Sumário

1. OBJETIVO: 2
2. ABRANGÊNCIA – PÚBLICO ALVO: 2
3. SIGLAS E NOMECLATURAS: 2
4. REFERÊNCIAS NORMATIVAS: 3
5. PAPEIS E RESPONSABILIDADES 4
5.1 Riscos & Compliance 5
5.2 DPO: 5
5.3 CGPSI: 7
5.4 Pessoas e Perfomance: 7
5.5 Titular de Dados: 8
6. DIRETRIZES 8
6.1 Privacy by Design: 9
6.2 Matriz Principiológica: 9
6.3 Registro de Operações de Tratamento de Dados: 10
6.4 Segurança da Informação: 11
6.5 Transparência: 12
6.6 Gestão de Consentimento: 12
6.7 Relação com terceiros: 12
6.8 Ciclo de vida dos Dados Pessoais: 13
6.8.1 Coleta: 13
6.8.2 Armazenamento: 13
6.8.3 Uso: 14
6.8.4 Exclusão e Descarte: 14
6.8.5 Tratamento de Dados Sensíveis: 14
6.8.6 Compartilhamento e Transfêrencia Internacional de Dados: 15
6.9 Condições minimas para parceiros de negócio e suprimentos: 16
6.10 Gestão de Riscos para Privacidade e Dados Pessoais: 17
6.10.1 Relatório de Análise de Impacto - RIPDP: 17
6.10.2 Incidentes de Privacidade e Dados Pessoais: 17
7. SANÇÕES 18
8. VIGÊNCIA E REVISÃO 18

1. OBJETIVO:

A Política Corporativa para gestão de Privacidade de Dados Pessoais estabelece instruções e diretrizes para assegurar conformidade com a Lei Geral de Proteção de Dados (LGPD) 13.709/2018.

Também tem o intuito de observar e adaptar para aplicação as diretrizes internacionais de Proteção de Dados pessoais de acordo com as melhores práticas de mercado.

Esclarecendo ainda as responsabilidades dos cooperados, colaboradores, terceiros, parceiros e fornecedores no cumprimento destas conformidades.

Sendo o intuíto principal:

- Estar em conformidade com as leis e regulamentos aplicáveis de Proteção de Dados Pessoais, seguindo sempre as melhores práticas dentro da realidade da Up Brasil;
- Proteger os direitos dos Colaboradores, clientes, fornecedores e parceiros contra os riscos, vulnerabilidades e violação aos seus Dados Pessoais;
- Ser transparente com relação aos procedimentos da Companhia no Tratamento de Dados Pessoais;
- Promover a conscientização em toda a Companhia em relação à proteção de Dados Pessoais e questões de Privacidade.

2. ABRANGÊNCIA – PÚBLICO ALVO:

Abrange qualquer processo e atividade que tratem, utilizem ou armazenem dados pessoais no ecossistema de negócios da UP Brasil, seja ele tecnológico ou digital.

Tanto dos dados pessoais na qual a UP Brasil é Controladora, Operadora, Controladora Conjunta (ou Co-Controladora) e Controladora por sucessão.

A Política e suas diretrizes se aplicam a toda UP Brasil incluindo seus usuários, clientes, colaboradores, estagiários, terceiros, prestadores de serviço, temporários, parceiros de negócios e fornecedores que tenham acesso ainda que minimamente a Dados Pessoais no ambiente Up Brasil.

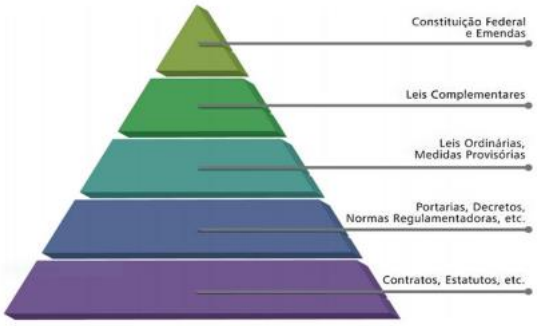
3. SIGLAS E NOMECLATURAS:

- **Anonimização:** Utilização de meios técnicos na qual o dado pessoal perde a característica de identificação direta ou indiretamente, passando a ser considerado um dado não pessoal;
- **ANPD:** Agência Nacional de Proteção de Dados que é a autarquia pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
- **Base Legal:** Hipótese legal que autoriza o tratamento de Dados Pessoais;
- **Colaborador:** Funcionário da Up Brasil;
- **Controlador de Dados Pessoais:** Pessoa Física ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais;

