Título: POLÍTICA DE PRIVACIDADE - SIMPAR
Número e versão: POL0089 - V.2 **Fase**: Vigente
Elaborado por: ENCARREGADO DE DADOS **Data criação:** 18/06/2024

1. OBJETIVO

A **SIMPAR S.A.** (“Companhia” ou “Grupo SIMPAR") reconhece a importância da privacidade de nossos colaboradores, clientes, fornecedores, parceiros e demais pessoas com quem nos relacionamos e, por isso, está comprometido com o tema.

Esta Política tem a finalidade de estabelecer padrões de conformidade à Lei Federal nº 13.709/2018 (“Lei Geral de Proteção de Dados Pessoais” ou “LGPD”) em relação a todos os dados pessoais tratados pela Companhia, bem como outras leis que façam referência ao tema proteção de dados, desde que aplicáveis aos negócios das empresas do grupo.

Assim, esta política descreve as regras aplicáveis ao tratamento de dados pessoais, e estabelece os pilares para a construção do Programa de Privacidade e Proteção de Dados Pessoais (“Programa”).

2. CAMPO DE APLICAÇÃO

Esta política se aplica a SIMPAR S.A. e todas as empresas por ela controladas (“Companhia” ou “Grupo SIMPAR”). Se aplica também a terceiros que mantenham algumas relações com a Companhia e seus negócios.

3. DOCUMENTOS DE REFERÊNCIA

- Código de Conduta da SIMPAR;
- Políticas Anticorrupção;
- Política de Gerenciamento de Riscos;
- Política de Manuseio de Dados Pessoais;
- Política de Segurança da Informação;
- Procedimento de Privacy by Design;
- Procedimento de Resposta a Incidentes com Dados Pessoais;
- Política para Uso e Gestão do Consentimento; e
- Política de Compartilhamento de Dados com Terceiros.

4. DEFINIÇÕES

Para os fins desta Política, as seguintes definições se aplicam:

Anonimização: processo pelo qual um dado relativo ao Titular não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Aviso de Privacidade: documento através do qual as principais informações relacionadas ao Tratamento dos Dados Pessoais dos Titulares são fornecidas, podendo ser Externo (direcionado para os clientes e público em geral) ou Interno (direcionado para colaboradores).

Autoridade Nacional de Proteção de Dados ("ANPD"): é o órgão da administração pública responsável pela regulamentação, fiscalização e aplicação de penalidades administrativas, relacionadas à Proteção de Dados Pessoais.

Alta Administração: vide responsabilidades descritas no item "Gestão e Governança", representados na pessoa do Diretor Presidente e/ou Diretor Administrativo Financeiro de cada empresa.

Base Legal: termo que se refere às hipóteses legais que autorizam o Tratamento de Dados Pessoais e Dados Pessoais Sensíveis dispostos nos artigos 7º e 11 da LGPD, respectivamente.

Dado Pessoal: qualquer informação relativa a uma pessoa singular identificada ou identificável. É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica, ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.

Dado Pessoal Sensível: o Dado Pessoal Sensível é a informação que pode representar um risco elevado à segurança e/ou às liberdades do Titular ou, ainda, que podem gerar discriminações ilícitas quando tratado. Incluem-se como dados pessoais sensíveis qualquer dado pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Dados de autenticação em sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, tokens e senhas.

Dados de adolescentes: envolve dados de titulares com idade igual ou superior a 12 anos e menor que 18 anos.

Dados de crianças: envolve dados de titulares de até 12 (doze) anos de idade.

Dados de idosos: envolve dados de titulares com idade igual ou superior a 60 anos.

Dados protegidos por sigilo legal, judicial ou profissional: dados pessoais cujo sigilo decorram de norma jurídica ou decisão judicial, ou ainda, cujo sigilo decorra do exercício de função, ministério, ofício ou profissão, e cuja revelação possa produzir danos a terceiros.

Encarregado pelo Tratamento de Dados Pessoais ("Encarregado"): pessoa ou organização formalmente indicada pela Companhia como responsável pela gestão do Programa de Privacidade, para atuar como canal de comunicação entre o Controlador, os Titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), dentre a execução de outras atividades próprias à função.

Não Conformidade com o Programa de Privacidade: qualquer falha na observância dos pontos descritos nesta Política, que possam gerar riscos de danos aos Titulares e/ou riscos à Companhia.

LGPD: Lei Geral de Proteção de Dados – Lei Federal nº 13.709/2018.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais, como a forma e duração do Tratamento. A Companhia será Controladora quando tomar as decisões sobre o Tratamento dos Dados Pessoais, como ocorre, por exemplo, em relação aos Dados Pessoais de todos os colaboradores integrantes do Grupo SIMPAR.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador.

