de Tratamento de Dados Pessoais;
 - As medidas de segurança;
 - O tempo de inatividade registrado das medidas técnicas de segurança;
 - A (não) conformidade estabelecida com as medidas organizacionais;
 - Quaisquer eventuais violações de Dados Pessoais e/ou incidentes de segurança;
 - As ameaças percebidas à segurança e aos Dados Pessoais; e,
 - As melhorias exigidas e/ou recomendadas.
- Notificação à PREVIDÊNCIA USIMINAS em até 24 horas sobre:
 - Qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais;
 - Qualquer descumprimento das obrigações contratuais relativas ao Tratamento dos Dados Pessoais;
 - Qualquer violação de segurança na contratada ou dos demais operadores;
 - Quaisquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais.
- Fornecer informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança.
- Definição clara quando à propriedade dos Dados Pessoais.
- Autorização da PREVIDÊNCIA USIMINAS quanto ao Tratamento de Dados Pessoais no exterior.
- Devolução dos Dados Pessoais, em até 30 dias, no caso de:
 - Solicitação da PREVIDÊNCIA USIMINAS;
 - Rescisão do contrato;
 - Término do Contrato.

- Direito de regresso diante de eventuais danos causados pela contratada em decorrência de descumprimento de contrato.

13. ATRIBUIÇÕES E RESPONSABILIDADES

13.1. DIRETORIA

- Cumprir e fazer cumprir esta Política e demais documentos que a compõem;
- analisar e aprovar a política de gestão de Dados Pessoais;
- Zelar para que a PREVIDÊNCIA USIMINAS esteja adequado à legislação de proteção de Dados Pessoais;
- Aprovar os investimentos em segurança da informação e proteção de Dados Pessoais, considerando a viabilidade, os custos, a técnica disponível e o Tratamento de Dados Pessoais;
- Analisar e aprovar, ou não, as exceções a esta Política, considerando os riscos que quaisquer exceções podem trazer à operação, caso vão de encontro às boas práticas em termos de proteção de Dados Pessoais.

13.2. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

- Elaborar e/ou revisar os procedimentos internos relativos à proteção de Dados Pessoais;
- Organizar e/ou ministrar treinamentos em proteção de Dados Pessoais aos Colaboradores ou prestadores de serviço;
- Analisar contratos que envolvam Tratamento de Dados Pessoais, seguindo o framework legal específico aplicável a cada situação em suas particularidades;
- Apoiar investigações para apuração de responsabilidade dos envolvidos em violações de Dados Pessoais e auxiliar na definição de aplicação das penalidades internas, quando necessário;
- Avaliar e auxiliar na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais;
- Manter mapeamento de fluxos de Dados Pessoais atualizado;
- Fazer cumprir a Tabela de Temporalidade;
- Desenvolver plano de análise e resposta a violações de Dados Pessoais que identifique o tipo de violação, o número de registros afetados, quais registros foram afetados e as categorias de Dados Pessoais envolvidas, as notificações apropriadas e plano de mitigação dos efeitos da violação;

- Receber as requisições dos Titulares dos Dados Pessoais sobre privacidade e proteção de Dados Pessoais, bem como as comunicações da Autoridade Nacional;
- Verificar a adequação das práticas e políticas da PREVIDÊNCIA USIMINAS no que se refere à transferência internacional de Dados Pessoais e ao manejo de Dados Pessoais Sensíveis.

13.3. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

- Definir controles para garantir a integridade, confidencialidade e disponibilidade dos Dados Pessoais, conforme preceituado pela lei;
- Definir os controles para garantir a existência de registros auditáveis de todo o ciclo de vida dos Dados Pessoais, desde o Consentimento para o Tratamento até o descarte, certificando-se que o descarte seja confirmado em dupla verificação, sempre que possível;
- Identificar e avaliar riscos relacionados à segurança da informação e proteção de Dados Pessoais e propor melhorias e recursos necessários;
- Analisar ou auxiliar na análise das violações de Dados Pessoais reportadas;
- Manter comunicação com o Encarregado pelo Tratamento de Dados Pessoais sobre os aspectos relevantes à segurança da informação e proteção de Dados Pessoais.