- **Co-Controlador de Dados Pessoais:** Se caracteriza uma relação de responsáveis solidários de dados pessoais quando, dois ou mais controladores determinarem conjuntamente os propósitos e meios de processamento, eles devem ser considerados controladores conjuntos e, por consequência, determinarem seu escopo de responsabilidade no cumprimento das obrigações legais, especialmente no que tange ao exercício dos direitos do titulares de dados e o fornecimento de informações por meio de acordo entre eles;
- **Controlador por sucessão:** É o controlador que se torna exclusivamente responsável pelos Dados Pessoais após o compartilhamento, seja devido a obrigação contratual ou por obrigações derivadas de atividades previstas no contrato;
- **Dados Pessoais:** É uma informação relacionada a pessoa natural que a torne identificada ou identificável;
- **Dados Pessoais Sensíveis:** São aqueles dados que identificam a pessoa como ser único, suas particularidades e nuances, dados como, cunho religioso, política, orientação sexual, entre vários outros;
- **Destinatário:** Pessoa física ou jurídica, autoridade pública, agência ou qualquer outro órgão a quem os dados pessoais são divulgados, independentemente de ser um terceiro ou não, no entanto, as autoridades que podem receber dados no âmbito de um inquérito especifico não serão consideradas destinatárias;
- **DPO ou Encarregado:** Pessoa física ou jurídica, responsável por atuar como um canal de comunicação entre o controlador, os titulares de dados e a ANPD;
- **LGPD:** Lei Geral de Proteção de Dados nº 13.709 promulgada em agosto de 2018, que versa principalmente sobre o tratamento de dados pessoais, tendo como objetivo principal defender os titulares dos dados e ao mesmo tempo regular o uso dos dados para finalidades diversas;
- **Operador de Dados Pessoais:** O responsável seja ele pessoa física ou jurídica pelo tratamento de dados pessoais em nome do controlador;
- **Pseudonimização:** É o tratamento por meio do qual um dado perde a possibilidade de associação direta ou indireta junto ao titular de dados, seja por meio de uso de informação adicional que é mantida separadamente pelo controlador em ambiente controlado e seguro;
- **Terceiro:** É todo aquele que não possui vínculo com a UP Brasil, seja ele comercial, empregatício ou de fornecimento que permita posse de seus dados, como por exemplo: Envio de currículos;
- **Titular de dados:** É a pessoa física dona dos dados fornecidos;
- **Tratamento de Dados Pessoais:** É toda e qualquer operação que envolvam dados pessoais, como por exemplo, a coleta, produção, recepção, classificação, utilização, armazenamento, acesso, reprodução, transmissão, processamento, arquivamento, modificação, entre outros.

4. REFERÊNCIAS NORMATIVAS:

A estrutura normativa desta política é composta por um conjunto de leis e normas brasileiras, com níveis hierárquicos distintos, relacionados à seguir, lembrando que normas do mesmo nível hierárquico estão em linha linear, salvo exceção quando uma delas legislar ou tratar sobre fato específico.



As seguintes normas e normativas nortearam essa política:

- **Lei 13.709/2018 –** Publicada em 14 de agosto de 2018 pela Presidência da República, dispõe sobre Proteção de Dados Pessoais;
- **Lei 12.965/2014 –** Publicada em 23 de julho de 2014 pela Presidência da República, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil;
- **Lei 12.527/2011 –** Publicada em 18 de novembro de 2011, é conhecida como a Lei de Acesso à Informação;
- **Portaria nº 93 –** Publicada em 26 de setembro de 2019 – Glossário de Segurança da Informação;
- **Norma ABNT NBR ISO/IEC 27001:2013 –** Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de Segurança da Informação;
- **Norma ABNT NBR ISO/IEC 27002:2013 –** Tecnologia da informação – Técnicas de Segurança – Código de prática para controles de segurança da informação;
- **Norma ABNT NBR ISO/IEC 29100:2020 –** Tecnologia da informação – Técnicas de Segurança – Estrutura de Privacidade;
- **Norma ABNT NBR ISO/IEC 27701:2019 –** Técnicas de Segurança – Extensão da ABNT NBR ISO/27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e Diretrizes.

5. PAPEIS E RESPONSABILIDADES

A UP Brasil está compromissada no tratamento compliance de dados pessoais, sejam de colaboradores, parceiros, terceiros, clientes e fornecedores, buscando preservar os seguintes direitos:

- Integridade;
- Privacidade;
- Confidencialidade;
- Conformidade legislativa e regulatória.

Como parte integrante da UP Brasil, nossos colaboradores, gestores e corpo diretivo, devem sempre no exercício de suas atividades, garantir que dados pessoais sejam tratados em conformidade com as diretrizes desta política.

Os Colaboradores da UP Brasil devem familiarizar-se, aderir e praticar as diretrizes contidas nesta política, bem como nos procedimentos e padrões relacionados a Gestão de Privacidade e Dados Pessoais.

5.1 Riscos & Compliance

Ser responsável pela Gestão de Privacidade e Dados pessoais na UP Brasil, fornecendo subsídios de Governança e Operacionais para adequação e manutenção do SGSI.