Privacidade desde a concepção (Privacy by Design): abordagem utilizada no desenvolvimento de um sistema ou projeto para incluir questões de privacidade e proteção de Dados Pessoais desde sua concepção.

Programa de Privacidade ou Programa: conjunto de regras, orientações internas e órgãos/estruturas de governança que possuem por objetivo estabelecer os parâmetros internos para manuseio de dados pessoais, mitigação de riscos e garantia de conformidade da Companhia com legislações de proteção de dados e melhores práticas a respeito do tema.

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, em ambiente controlado e seguro.

Projeto: desenvolvimento ou realização de alterações significativas de produtos ou serviços fornecidos pela Companhia.

Questionário de Avaliação de Criticidade (QAC): documento que busca identificar informações relacionadas às operações de Tratamento de Dados Pessoais no Projeto, de modo a permitir a avaliação e classificação do nível de criticidade.

Questionário de Teste de Balanceamento: documento que busca identificar informações relacionadas à utilização do legítimo interesse ou prevenção à fraude como Base Legal de Tratamento de Dados Pessoais no Projeto.

Relatório de Impacto à Proteção de Dados Pessoais ("RIPD"): documentação que contém a descrição dos processos de Tratamento de Dados Pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Securiti: ferramenta oficial de gestão e Tratamento de Dados Pessoais homologada pela Companhia, para atender oficialmente a todos os requisitos de conformidade com LGPD e demais legislações aplicáveis sobre o tema.

Titular: pessoa física a quem os Dados Pessoais se referem.

Terceiro: são todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais e fornecedores da Companhia.

T**ratamento: qualquer operação efetuada com Dados Pessoais, por meios automatizados ou não automatizados, tais como:** 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.

Tratamento de dados pessoais em larga escala: envolve o tratamento de dados de, pelo menos, 2 milhões de titulares. Caso o tratamento de dados seja inferior a este quantitativo, deverá ser apurada a existência ou não de "tratamento em larga escala" com base também no volume de dados envolvido, bem como na duração, frequência e extensão geográfica do tratamento, considerando a metodologia adotada pela ANPD.

Tratamento de dados que afeta significativamente interesses e direitos dos titulares: o tratamento de dados que pode, em potencial, impedir o titular de exercer direitos garantidos pela legislação brasileira, ou acessar produtos/serviços essenciais, ou, ainda, ocasionar danos materiais ou morais aos titulares, tais como (sem se limitar) discriminação, violação à integridade física, direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Tratamento automatizado de dados: envolve a utilização de algoritmos ou outras tecnologias para realizar o tratamento automatizado de dados, podendo realizar operações ou tomar decisões relacionadas a dados pessoais (p.ex. classificação, avaliação, aprovação ou rejeição de dados pessoais, com base em critérios pré-definidos).

Tratamento de dados que envolve uso de tecnologias emergentes e/ou inovadoras: envolve a utilização, por exemplo, de tecnologias tais como inteligência artificial, aprendizado de máquina e IA generativa, sistemas de reconhecimento facial, veículos autônomos e/ou de quaisquer inovações que possam ter aplicações práticas com alto grau de interesse empresarial, com potencial de impacto na sociedade, mas que ainda não foram plenamente exploradas e seus riscos não são totalmente conhecidos.

Tratamento de dados que envolve vigilância ou controle de zonas acessíveis ao público e monitoramento sistemático, como por exemplo o rastreamento da localização de indivíduos: envolve o tratamento de dados pessoais com a finalidade de monitorar ou controlar a presença de pessoas em áreas públicas ou privadas, com possível utilização de ferramentas, tais como câmeras de segurança, drones, dispositivos de rastreamento via GPS, entre outros.

Tratamento de dados que vise a formação de perfil comportamental da pessoa natural: tratamento que envolve a utilização de dados comportamentais para geração de profiling, que poderá ou não embasar decisões automatizadas.