13.4. ÁREA DE TECNOLOGIA DA INFORMAÇÃO

- Cumprir e fazer cumprir esta Política e demais documentos que a compõem;
- Assegurar continuamente que todos os sistemas, serviços e equipamentos usados para o Tratamento de Dados Pessoais estejam dentro de um padrão aceitável de segurança;
- Analisar os aspectos técnicos de todo e qualquer produto ou serviço de terceiros que a PREVIDÊNCIA USIMINAS esteja considerando contratar para processar ou armazenar Dados Pessoais (exemplos: nuvem, hardware, equipamentos de rede);
- Atuar de forma coordenada com o Encarregado pelo Tratamento de Dados Pessoais e a Área de Segurança da Informação para viabilizar a implementação de procedimentos e rotinas necessárias para o Tratamento de Dados Pessoais, como a dupla verificação da exclusão de Dados Pessoais;
- Indicar Colaborador ou prestador de serviço para supervisionar cada sistema que contenha Dados Pessoais coletados, utilizados ou armazenados e garantir que as medidas necessárias e apropriadas para manutenção da confidencialidade, integridade e disponibilidade dos Dados Pessoais estejam sendo tomadas;
- Coletar e manter registros das atividades de Tratamento de Dados Pessoais, desde

evidências que comprovem o Consentimento dos Titulares dos Dados Pessoais (logs de Consentimento, por exemplo) até registro de utilização, compartilhamento, exclusão e outros, pelo período legal exigido conforme a Tabela de Temporalidade.

13.5. ÁREA JURÍDICA

- Participar previamente dos processos de contratação e aquisição de produtos e serviços da PREVIDÊNCIA USIMINAS, validando as minutas visando que atendam aos controles de proteção de Dados Pessoais aplicáveis;
- Apoiar o Encarregado pelo Tratamento de Dados Pessoais quanto a possibilidades de Tratamento de Dados Pessoais no exterior, auxiliando no entendimento de validação do nível de proteção de Dados Pessoais do país destino;
- Analisar, com apoio do Encarregado pelo Tratamento de Dados Pessoais, possibilidade de compartilhamento de Dados Pessoais para outros países, validando o nível de proteção de Dados Pessoais do país destino;
- Elaborar comunicados oficiais de respostas à Autoridade Fiscalizadora e Autoridades Judiciais Competentes, com apoio do Encarregado pelo Tratamento de Dados Pessoais;
- Fornecer orientação à Diretoria, aos Colaboradores ou aos prestadores de serviço, com apoio do Encarregado pelo Tratamento de Dados Pessoais, quanto a medidas a serem tomadas no caso de violação de Dados Pessoais.

13.6. ÁREA DE RECURSOS HUMANOS

- Promover, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, a cultura de proteção de Dados Pessoais na PREVIDÊNCIA USIMINAS, realizando campanhas de capacitação e divulgação da proteção dos Dados Pessoais;
- Assegurar a divulgação e a disponibilidade dos documentos que compõem esta Política e outras políticas internas para proteção de Dados Pessoais na PREVIDÊNCIA USIMINAS;
- Assegurar que os Colaboradores que tratam Dados Pessoais tenham assinado Cláusulas de Confidencialidade que incluam disposições específicas para o Tratamento de Dados Pessoais;
- Estipular controles de proteção de Dados Pessoais especificamente relacionados aos processos de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões).

13.7. ÁREA DE COMUNICAÇÃO

- Elaborar, com o apoio do Encarregado pelo Tratamento de Dados Pessoais, campanhas de conscientização e materiais de divulgação e alerta relacionados à proteção de Dados Pessoais;
- Analisar e aprovar a forma das comunicações relacionadas à proteção de Dados Pessoais;
- Responder, seguindo as orientações do Encarregado pelo Tratamento de Dados Pessoais, eventuais questionamentos de veículos de imprensa;
- Submeter à análise do Encarregado pelo Tratamento de Dados Pessoais textos e comunicados sobre privacidade e proteção de Dados Pessoais, antes de sua publicação.

13.8. GESTORES

- Cumprir, fazer cumprir e gerenciar o cumprimento desta Política e demais documentos complementares por parte de seus Colaboradores ou prestadores de serviço;
- Assegurar que qualquer Dado Pessoal só poderá ser recebido, tratado, excluído ou compartilhado por sua Área mediante notificação ao Encarregado pelo Tratamento de Dados Pessoais;
- Garantir a observação desta Política e da legislação competente pelos parceiros de negócio que recebam Dados Pessoais enviados por sua Área, devendo:
 - Obter documentos (procedimentos internos de segurança da informação, treinamento aplicado aos Colaboradores ou prestadores de serviços que manuseiam os Dados Pessoais, lista de controle de acesso, por exemplo) e garantias (acordo de confidencialidade assinado pelos Colaboradores, cláusulas contratuais, dentre outras) do parceiro de negócio que confirmem a segurança no manuseio dos Dados Pessoais sob responsabilidade da PREVIDÊNCIA USIMINAS;
 - Firmar Acordo de Confidencialidade com o parceiro de negócios;
 - Requerer, por meio de contrato, que o parceiro de negócios obtenha aprovação prévia e por escrito da PREVIDÊNCIA USIMINAS antes de qualquer subcontratação para fins de Tratamento de Dados Pessoais sob responsabilidade da PREVIDÊNCIA USIMINAS, independente de previsão legal nesse sentido;
 - Requerer, por meio de contrato, que o parceiro de negócios se abstenha de utilizar os Dados Pessoais sob responsabilidade da PREVIDÊNCIA USIMINAS para qualquer outro propósito, e que, após concluído o objeto do contrato, que sejam devolvidos e/ou eliminados todos os Dados Pessoais enviados ou compartilhados pela PREVIDÊNCIA

USIMINAS ao parceiro.