É responsável pela Governança de Privacidade de Dados e Segurança da Informação, tendo como atividades:

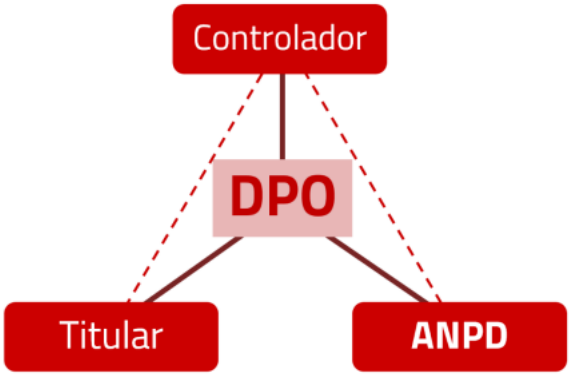
- Criação, Revisão e Atualização de Políticas voltadas ao SGSI;
- Criação e Aplicação do Treinamento anual de Privacidade de Dados para UP Brasil;
- Identificação de pontos de melhoria no ecossistema de Privacidade de Dados;
- Responsável pelo elaboração do Data Mapping anual ou sempre que necessário, conduzindo as entrevistas com as áreas;
- Criação dos relatórios RIPDP (Relatório de Impacto de Proteção de Dados Pessoais) e LIA (Relatório de viabilidade e identificação do legítimo interesse nas tratativas de dados pessoais);
- Acompanhamento de auditorias ligadas a Segurança da Informação e Privacidade de Dados;
- Responsável pela Governança de Segurança da Informação;
- Responsável pela Gestão de Riscos de Fornecedores que envolvam a tratativas de dados pessoais e/ou corporativos que impactem a Privacidade de Dados ou a Segurança da Informação;
- Responsável pelo atendimento das solicitações de titulares de dados com a orientação do DPO;
- Responsável pelo apoio estratégico na implementação da gestão de consentimento e cookies nas plataformas e sites UP Brasil;
- Análise legislativa referente a normativos e leis ligados à privacidade de dados;
- Responsável pela emissão do relatório anual de privacidade de dados;
- Demais rotinas ligadas ao dia a dia da Privacidade de dados;
- Desenvolver e publicar internamente o relatório de impacto de tratamento de dados pessoais anualmente;
- Acompanhar e monitorar evolução de leis e regulações relacionadas a gestão de privacidade e dados pessoais;
- Revisar, monitorar e aprovar registros de tratamento de dados pessoais.

5.2 DPO:

É a pessoa indicada pelo CGPSI e CODIR para representar a UP Brasil, atuando como um canal de comunicação entre a UP Brasil, os Titulares dos

Dados e a Autoridade Nacional de Proteção de Dados.

Ele deve possuir independência para orientar de maneira técnica e embasar as decisões corporativas para que estejam aderentes com a Legislação de Proteção de Dados Pessoais.



As responsabilidades do Encarregado de Dados incluem, mas não se limitam a:

- Apoiar, aconselhar, monitorar e fiscalizar o Comitê de Gestão de Privacidade e Segurança da Informação;
- Acompanhar a manutenção e revisão anual das normas e políticas de privacidade e dados da UP Brasil, incluindo esta política, garantindo a geração de histórico e evidências;
- Garantir a realização, acompanhar e monitorar auditorias internas e anuais externas, para a gestão de privacidade e dados pessoais;
- Fiscalizar o cumprimento das normas e políticas de privacidade da UP Brasil;
- Acompanhar e monitorar eventos externos de interesse relativo a LGPD 13.709/2018, tais como incidentes, publicações, notícias e tendências;
- Garantir a apresentação de relatório de impacto de tratamento de dados pessoais a ANPD e/ou outras entidades pertinentes no caso da obrigação legal ou quando solicitados por força maior;
- Acompanhar e monitorar evolução de leis e regulações relacionadas a gestão de privacidade e dados pessoais;
- Manter-se atualizado e interagir com a equipe de Segurança da Informação sobre aspectos de proteção de dados pessoais e monitoramento de incidentes de SI;
- Manter a alta direção informada sobre aspectos internos da gestão de privacidade e dados pessoais;
- Comunicar a alta direção imediatamente a ocorrência de incidentes e mantê-los atualizados sobre o estado de tratamento destes;
- Comunicar à ANPD incidentes de relevância de acordo com o procedimento para Gestão de Incidentes;
- Acompanhar, monitorar e propor medidas corretivas para os processos associados a Direitos do Titular;
- Acompanhar e monitorar em conjunto com o Comitê de Gestão de

Privacidade e Segurança da Informação, o nível de conformidade da UP Brasil, para com os princípios e requisitos da LGPD 13.709/2018 e diretrizes desta política;

- Estabelecer processo contínuo de comunicação interna com a Alta Direção sobre o nível de conformidade da organização, indicadores de gestão de incidentes e relatórios de impacto;
- Impulsionar a cultura de privacidade na organização por meio da conscientização, interação com os departamentos, promoção de atividades específicas, entre outros.

5.3 CGPSI:

O Comitê De Governança, Privacidade e Segurança da Informação é responsável pela governança de privacidade e dados pessoais na UP Brasil.

Deve ainda estabelecer e acompanhar a implementação dos controles desta Política e dos procedimentos ligados a Privacidade de Dados e Segurança da Informação.

As principais responsabilidades do CGPSI são:

- Assegurar e zelar pela manutenção adequada e suficiente do Programa de Gestão de Privacidade e Dados Pessoais, de acordo com os controles internos estabelecidos na Declaração de Aplicabilidade;
- Aprovar a revisão desta política;
- Fiscalizar o cumprimento das diretrizes desta política;
- Monitorar o nível de conformidade da organização por meio da apresentação Bimestral de KPI's, definindo e aprovando planos de ação para correção de lacunas;
- Acompanhar o desempenho do tratamento de incidentes de privacidade ou segurança.