5. PRINCÍPIOS NORTEADORES DA PROTEÇÃO DE DADOS PESSOAIS

O Grupo SIMPAR cuidará para que todas as suas atividades de Tratamento de Dados Pessoais estejam em conformidade com os princípios da LGPD, abaixo relacionados:

Princípios	Direcionamentos
Boa-Fé	O Tratamento de Dados Pessoais deverá ser sempre pautado em **boas intenções**, assim como na ética e respeito aos Titulares.
Finalidade e Adequação	O Tratamento de Dados Pessoais deve se limitar aos **propósitos legítimos**, **específicos**, **explícitos** e **informados** ao Titular, e somente deve ocorrer de formas compatíveis com estas finalidades.
Necessidade	A coleta e utilização de Dados Pessoais deverá ser limitada ao **mínimo necessário** para o cumprimento das finalidades definidas. Ainda, tais informações devem ser armazenadas pelo menor tempo possível / necessário.
Livre Acesso e Qualidade	Aos Titulares, deverá ser garantida a **consulta facilitada** e **gratuita** quanto à forma e duração do Tratamento, e integralidade de seus Dados Pessoais, estando assegurada a exatidão, clareza, relevância e atualização destes.
Segurança e Prevenção	A segurança e confidencialidade dos Dados Pessoais devem ser garantidas por meio de Medidas Técnicas e Organizacionais, a fim de **prevenir** a ocorrência de Incidentes de Segurança envolvendo Dados Pessoais.
Transparência	Deverão ser fornecidas, aos Titulares **informações claras**, **precisas** e **facilmente acessíveis** sobre a realização do Tratamento dos seus dados e os respectivos agentes nele envolvidos, observados os segredos comerciais e industriais da Companhia.
Não Discriminação	O Tratamento de Dados Pessoais **jamais** será realizado para fins discriminatórios, ilícitos ou abusivos.
Responsabilização e Prestação de Contas	Deverão ser armazenados **registros** de todas as atividades de Tratamento de Dados Pessoais e as respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e proteção de Dados Pessoais, comprovando, inclusive, a eficácia e eficiência destas medidas.

6. DIRETRIZES GERAIS E ESTRUTURA DE GOVERNANÇA

6.1 ESTRUTURA NORMATIVA DO PROGRAMA

A estrutura normativa do Programa de Privacidade da Companhia é composta pelo conjunto de documentos elaborados pelas áreas técnicas, aprovados pelos órgãos internos de governança e registrados no sistema de gestão de documentos da Companhia.

6.2 GESTÃO E GOVERNANÇA

A gestão e governança do Programa de Privacidade do Grupo SIMPAR deverá ser conduzida pelos responsáveis abaixo:

6.2.1 Alta Administração

Cabe à Alta Administração a responsabilidade de atuar diretamente no gerenciamento de riscos (baixo, médio e alto) relacionados ao Tratamento de Dados Pessoais, entendendo e se responsabilizando pelas seguintes etapas: identificação, avaliação, tratamento e monitoramento, buscando garantir a melhor tomada de decisão para a Companhia.

A Alta Administração, quando necessário e observando regimentos e estatutos vigentes, reporta-se diretamente aos órgãos de governança, tais como o Conselho de Administração e Comitê de Auditoria, entre outros.

Cabe, ainda, à Alta Administração garantir uma estrutura adequada para a gestão do Programa de Privacidade.

6.2.2 Encarregado Pelo Tratamento De Dados Pessoais

O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer ou DPO, deve possuir conhecimentos jurídicos e técnicos relacionados à proteção de Dados Pessoais e experiência na área. O profissional ou organização que atuar como Encarregado deve ter grau razoável de independência em relação ao restante da administração e suas funções não devem incluir atividades que possam conflitar com a responsabilidade da Companhia para com os Titulares.

A atuação do Encarregado deve garantir a conformidade da Companhia em relação às leis e demais políticas de privacidade e proteção de Dados Pessoais aplicáveis. Suas principais atribuições incluem:

a) Gerir o Programa de Privacidade;
b) Desenvolver, manter e propor a revisão das políticas de privacidade do Grupo SIMPAR;
c) Atuar como ponto de contato do Grupo SIMPAR com a ANPD e com os Titulares;
d) Receber e fazer a gestão das solicitações de Titulares; e
e) Revisar Relatórios de Impacto à Proteção de Dados Pessoais (“RIPD”), com apuração e revisão dos riscos das atividades.

Cabe ao Encarregado, apoiado pela Área de Controles Internos, Riscos e Conformidade - CRC e por algumas áreas de negócio e/ou áreas técnicas, o auxílio consultivo à Alta Administração em suas tomadas de decisão sobre as atividades de Tratamento de Dados Pessoais conduzidas pela Companhia.

Por fim, o Encarregado deve auxiliar no esclarecimento de dúvidas e orientar demais membros da Companhia durante a execução de suas atividades, quando envolverem operações de Tratamento de Dados Pessoais.