- Preparar e manter atualizada uma lista com todas as categorias de Dados Pessoais tratados em sua Área, e submeter essa lista ao Encarregado pelo Tratamento de Dados Pessoais;
- Assegurar que os Dados Pessoais são coletados, usados ou gerenciados apenas por Colaboradores ou prestadores de serviços autorizados, devendo:
 - Classificar os Dados Pessoais tratados em sua Área como confidenciais;
 - Aprovar acessos aos Colaboradores ou prestadores de serviço diretamente envolvidos nas atividades que demandam os Dados Pessoais;
 - Assegurar que os Colaboradores ou prestadores de serviço sob sua supervisão realizem treinamentos em proteção de Dados Pessoais e conheçam as políticas internas da PREVIDÊNCIA USIMINAS;
 - Atuar em parceria com as demais Áreas da PREVIDÊNCIA USIMINAS para identificar as vulnerabilidades e ameaças à proteção de Dados Pessoais nos processos e atividades de sua responsabilidade;
 - Assegurar que os Dados Pessoais sob a responsabilidade da PREVIDÊNCIA USIMINAS sejam utilizados com cuidado e de acordo com as orientações legais aplicáveis;
- Ao identificar violações de Dados Pessoais ou qualquer ação duvidosa, comunicar o Encarregado pelo Tratamento de Dados Pessoais imediatamente.

13.9. COLABORADORES E PRESTADORES DE SERVIÇO

- Cumprir e fazer cumprir, manter-se atualizado com esta Política e demais documentos que a compõem;
- Tratar os Dados Pessoais sob responsabilidade da PREVIDÊNCIA USIMINAS somente para fins autorizados, de forma ética e legal, respeitando os direitos do Titular dos Dados Pessoais e de acordo com as orientações desta Política e da legislação aplicável;
- Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos Dados Pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente estes Dados Pessoais, em qualquer local ou mídia, inclusive na Internet;
- Cumprir a legislação vigente e demais instrumentos regulamentares relacionados à proteção de Dados Pessoais;

- Reportar formalmente ao Encarregado pelo Tratamento de Dados Pessoais quaisquer eventos relativos à violação ou possibilidade de violação de Dados Pessoais ou atividades suspeitas de que tiver conhecimento;
- Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais na PREVIDÊNCIA USIMINAS;
- Reportar formalmente ao Encarregado pelo Tratamento de Dados Pessoais quaisquer eventos relativos à violação Dados Pessoais ou atividades suspeitas, por meio do e-mail: dpo@previdenciausimina.com.

14. DAS DISPOSIÇÕES FINAIS

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas e Procedimentos aplicáveis pela PREVIDÊNCIA USIMINAS.

Esta Política bem como os demais documentos que a complementam encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitados ao Encarregado pelo Tratamento de Dados Pessoais.

Qualquer dúvida relativa a esta Política deve ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais> por meio do e-mail: dpo@previdenciausiminas.com

Esta Política entra em vigor na data de sua publicação.

15. DEFINIÇÕES

- **Agente de Tratamento:** O controlador e o operador;
- **Anonimização:** Utilização de meios técnicos razoáveis e disponíveis no momento do Tratamento para retirar a possibilidade de associação, direta ou indireta, do Dado Pessoal a um indivíduo.
- **Ambiente Lógico:** Ambiente virtual composto pelos Recursos de TIC, sistemas, bases de Dados, da PREVIDÊNCIA USIMINAS, de forma intangível.
- **Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano à PREVIDÊNCIA USIMINAS.
- **Ativo:** É qualquer coisa que tenha valor material ou imaterial, sendo tangível ou intangível, para a PREVIDÊNCIA USIMINAS e precisa ser adequadamente protegido.
- **Ativo Tangível:** caracteriza-se por possuírem um corpo físico.
- **Ativo Intangível:** Todo elemento que possui valor para PREVIDÊNCIA USIMINAS e que

esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando a Dados, reputação, imagem, marca e conhecimento.