As demais responsabilidades e diretrizes deste comitê estão detalhadas no Regimento Interno do Comitê (Estatuto-Regimitento-Interno-Comitê-CGPSI-Vfinal).

O CGPSI é responsável pelo esclarecimento de dúvidas, recepção e tratativa de sugestões relativas a esta política. Dúvidas, sugestões e relatos de incidentes devem ser enviados para o endereço: lgpd@upbrasil.com ou comunicadas através dos canais de atendimento da UP Brasil.

Exceções a esta política devem ser apresentadas a gerência imediata do colaborador, a qual deverá submetê-las ao Comitê de Gestão de Privacidade e Segurança da Informação, onde serão discutidas e avaliadas. Caso necessário, a exceção será submetida para apreciação da Alta Direção.

5.4 Pessoas e Perfomance:

A área de pessoas e perfomance é responsável por fomentar a criação de um ecossistema seguro, baseado na cultura de proteção de dados pessoais, por meio do estabelecimento de uma programa de conscientização das partes interessadas acerca das diretrizes e procedimentos de proteção de dados pessoais.

Deve garantir que todos os colaboradores recebam orientações sobre esta Política antes da contratação e treinamentos especificos durante a vigência da relação trabalhista.

No processo de seleção e recrutamento, o candidato recebe informações sobre os requisitos e sensibilidade do tratamento de dados pessoais na Up Brasil. Todos os contratados devem receber treinamento introdutório (integração) sobre a gestão de privacidade e dados pessoais, incluindo conceitos básicos sobre a LGPD.

O time de Pessoas e Perfomance deve garantir e armazenar registro de participação dos colaboradores nos treinamentos e eventos de Privacidade e Dados Pessoais, se responsabilizando também pela efetividade anual de participação de 100% dos colaboradores.

5.5 Titular de Dados:

É a pessoa física dona dos dados fornecidos. A UP Brasil deverá garantir pleno atendimento aos Direitos do Titular estabelecidos na LGPD por meio da disponibilização de recursos humanos, de tecnologia e canais de comunicação para tal finalidade.

É condição primária para o atendimento ao Direito do Titular a verificação e aplicação de meios para tal de identidade do Titular solicitante.

A Up Brasil através do procedimento de direitos do titular as etapas e responsabilidades para cumprimento da obrigação legal referente a:

- Confirmação da existência do Tratamento: É o direito do titular de confirmar se a empresa realiza algum tratamento sobre seus dados pessoais;
- Acesso aos dados: É o direito do titular de obter uma cópia de seus dados pessoais que são tratados pela empresa;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados: É direito do titular saber com quem (quais terceiros) os seus dados estão sendo compartilhados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o dispositivo;
- Eliminação dos dados pessoais tratados com o consentimento do Titular, exceto nas hipóteses previstas no art. 16 da LGPD;
- Revogação do consentimento;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comerciais e industriais.

6. DIRETRIZES

Em detrimento do que é solicitado legalmente e por seus compromissos assumidos nesta política, a UP Brasil seguirá em seus processos as seguintes diretrizes derivadas dos princípios e fundamentos legais:

6.1 Privacy by Design:

A Up Brasil aplicará conceitos e práticas para estabelecer e evidenciar o princípio da prevenção, por meio de segurança desde a concepção e por padrão (default). As diretrizes para esta abordagem estão definidas no escopo de Privacy by Design e Security by Design. Sendo responsabilidade das áreas de Tecnologia da Informação e Riscos & Compliance garantir esta abordagem por meio de aplicação de tecnologia em todos os sistemas e aplicações da UP Brasil durante o ciclo de desenvolvimento ou no processo de aquisição.

Tem como objetivo entregar os maiores nível de privacidade quanto possível e assegurar que dados privados sejam automaticamente protegidos em qualquer sistema de TI ou prática de negócios. Desta forma o titular não precisa ter nenhuma ação para que sua privacidade permaneça intacta, ela já faz parte da essência do sistema por padrão e, portanto, nenhuma ação por parte do usuário é necessária para preservá-la por meio de:

- Especificação do propósito;
- Limitação da coleta;
- Minimização dos dados;
- Limitação no uso, retenção e divulgação.

Todo e qualquer projeto que envolva dados pessoais deve passar pelo fluxo de validação de Riscos & Compliance e DPO antes de seguir com o desenvolvimento, o check-list de ações que os projetos devem seguir estão previstos no Escopo de Privacy by Design aprovado em 10/06/2022.