6.2.3 Área De Controles Internos, Riscos E Conformidade - Crc

A Área de Controles Internos, Riscos e Conformidade da Companhia será responsável, em conjunto com o Encarregado e, quando necessário, com o apoio de algumas áreas de negócio e técnicas, pela análise dos riscos envolvidos nas atividades relacionadas a tratamento de dados pessoais.

Além disso, será responsável por outras atividades, quais sejam:

a) análise de projetos que envolvam Dados Pessoais;
b) aprovação de avisos de privacidade das unidades de negócio, antes de sua efetiva publicação, com a elaboração do Encarregado;
c) execução de atividades gerais relacionadas ao Programa de Privacidade;
d) revisão de políticas/procedimentos do Programa;
e) aplicação de medidas disciplinares por descumprimentos das políticas/ procedimentos relacionados ao Programa;
f) garantia de que as investigações internas que tenham como objeto a avaliação de eventual descumprimento de leis relacionadas a privacidade/tratamento de dados pessoais sejam realizadas de forma imparcial e independente;
g) garantir a documentação e suporte das atividades relacionadas ao Programa; e
h) reportar ao Comitê de Auditoria os indicadores do Programa e riscos relacionados ao tema.

6.2.4 Embaixadores De Privacidade

Os Embaixadores de Privacidade são pontos focais que podem ser alocados em áreas da Companhia para atuar como contato direto do Encarregado e da área de CRC. Os Embaixadores têm as funções de facilitar comunicações, treinamentos e levantamento de informações relativos à sua área.

Estes agentes serão nomeados pela área de CRC e poderão ou não formar um Comitê de Embaixadores, o qual será responsável pela supervisão do cumprimento das diretrizes do Programa, bem como fazer recomendações sobre o Tratamento de Dados Pessoais, mediante alinhamento prévio com a área de CRC e, quando necessário, com o Encarregado.

6.2.5 Comitê De Auditoria

O Comitê de Auditoria deve funcionar nos exatos termos do seu Regimento Interno e tem como competência supervisionar a aderência às normas legais, estatutárias e regulatórias, a adequação dos processos relativos à gestão de riscos e a efetividade do Programa de Privacidade.

Caberá ao Comitê de Auditoria, quando necessário, reportar ao Conselho de Administração nos termos do seu Regimento e Estatuto.

Para o desempenho de suas funções, o Comitê de Auditoria disporá de autonomia operacional e dotação orçamentária, dentro de limites aprovados pelo Conselho de Administração, nos termos do Estatuto Social da Companhia.

6.3 DIRETRIZES BÁSICAS DO PROGRAMA DE PRIVACIDADE

a) Toda operação de Tratamento de Dados Pessoais realizada pelo Grupo SIMPAR deverá seguir os princípios dispostos na LGPD, em seu artigo 6º, descritos no item 5 deste instrumento;

b) Toda operação de Tratamento de Dados Pessoais deverá ser fundamentada em uma das hipóteses legais previstas na LGPD (art. 7º para Dados Pessoais Simples ou art. 11 para Dados Pessoais Sensíveis);

c) A Companhia deverá possuir o registro das atividades de Tratamento de dados pessoais, contendo, preferencialmente, as seguintes informações que permitam a identificação: i) do fluxo dos dados pessoais em cada etapa de seu ciclo de vida; ii) do perfil do titular; iii) dos tipos de dados tratados; iv) da finalidade de tratamento; v) dos responsáveis internos pela atividade; vi) volumetria dos dados pessoais envolvidos; vii) da hipótese legal de tratamento aplicável; e viii) outras informações necessárias para garantia de conformidade do Grupo SIMPAR à legislação aplicável e/ou para viabilizar a gestão e direcionar as ações estratégicas do Programa de Privacidade;

d) As operações de compartilhamento de Dados Pessoais com terceiros deverão estar documentadas e adequadamente resguardadas mediante aplicação de cláusulas de proteção de dados pessoais. Estas operações deverão seguir o disposto na Política de Compartilhamento de Dados Pessoais com Terceiros do Grupo SIMPAR;

e) Todos os novos produtos, projetos e iniciativas que envolverem tratamento de Dados Pessoais deverão ser analisados nos termos do Procedimento de privacidade desde a concepção (Privacy by Design);

f) As operações de tratamento de Dados Pessoais que necessitarem da coleta de consentimento deverão ser pautadas pelas instruções descritas na Política para Uso e Gestão do Consentimento da Companhia;

g) Os Dados Pessoais tratados devem possuir um prazo de retenção definido, devidamente justificado, podendo serem excluídos após finalizado o período pré-determinado. Os períodos de retenção devem levar em consideração as necessidades internas da Companhia, devendo estar previstos em documento apartado que compile todos os prazos mínimos de guarda; e

h) As informações sobre o tratamento de dados pessoais deverão ser divulgadas por meio de Avisos de Privacidade e/ou outros meios que forneçam a transparência necessária ao Titular.