- **Autenticidade:** Garantia de que a informação foi criada, editada ou emitida por quem se disse ter sido, sendo capaz de gerar evidências não repudiáveis em relação ao criador, editor ou emissor.
- **Autoridade competente:** Órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da Lei de Proteção de Dados Pessoais aplicável.
- **Backup:** Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de restauração ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada da PREVIDÊNCIA USIMINAS.
- **Banco de Dados:** Conjunto estruturado de Dados, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **Colaborador:** Empregado, estagiário, menor aprendiz, ou qualquer outro indivíduo ocupante de cargo ou emprego na PREVIDÊNCIA USIMINAS.
- **Ciclo de Vida do Dado Pessoal:** Fluxo do Tratamento do Dado Pessoal, que envolve as ações de Coleta, Armazenamento, Uso, Compartilhamento e Eliminação do Dado Pessoal.
- **Compartilhamento de Dados Pessoais:** Comunicação, difusão, transferência nacional ou internacional, interconexão de Dados Pessoais ou Tratamento compartilhado de bancos de Dados Pessoais por órgãos, entidades ou pessoais, e para uma ou mais modalidades de Tratamento.
- **Confidencialidade:** Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não autorizados.
- **Consentimento:** Manifestação livre, informada e inequívoca pela qual o Titular dos Dados Pessoais concorda com o Tratamento de seus Dados Pessoais para uma finalidade determinada.
- **Controlador:** Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.
- **Credencial de Acesso:** É a identificação do Colaborador ou prestador de serviço em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token

e biometria.

- **Dado anonimizado:** Dado que não identifica de forma direta ou indireta um Titular dos Dados Pessoais, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu Tratamento.
- **Dado Pessoal:** Informação relacionada à pessoa física identificada ou identificável. Para os propósitos desta Política, os Dados Pessoais são classificados como Informação Confidencial.
- **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 física.
- **Dados de saúde:** Dados Sensíveis que permitem inferir informações referentes à saúde do Titular.
- **Disponibilidade:** Garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.
- **Dispositivos móveis:** equipamentos que podem ser facilmente transportados devido a sua portabilidade, com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexões com a Internet e outros sistemas, redes ou qualquer dispositivo.
- **Dispositivos removíveis de armazenamento de informação:** Dispositivos capazes de armazenar informações que pode ser removida do equipamento, possibilitando a portabilidade dos Dados, como CD, DVD, pen drive e HD externo.
- **Encarregado pelo Tratamento de Dados Pessoais:** Pessoa jurídica indicada pela PREVIDÊNCIA USIMINAS e que atua como canal de comunicação entre a PREVIDÊNCIA USIMINAS com os Titulares dos Dados Pessoais ou a Autoridade Fiscalizadora.
- **Homologação:** Processo de avaliação e aprovação técnica de Recursos de TIC para serem utilizados dentro do ambiente da PREVIDÊNCIA USIMINAS.
- **Identidade Digital:** É a identificação do Colaborador ou prestador de serviço em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.
- **Incidente de Segurança da Informação e Comunicação:** Ocorrência identificada de um estado de sistema, Dados, informações, serviço ou rede que indica possível violação à Política de Segurança da Informação e Comunicação ou documentos complementares, falha de

controles ou situação previamente desconhecida e que possa ser relevante à Segurança da Informação.

- **Informação:** É o conjunto de Dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.
- **Integridade:** Garantia de que as informações estejam fidedignas em relação à última alteração desejada durante o seu ciclo de vida.
- **Internet:** Rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente.
- **Legalidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.
- **Operador:** Pessoa física ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador.
- **Pseudonimização:** é o Tratamento por meio do qual um Dado Pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
- **Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC):** Hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.
- **Relatório de Impacto à Proteção de Dados Pessoais:** Documento que contém a descrição dos processos de Tratamento de Dados Pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos Titulares dos Dados Pessoais, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos.
- **Requisições dos Titular dos Dados Pessoais:** Requisição do Titular dos Dados Pessoais acerca de seus direitos estabelecidos em lei e relativos ao Tratamento dos seus Dados Pessoais.
- **Risco:** Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.
- **Segurança da Informação e Comunicação:** É a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a

informação e os Recursos de TIC que as contêm dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos às atividades em caso de incidentes, além de maximizar o retorno dos investimentos e de novas oportunidades de transação.

- **Sigilo profissional:** Trata da manutenção de segredo para informação valiosa, cujo domínio de divulgação deva ser fechado, ou seja, restrito a um cliente, a uma organização ou a um grupo, uma vez que a ele é confiada a manipulação da informação.
- **Tentativa de Burla:** Atos que busquem violar as diretrizes estabelecidas nos documentos normativos da PREVIDÊNCIA USIMINAS e sejam frustrados por erro durante o planejamento ou durante sua execução.
- **Titular dos Dados Pessoais:** Pessoa física a quem se referem os Dados Pessoais que são objeto de Tratamento.
- **Tratamento de Dados Pessoais:** toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- **Violação:** Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos da PREVIDÊNCIA USIMINAS.
- **Violação de Dados Pessoais:** Destruição, perda, alteração, divulgação acidental ou ilegal, não autorizada ou acesso a Dados Pessoais transmitidos, armazenados ou de outra forma processados, resultante de incidente.