6.2 Matriz Principiológica:

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes principios:

I. **BOA-FÉ OBJETIVA:** Significa uma atuação “refletida”, pensando no outro (Titular), exercendo a empatia, respeitando seus interesses legítimos, suas expectativas razoáveis, seus direitos, agindo com lealdade, sem abuso, sem obstrução, sem causar lesão ou desvantagem excessiva, gerando para atingir a boa finalidade das obrigações, o cumprimento do objetivo contratual e a realização de interesses das partes. O tratamento de dados deve pautar-se nas boas intenções, na moral e bons costumes aceitos pela sociedade;

II. **FINALIDADE:** Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Dados pessoais não poderão ser coletados para uma finalidade e depois utilizados para outra;

III. **Adequação:** Compatibilidade do tratamento com as finalidades informadas ao Titular, de acordo com o contexto do tratamento;

IV. **Necessidade:** Limitação do tratamento no mínimo necessário para a realização de suas finalidades, com a abrangência dos dados pertinentes, proporcionais e não excessivos em relação

às finalidades do tratamento de dados;

V. **Livre Acesso:** Garantia, aos titulares, consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem com sobre a integralidade de seus dados pessoais;

VI. **Qualidade:** Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VII. **Transparência:** Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comerciais e industriais;

VIII. **Segurança:** Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

IX. **Prevenção:** Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

X. **Não Discriminação:** Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

XI. **Responsabilização e prestação de contas:** Demonstração, pelo agente, 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.

6.3 Registro de Operações de Tratamento de Dados:

É responsabilidade do gestor de cada departamento garantir, manter e revisar anualmente o inventário de dados dos processos de tratamento de dados pessoais ou em caso de eventos excepcionais, incluindo:

- Ocorrência de incidentes graves;
- Alteração de processos que envolvam tratamento de dados pessoais;
- Recomendação de auditorias internas ou externas;
- Solicitação do Encarregado de Dados ou CGPSI**.**

O registro das operações de tratamento de dados pessoais deve ser realizado conforme procedimento para gestão de inventário de dados pessoais e conter os seguintes campos:

I. Nome completo do responsável pelo tratamento de dados pessoais (processo);
II. Nome da área/departamento;
III. Identificação do processo;
IV. Informação de como os dados são coletados;
V. Finalidade do tratamento;
VI. Base legal que suporta o tratamento;
VII. Dados pessoais envolvidos no tratamento;

VIII. Dados sensíveis envolvidos no tratamento;
IX. Descrição das etapas do tratamento;
X. Informações sobre o local de armazenamento dos dados (localmente, nuvem de terceiro, co-location em ambiente externo, entre outros).
XI. Período de retenção dos dados pessoais;
XII. Entidades envolvidas no compartilhamento e/ou transferência;
XIII. Aspectos de Segurança da Informação relacionados ao tratamento de dados pessoais;
XIV. Nível de risco do processo de tratamento de dados pessoais;

É responsabilidade da área de Tecnologia da Informação garantir a existência de registro sistêmico (logs) das operações básicas de coleta, inserção, alteração, consulta e exclusão de dados pessoais em bancos de dados, de acordo com os requisitos de cada processo de tratamento de dados pessoais. Essa garantia deve ser aplicada para sistemas e/ou aplicações desenvolvidas internamente e/ou contratadas via fornecedores externos, por meio de cláusulas contratuais com fornecedores externos, que devem garantir e preservar a existência das operações básicas.

6.4 Segurança da Informação:

Os dados pessoais serão tratados de forma segura, protegidos do tratamento não autorizado ou ilícito e contra sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

A UP Brasil dispõe de uma Política de Segurança da informação que especifica e determina a adoção de conjunto de medidas técnicas e administrativas de segurança para a proteção de dados pessoais contra acessos não autorizados e situações acidentais, ou incidentes culposos ou dolosos de destruição, perda, adulteração, compartilhamento indevido ou qualquer forma de tratamento inadequado ou ilícito.

Manterá procedimentos e ferramentas implementadas, os quais seguem padrões das normas técnicas de Segurança da Informação e diretrizes da DSC-007 Política de Segurança da Informação. As boas práticas adotadas para proteção de dados pessoais deverão ser objetos de campanhas informativas na UP Brasil, seus sites, aplicativos, fornecedores, visando disseminar a cultura protetiva com conscientização e sensibilização dos interessados.

O CGPSI, o DPO e a área de Segurança da Informação da UP brasil deverão trabalhar em conjunto para garantir a Segurança da Informação dos dados pessoais de acordo com o nível de riscos e controles requeridos, maximizando a prevenção a exposições de dados indevida, vazamentos e acesso indevido. Também deverão garantir a consonância entre as políticas de gestão de privacidade e segurança da informação.

Para garantir que as medidas de segurança implementadas pela UP Brasil se mantenham sempre atualizadas e em consonância com as melhores práticas e ferramentas disponíveis atualmente no mercado, estas políticas e procedimentos devem ser revisados e auditados periodicamente, em prazos não superiores a 12 (doze) meses, identificando e corrigindo eventuais falhas.

6.5 Transparência:

Todas as atividades de tratamento de dados realizadas pela UP Brasil na condição de controladora e/ou operadora, devem pautar-se nos princípios de governança de privacidade e dados pessoais, observando especialmente a transparência neste tratamento por meio de avisos de privacidade internos e externos.

Os avisos ou políticas de privacidade, termos de uso dos serviços, coleta e uso de cookies devem constar nos portais web, sistemas e aplicativos para equipamentos de mobilidade (smartphone, notebook, tablet, smartwatch e outros).

Os avisos de privacidade devem passar por aprovação formal do Encarregado de Dados e/ou CGPSI.