6.4 DIREITOS DOS TITULARES

A Companhia está comprometida a observância da LGPD, especialmente em relação aos direitos dos titulares:

Direitos do Titular	Descrição
Direito à Confirmação da Existência do Tratamento	Garantia aos Titulares de obter, a qualquer momento e mediante requisição, confirmação sobre a existência ou não do Tratamento de seus Dados Pessoais.
Direito de Acesso aos Dados Pessoais	Garantia aos Titulares de consulta facilitada e gratuita sobre a forma e a duração do Tratamento, bem como sobre a integralidade de seus Dados Pessoais.
Direito à Correção de Dados Pessoais incompletos, inexatos ou desatualizados	Garantia, aos Titulares de exatidão, clareza, relevância e atualização dos Dados Pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu Tratamento.
Direito à Anonimização, Bloqueio ou Eliminação dos Dados Pessoais	Garantia, aos Titulares, de anonimização, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD.
Direito à Portabilidade	Garantia aos Titulares de portabilidade de seus Dados Pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da ANPD, observados os segredos comercial e industrial.
Direito à Informação	Garantia aos Titulares, de informações, inclusive sobre as entidades públicas e privadas com as quais foi realizada o compartilhamento de seus Dados Pessoais.
Direito a Não Consentir e Direito à Revogação do Consentimento	Garantia aos Titulares, de serem informados sobre a possibilidade de não fornecer o seu consentimento e sobre as consequências da negativa. Igualmente, abarca a possibilidade de revogar o consentimento, quando este for a base legal aplicável.
Direito à Revisão de Decisão Automatizada	Garantia, aos Titulares, de revisão de decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

O atendimento dos direitos dos Titulares será realizado por meio de canal próprio para este fim, exclusivo e adequado para cumprimento da legislação.

a) No contexto do atendimento às requisições dos titulares, a Companhia deverá levar em consideração as seguintes diretrizes:

b) Manter um canal adequado e disponível para o recebimento das solicitações a qualquer momento do dia, possuindo uma confirmação de recebimento da solicitação, ainda que automatizada;

c) Garantir a geração de evidências em todas as etapas do processo, desde o recebimento das solicitações até o momento do envio da resposta;

d) Garantir a cooperação entre as áreas de negócio envolvidas, para viabilizar a resposta e a adoção de providências;

e) Atender à requisição do titular em conformidade com os prazos legais aplicáveis; e

f) Facilitar o procedimento de resposta, mantendo os dados armazenados em formatos que facilitem sua consulta.

6.5 RELATÓRIO DE IMPACTO A PROTEÇÃO DE DADOS PESSOAIS - RIPD

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é uma ferramenta importante para conformidade com a LGPD, pois auxilia a Companhia a avaliar adequadamente os riscos que uma determinada atividade representa aos titulares, além de definir e demonstrar a adoção de medidas adequadas para mitigação dos riscos identificados.

Tendo-se em conta a natureza, o contexto e a finalidade da operação de Tratamento de Dados Pessoais, o RIPD será realizado sempre que uma determinada atividade representar um elevado risco à garantia de um dos princípios gerais elencados na LGPD e aos direitos e liberdades dos Titulares.

Sem prejuízo de outras situações nas quais o Encarregado julgar necessárias, a elaboração do RIPD deverá ocorrer quando uma atividade de tratamento for enquadrada em criticidade “alta”, com base na matriz de criticidade constante do Anexo I.

Tais documentos não deverão ser publicados ou disponibilizados a terceiros sem a expressa autorização do Encarregado e da Diretoria da área de CRC. Contudo, devem ser arquivados em ferramenta/rede homologada pela Companhia, uma vez que poderão ser objeto de requisição da ANPD e/ou de auditoria interna e externa.

7. LINHA TRANSPARENTE

Qualquer dúvida e/ou solicitação de informações sobre a presente política e outras políticas e procedimentos do Programa de Privacidade da Companhia poderão ser esclarecidas por meio da Linha Transparente, pelos seguintes meios de comunicação: 0800 726 7250 ou conformidade@simpar.com.br (ou utilize o domínio da empresa sobre a qual pretende falar, exemplo: @jsl, @movida, @grupovamos, etc).

8. NÃO CONFORMIDADE COM O PROGRAMA DE PRIVACIDADE E O CANAL DE DENÚNCIA

A Companhia se compromete a envidar todos seus esforços para adotar medidas técnicas e administrativas aptas a proteger e prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais.

A Companhia dispõe de um Canal de Denúncias que deverá ser utilizado para comunicações de não conformidades em relação às leis aplicáveis, bem como às políticas/procedimentos relacionadas ao Programa de Privacidade da Companhia.

Esse canal segue as melhores práticas de governança do mercado, funciona 24 horas por dia, 7 dias por semana, garantindo a possibilidade de anonimato ao denunciante de boa-fé. O Canal de Denúncias é gerenciado por empresa terceira, contratada para esta finalidade específica e pode ser acionado nos seguintes contatos: 0800 726 7111 ou contatoseguro.com.br/SIMPAR (ou utilize o domínio da empresa sobre a qual pretende falar, exemplo: @jsl, @movida, @grupovamos, etc.)

O descumprimento de qualquer disposição desta Política, de outras regras do Programa de Privacidade e/ou de qualquer disposição legal aplicável acarretará a aplicação das sanções cabíveis, sem prejuízo da sujeição a outras medidas legais pertinentes.

9. CONSIDERAÇÕES FINAIS

Esta Política foi aprovada pelo Conselho de Administração da SIMPAR e entrará em vigor na data de sua divulgação, revogando e substituindo qualquer diretriz similar e anterior sobre o mesmo assunto.

ANEXO I – MATRIZ DE CRITICIDADE

Nível de criticidade	Critérios
Baixa	- Tratamento de dados pessoais não enquadrado nas categorias “média” ou “alta”.
Média	- Tratamento de dados pessoais enquadrado em qualquer um dos critérios (geral ou específico) indicados para nível de criticidade “alta”; - Tratamento de dados pessoais financeiros; - Tratamento de dados de autenticação em sistemas; - Tratamento de dados protegidos por sigilo legal, judicial ou profissional; e/ou - Tratamento cujos dados são provenientes de fontes públicas ou privadas de terceiros.
Alta	A criticidade será considerada alta quando presente pelo menos 1 critério geral, somado a pelo menos 1 específico: **Critérios Gerais** - Tratamento de dados pessoais em larga escala; ou - Tratamento de dados que afeta significativamente interesses e direitos dos titulares. + **Critérios Específicos** - Tratamento de dados que envolve vigilância ou controle de zonas acessíveis ao público e monitoramento sistemático, como por exemplo o rastreamento da localização de indivíduos; - Tratamento de dados que vise a formação de perfil comportamental da pessoa natural; - Tratamento automatizado de dados; - Tratamento de dados que envolve o uso de tecnologias emergentes ou inovadoras; e/ou - Tratamento de dados sensíveis ou que envolvem titulares crianças, adolescentes e/ou idosos.

1. PURPOSE

SIMPAR S.A. (“Company” or “SIMPAR Group”) recognizes the importance of the privacy of our employees, clients, suppliers, partners and other people with whom we interact and is therefore committed to this issue.

The purpose of this Policy is to establish standards in compliance with Federal Law No. 13709/2018 (“General Personal Data Protection Law” or “LGPD”) in relation to all personal data processed by the Company, as well as other laws that refer to the subject of data protection, provided that they are applicable to the business of the group's companies.

Therefore, this policy describes the rules applicable to the processing of personal data, and establishes the pillars for the construction of the Privacy and Personal Data Protection Program (“Program”).

2. FIELD OF APPLICATION

This policy applies to SIMPAR S.A. and all the companies it controls (“Company” or “SIMPAR Group”). It also applies to third parties who have a relationship with the Company and its businesses.

3. REFERENCE DOCUMENTS

- SIMPAR Code of Conduct;
- Anti-Corruption Policies;
- Risk Management Policy;
- Personal Data Handling Policy;
- Information Security Policy;
- Privacy by Design Procedure;
- Personal Data Incident Response Procedure;
- Policy for the Use and Management of Consent; and
- Policy for Sharing Data with Third Parties.

4. DEFINITIONS

For the purposes of this Policy, the following definitions apply:

Anonymization: process by which data relating to the Data Subject cannot be identified, taking into account the use of reasonable technical means available at the time of its processing.

Privacy Notice: document through which the main information relating to the Processing of Data Subjects' Personal Data is provided, which may be External (aimed at clients and the general public) or Internal (aimed at employees).

National Data Protection Authority (“ANPD”): is the public administration agency responsible for regulating, supervising and applying administrative penalties related to Personal Data Protection.

Senior Management: see responsibilities described under "Management and Governance", represented in the person of the Chief Executive Officer and/or Chief Financial Officer of each company.