6.6 Gestão de Consentimento:

O consentimento é uma das bases legais que podem suportar o tratamento de dados pessoais. Devendo ser de manifestação livre, informada e inequívoca:

- **Manifestação Livre:** O Titular deve fornecer o consentimento de maneira livre, sem que seja obrigado para tanto para, por exemplo, usufruir do serviço/produto relacionado;
- **Manifestação Informada:** O Titular teve acesso ao aviso de privacidade correspondente a atividade na qual foi sujeito, antes do fornecimento de sua autorização, garantindo possuir plena ciência da finalidade e dos limites da atividade de tratamento realizada;
- **Manifestação Inequívoca:** O Titular forneceu os seus dados pessoais, sem qualquer dúvida ou questionamento quanto aos limites da atividade. O Titular forneceu a sua autorização (consentimento) para que fosse realizado o tratamento em situações específicas e determinadas.

É responsabilidade do Time de Tecnologia da Informação garantir o registro do consentimento dos processos de tratamento de dados pessoais que possuam este como base legal, sob a orientação estratégica do time de Riscos & Compliance. Bem como da existência de direito a revogação para o titular de dados.

É responsabilidade da área de Tecnologia da Informação fornecer recursos automatizados para a gestão de consentimento.

6.7 Relação com terceiros:

A Lei Geral de Proteção de Dados positiva a responsabilização Civil no caso de Danos, sejam eles, individuais, coletivos morais ou até mesmo patrimoniais, estabelecendo que todos os agentes de tratamento de dados pessoais possuem responsabilidade solidária.

Nesse sentido, a UP Brasil é responsável pelas ações de terceiros, devendo o dever de empregar as melhores metodologias e automatizações afim

de avaliar, verificar e garantir que os terceiros são aderentes as legislações de proteção de dados aplicáveis.

Ações de adequação a terceiros:

- Garantir que todos os contratos com terceiros constem, cláusulas referentes a proteção de dados pessoais, estabelecendo deveres e obrigações envolvendo a temática, e atestando a aderência destes com as legislações de dados em vigência em nosso pais;
- Solicitar que todos os terceiros assinem o termo de aceitação desta política assim como as de Segurança de Informação e o Plano de Resposta a Incidentes de Segurança.

6.8 Ciclo de vida dos Dados Pessoais:

Todos os processos de tratamento de dados pessoais da UP Brasil devem seguir os princípios diretrizes estabelecidas nesta Política. As etapas contidas no ciclo de vida dos dados pessoas são: coleta, armazenamento, uso, exclusão e/ou descarte.

6.8.1 Coleta:

O procedimento de coleta de dados pessoais deverá ser restrito aqueles essencias (mínimos) para o cumprimento da finalidade primária, determinada e informada ao Titular dos Dados, sempre observando a necessidade de manter atualizados os dados coletados.

Sempre que coleta for realizada em pontos ativos (onde os titulares fornecem seus próprios dados), os titulares dos dados pessoais deverão ser informados, antes da coleta, de todos os detalhes sobre a atividade de tratamento, observando os requisitos de transparência.

Dados pessoais somente poderão ser coletados em pontos passivos (através de acesso a bases públicas/privadas de dados, por exemplo) se tais bases forem notoriamente fidedignas (atribuídas a órgãos ou entidades públicas e oficiais), se existir um contrato entre o provedor da base e a UP Brasil, ou mediante expressa autorização do DPO ou do CGPSI.

Dados fornecidos por terceiros somente poderão ser recebidos mediante celebração de contrato que inclua cláusula de privacidade robusta o suficiente, conforme orientações do departamento jurídico e do DPO, que deverão verificar a idoneidade de todos os terceiros que fornecerem dados a UP Brasil. Nestes casos, os dados pessoais deverão possuir uma descrição completa do seu ciclo de vida, antes da realização do compartilhamento à UP Brasil, garantindo que, em nenhuma destas etapas, tenha ocorrido qualquer forma de tratamento ilícito ou inadequado.

6.8.2 Armazenamento:

O armazenamento de dados pessoais deverá ser realizado pelo tempo mínimo necessário para atendimento da finalidade pretendida e cumprimento de eventuais obrigações legais que regulam determinada atividade de tratamento, seguindo a matriz de temporalidade e inventário de dados pessoais da UP Brasil.

Os dados deverão ser armazenados, seguindo meios adequados, abaixo

especificados:

- **Dados pessoais em formato físico:** O armazenamento de formulários e documentos em papel deve considerar repositórios, como armários e gavetas com trancas, acesso físico controlado e monitorado;
- **Dados pessoais em formato eletrônico:** O armazenamento de dados pessoais, em especial dados pessoais sensíveis, de criança e adolescente, devem considerar técnicas de pseudonimização. Mecanismos de controle e segregação de acessos devem ser empregados para assegurar a confidencialidade dos dados pessoais.

6.8.3 Uso:

O uso dos dados pessoais está associado, mas não se limite a: leitura, acesso, alteração, reuso, compartilhamento, transporte e revisão. A utilização dos dados pessoais deverá estar baseada nos princípios da finalidade, adequação e necessidade.

Limitada à expectativa que o titular dos dados possuía na realização da coleta das informações. Na eventual hipótese de necessidade de alteração da finalidade previamente informada ao titular, este deverá ser novamente informado sobre as intenções da Up Brasil, avaliando a necessidade de qualquer adequação. O mesmo dado jamais poderá ser utilizado para outra finalidade exceto com nova autorização do titular de dados.