Legal Basis: term that refers to the legal hypotheses that authorize the Processing of Personal Data and Sensitive Personal Data set out in articles 7 and 11 of the LGPD, respectively.

Personal data: any information relating to an identified or identifiable individual. An identifiable individual is one who can be directly or indirectly identified, in particular by reference to an identifier such as a name, an identification number, location data, electronic identifiers, or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Personal Data: Sensitive Personal Data is information that may represent a high risk to the security and/or freedoms of the Data Subject or that may give rise to unlawful discrimination when processed. Sensitive personal data includes any personal data relating to racial or ethnic origin, religious conviction, political opinion, membership of a trade union or religious, philosophical or political organization, as well as data relating to health or sex life, genetic or biometric data.

System authentication data: any personal data used as a credential to determine access to a system or to confirm the identification of a user, such as login accounts, tokens and passwords.

Teenagers' data: involves data from data subjects aged 12 or over and under 18.

Children's data: involves data from data subjects up to twelve (12) years of age.

Elderly data: involves data from data subjects aged 60 or over.

Data protected by legal, judicial or professional secrecy: personal data whose secrecy derives from a legal rule or court decision, or whose secrecy derives from the exercise of a role, ministry, office or profession, and whose disclosure may cause damage to third parties.

Person in Charge of Personal Data Processing ("Data Controller"): a person or organization formally appointed by the Company to be responsible for the management of the Privacy Program, to act as a communication channel between the Controller, the Data Subjects and the National Data Protection Authority (ANPD), among the performance of other activities specific to the role.

Non-Compliance with the Privacy Program: any failure to comply with the points described in this Policy, which may give rise to risks of damage to Data Subjects and/or risks to the Company.

LGPD: General Data Protection Law - Federal Law No. 13709/2018.

Controller: individual or legal entity governed by public or private law, who is responsible for decisions regarding the Processing of Personal Data, such as the form and duration of said Processing. The Company will be the Controller when it takes decisions on the Processing of Personal Personal Data, as is the case, for example, with the Personal Data of all SIMPAR Group employees.

Operator: individual or legal entity governed by public or private law, who carries out the Processing of Personal Data on behalf of the Controller.

Privacy by Design: approach used in the development of a system or project to include privacy and Personal Data protection issues from the outset.

Privacy Program or Program: set of rules, internal guidelines and governance bodies/structures aimed at establishing internal parameters for handling personal data, mitigating risks and ensuring the Company's compliance with data protection laws and best practices on the matter.

Pseudonymization: is the Processing by which Personal Data loses the possibility of direct or indirect association with an individual, if not for the use of additional information, kept separately, in a controlled and secure environment.

Project: developing or making significant changes to products or services provided by the Company.

Criticality Assessment Questionnaire (QAC): document that seeks to identify information related to Personal Data Processing operations in the Project, in order to allow the assessment and classification of the level of criticality.

Balancing Test Questionnaire: document that seeks to identify information related to the use of legitimate interest or fraud prevention as the Legal Basis for Processing Personal Data in the Project.

Personal Data Protection Impact Report ("PDPIR"): document that contains a description of the Personal Data Processing processes that may give rise to risks to civil liberties and fundamental rights, as well as measures, safeguards and risk mitigation mechanisms.

Securiti: official Personal Data Management and Processing tool approved by the Company, to officially meet all the requirements of compliance with the LGPD and other applicable laws on the matter.

Data Subject: Individual to whom the Personal Data refers.

Third Party: all service providers, outsourced workers, business partners and suppliers of the Company.

Processing: any operation carried out with Personal Data, by automated or non-automated means, such as: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination or extraction.

Large-scale processing of personal data: involves processing the data of at least 2 million data subjects. If the data processing is less than this amount, the existence or not of "large-scale processing" must be determined based also on the volume of data involved, as well as the duration, frequency and geographical extent of the processing, taking into account the methodology adopted by the ANPD.

Data processing that significantly affects the interests and rights of data subjects: data processing that could potentially prevent the data subject from exercising rights guaranteed by Brazilian law, or accessing essential products/services, or even cause material or moral damage to data subjects, such as (but not limited to) discrimination, violation of physical integrity, right to image and reputation, financial fraud or identity theft.

Automated data processing: involves the use of algorithms or other technologies to carry out automated data processing, which may carry out operations or make decisions relating to personal data (e.g. classification, evaluation, approval or rejection of personal data, based on predefined criteria).

Data processing involving the use of emerging and/or innovative technologies: involves the use, for example, of technologies such as artificial intelligence, machine learning and generative AI, facial recognition systems, autonomous vehicles and/or any

innovations that may have practical applications with a high degree of business interest, with the potential to impact society, but which have not yet been fully explored and their risks are not fully known.