6.8.4 Exclusão e Descarte:

Sendo cumprida a finalidade e obserdados os prazos legais de necessária retenção da informação, os dados deverão ser descartados, o que por sua vez deverá seguir meios adequados, abaixo especificados:

- **Dados pessoais em formato físico:** O descarte deverá ser realizado por meio de fragmentadoras de papel ou incineração acompanhada e registrada, sendo proibido o descarte direto em lixeiras;
- **Dados pessoais em formato eletrônico:** O descarte deverá ser realizado preferencialmente através de limpeza/exclusão em bancos de dados, e ou quaisquer outros tipos de arquivo.

6.8.5 Tratamento de Dados Sensíveis:

A Lei Geral de Proteção de Dados define as seguintes informações como dados pessoais sensíveis:

I. Origem racial ou étnica;
II. Convicção Religiosa;
III. Opinião Política;
IV. Filiação a Sindicato ou a organização de Carácter religioso, filosófico ou político;
V. Dados referente à saúde ou à vida sexual;
VI. Dados Genéticos ou Biométricos quando relacionados a um indivíduo.

O tratamento envolvendo dados pessoais sensíveis deverão receber

máxima prioridade na Segurança e armazenamento, devendo em todos novos projetos que envolva tais dados, ter o time de Riscos & Compliance envolvido para que possa atuar de maneira consultiva sobre a análise dos riscos e ter orientações de boa prática para manipulação de dados sob a ótica do Privacy by Design.

O processo de exclusão ou anonimização após a perda de finalidade, deve acompanhar a política de temporalidade e quando esta não for possível de ser cumprida por razões fundamentadas, a guarda deve ser acompanhada de parecer realizado pela equipe de Riscos & Compliance e aprovado pelo CGPSI.

Ainda neste diapasão, o tratamento de dados pessoais de criança, adolescente e/ou absolutamente incapaz nos termos do Código Cívil (quando a pessoa ainda que maior de 18 anos não possui capacidade de tomar decisões que afetem sua vida civil de maneira totalmente independente), somente pode ser realizado nas seguintes hipóteses:

- Visando o melhor interesse dos indivíduos, ou seja, com a finalidade de beneficiá-los, ainda que de forma indireta, respeitando sempre o principio da findalidade;
- De forma clara e compreensível, de modo que informações destinadas a este público deverão ser prestadas de maneira transparente, acessível, considerando as condições físicas, mentais e sensoriais do individuo.

O tratamento de dados para o grupo supramencionado, deverá necessariamente haver a coleta do consentimento específico e em destaque, dado por pelo menos um dos pais ou pelo responsável legal, mantendo públicas as informações sobre o tipo de dados coletas e a finalidade de utilização.

A UP Brasil trata dados do grupo supramencionado nas atividades de recrutamento e seleção para fins de contratação e para gestão de benefícios dos colaboradores UP Brasil. Estes dados são associados sempre ao colaborador.

6.8.6 Compartilhamento e Transfêrencia Internacional de Dados:

Na hipótese de compartilhamento e transferência de dados pessoais para países estrangueiros, a UP Brasil deverá adotar as salvaguardas a seguir:

- Avaliar e garantir a existência de regulação de proteção de dados compatível e não conflitante com a Lei Geral de Proteção de Dados no país estrangeiro;
- Estabelecer cláusulas contratuais para garantir a integridade, disponibilidade e confidenciabilidade dos dados pessoais;
- Informar ao titular de dados pessoais quais processos e etapas do ciclo de vida dos dados são tratados em outros países (e quais não são). Garantindo desta forma, o princípio da transparência.

O CGPSI deve avaliar em conjunto com o DPO toda transferência internacional de dados, sendo necessário em caso de identificação de Riscos por parte do DPO a elaboração do parecer de riscos a ser elaborado pelo time de Riscos & Compliance, devendo ser aprovado formalmente pelo CGPSI por fórum de maioria absoluta.

6.9 Condições minimas para parceiros de negócio e suprimentos:

Os parceiros de negócio, terceiros, fornecedores e quaisquer outras empresas que participem da cadeia de negócios e suprimentos da UP Brasil, cuja prestação dos serviços inclua o tratamento de dados pessoais confiados a UP brasil pelo titular, deverão aderir a esta Política, além de cumprir os deveres legais e contratuais respectivos, dentro os quais se incluirão, mas não se limitarão aos seguintes:

I. Assinar contrato ou termo de compromisso com Cláusula específica sobre a proteção de dados pessoais nos padrões de qualidade Up Brasil;
II. Apresentar evidências e garantias suficientes de que aplica adequado conjunto de medidas técnicas e administrativas de segurança para a proteção dos dados pessoais segundo a LGPD, os instrumentos contratuais e controles interno;
III. Manter os registros de tratamento de dados pessoais que realizar, com condições de rastreabilidade e de prova eletrônica a qualquer tempo;
IV. Seguir fielmente as diretrizes e instruções transmitidas pela UP Brasil;
V. Facultar acesso a dados pessoais somente para o pessoal autorizado que tenha estrita necessidade respectiva e que tenha assumido compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo estar sempre disponível para visualização de evidência para UP Brasil.
VI. Permitir a realização de auditorias, incluindo inspeções da UP Brasil ou de auditor independente por ela autorizado, e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas;
VII. Auxiliar em toda providência que estiver ao seu alcance, no atendimento pela UP Brasil de obrigações perante Titulares de dados, autoridade competentes ou quaisquer outros legítimos interessados;
VIII. Manter processo e recursos para tratamento de incidentes de privacidade e dados pessoais considerando melhores práticas, conhecimento e habilidades necessárias;
IX. Comunicar formalmente e de imediato a UP Brasil a ocorrência de qualquer risco, ameaça ou incidente de privacidade e dados pessoais que possa acarretar comprometimento ou dano potencial ou efetivo ao Titular de dados pessoais, evitando atrasos por conta de verificações ou inspecções;
X. Auxiliar UP Brasil, em toda providência que estiver ao seu alcance, no suporte para o tratamento de incidentes de privacidade e dados pessoais que envolvam as partes da LGPD: Controlador, ANPD, Titular de Dados, Operadores;
XI. Descartar de forma irrecuperável, ou devolver para a Up Brasil, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

6.10 Gestão de Riscos para Privacidade e Dados Pessoais:

Todos os processos de tratamento de dados pessoais devem possuir análise e gestão de riscos inerentes à privacidade de dados pessoais conforme a Política de Gestão de Riscos da Up Brasil.

É fundamental que todo projeto, melhoria, atualização ou outra atividade que envolva mudança ou criação de fluxo de trabalho que envolva dados pessoais, envolva o time de Riscos & Compliance para que possa ser aplicado os principios de Privacy by Design e Privacy by Default.

É responsabilidade da área de Riscos & Compliance em conjunto com o CPGSI avaliar os riscos das atividades de tratamento de dados pessoais conforme procedimento de Gestão de Inventário de Dados Pessoais (Data Mapping).

O Time de Riscos & Compliance deve manter a manutenção ciclica da avaliação de riscos das atividades de tratamento de dados pessoais nos termos da ISO 27005.

6.10.1 Relatório de Análise de Impacto - RIPDP:

Os relatórios de impacto à proteção de dados pessoais são documentos que contêm a descrição dos processos que envolvem o tratamento de dados pessoais que, por sua natureza, são passíveis de gerar riscos às liberdades civis e individuais dos Titulares de Dados Pessoais.

A UP Brasil deverá manter o processo e recursos para a apresentação imediata deste documento quando:

- O tratamento de dados envolver dados sensíveis ou de crianças, adolescentes ou indivíduos absolutamente incapazes nos termos do Código Civil;
- Quando o tratamento de dados envolver ou possa gerar alto riscos aos Titulares de Dados Pessoais;
- Quando o tratamento de dados pessoais for amparado pela base legal do interesse legítimo.
- Quando da ocorrência de incidentes envolvendo dados pessoais;
- Por solicitação da ANPD ou outros órgãos legais.

O Relatório deve conter uma linguagem fácil e acessível as demais áreas, juntamente com a classificação de Risco e os planos de ação sugerido para cada Risco, ficando sob a responsabilidade de cada diretoria aceitar ou assumir o Risco caso julgue necessário.

6.10.2 Incidentes de Privacidade e Dados Pessoais:

Os incidentes de privacidade e dados pessoais podem ser caracterizados como:

- **Violação de Dados Pessoais:** Um ou mais eventos que possam comprometer a disponibilidade, integridade e/ou a confidencialidade de dados pessoais comuns ou sensíveis;
- **Violação da Privacidade:** Um ou mais eventos que possam comprometer a intimidade, a vida privada, a honra e a imagem das pessoas.

A UP Brasil manterá canais internos e externos para a comunicação de

incidentes de privacidade e dados pessoais. Todo e qualquer incidente de privacidade e dados pessoais deverá ser tratado por equipe com conhecimento, habilidades específicas e lastreadas em melhores práticas. Exercícios práticos deverão ser conduzidos por esta equipe periodicamente, visando a preparação e evolução de estratégias de detecção, análise, contenção, erradicação e recuperação de incidentes.

A UP Brasil, por meio do Procedimento para Gestão de Incidentes de Privacidade de Dados Pessoais e Segurança da Informação, define as diretrizes e etapas necessárias ao processo de tratamento de incidentes para cumprir com os rigores da LGPD e minimizar os riscos e possíveis impactos para o titular de dados.

7. SANÇÕES

Eventuais falhas e descumprimentos das condutas e atividades previstas nas políticas, normas e procedimentos, sujeitarão seus autores a medidas disciplinares e/ou penalidades, conforme as circunstâncias.

8. VIGÊNCIA E REVISÃO

Esta política entra em vigor em 16 de Fevereiro de 2023, com revisão anual ou sempre que houver necessidade, de acordo com a área responsável.

Data	Versão	Tópico Alterado	Editado por	Aprovador
26/01/2022	2	Atualização da Política e Revisão do Novo Layout	Matheus Carvalho – Riscos & Compliance	CGPSI
26/12/2022	3	Atualização da Política	Matheus Carvalho – Riscos & Compliance	CGPSI