Data processing involving surveillance or control of areas accessible to the public and systematic monitoring, such as tracking the location of individuals: involves the processing of personal data for the purpose of monitoring or controlling the presence of people in public or private areas, with the possible use of tools such as security cameras, drones, GPS tracking devices, among others.

Processing of data aimed at forming a behavioral profile of individuals: processing that involves the use of behavioral data to generate profiling, which may or may not be the basis for automated decisions.

5. GUIDING PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA

The SIMPAR Group will ensure that all its Personal Data Processing activities comply with the principles of the of the LGPD listed below:

Principles	Guidelines
Good Faith	The Processing of Personal Data should always be based on **good intentions,** ethics and respect for Data Subjects.
Purpose and Adequacy	The Processing of Personal Data must be limited to **legitimate, specific, explicit** purposes that have been informed to the Data Subject, and must only take place in ways that are compatible with these purposes.
Necessity	The collection and use of Personal Data must be limited to the **minimum necessary** to fulfill the defined purposes. Furthermore, such information must be stored for as short a time as possible / necessary.
Free Access and Quality	Data Subjects must be guaranteed **free and easy** access to information on the form and duration of Processing and the completeness of their Personal Data, ensuring that it is accurate, clear, relevant and up-to-date.
Security and Prevention	The security and confidentiality of Personal Data must be guaranteed through Technical and Organizational Measures in order to **prevent** the occurrence of Security Incidents involving Personal Data.
Transparency	Data Subjects must be provided with clear, **precise and easily accessible information** about the processing of their data and

	the respective agents involved, in compliance with the Company's commercial and industrial secrets.
Non-discrimination	Personal data will **never** be processed for discriminatory, unlawful or abusive purposes.
Responsibility and Accountability	**Records** must be kept of all Personal Data Processing activities and the respective measures taken to adapt these activities to the rules on privacy and protection of Personal Data, including proof of the effectiveness and efficiency of these measures.

6. GENERAL GUIDELINES AND GOVERNANCE STRUCTURE

6.1. NORMATIVE STRUCTURE OF THE PROGRAM

The regulatory structure of the Company's Privacy Program is made up of a set of documents drawn up by the technical departments, approved by the internal governance bodies and registered in the Company's document management system.

6.2. MANAGEMENT AND GOVERNANCE

The SIMPAR Group's Privacy Program shall be managed and governed by those responsible below:

6.2.1. Senior Management

Senior Management is responsible for acting directly in the management of risks (low, medium and high) related to the Processing of Personal Data, understanding and taking responsibility for the following stages: identification, evaluation, treatment and monitoring, seeking to ensure the best decision-making for the Company.

When necessary, and in compliance with current regulations and bylaws, Senior Management reports directly to the governance bodies, such as the Board of Directors and Audit Committee, among others. Senior Management is also responsible for ensuring that there is an adequate structure in place to manage the Privacy Program.

6.2.2. Personal Data Controller

The party responsible for processing personal data, also known as the Data Protection Officer or DPO, must have legal and technical knowledge related to the protection of personal data and experience in the field. The professional or organization acting as Data Protection Officer must have a reasonable degree of independence from the rest of management and their duties shall not include activities that could conflict with the Company's responsibility towards Data Subjects.

The role of the Data Protection Officer must ensure the Company's compliance with applicable laws and other privacy and Personal Data protection policies. Their main duties include:

a) Manage the Privacy Program;
b) Developing, maintaining and proposing reviews of the SIMPAR Group's privacy policies;
c) Acting as the SIMPAR Group's point of contact with the ANPD and the Card Holders;
d) Receive and manage requests from Data Subjects; and
e) Reviewing Personal Data Protection Impact Reports ("RIPD"), ascertaining and reviewing the risks of the activities.

The data controller, supported by the Internal Controls, Risks and Compliance Department (CRC) and by some business and/or technical departments, is responsible for providing advisory support to senior management in their decision-making on the Personal Data Processing activities carried out by the Company.
Finally, the data controller must help clear any doubts and guide other members of the Company during the execution of their activities, when they involve Personal Data Processing operations.

6.2.3. Internal Controls, Risks and Compliance Area - CRC

The Company's Internal Controls, Risks and Compliance Department shall be responsible, together with the data controller and, when necessary, with the support of some business and technical departments, for analyzing the risks involved in activities related to the processing of personal data.
They will also be responsible for other activities, such as:

a) analyzing projects involving Personal Data;
b) approving the privacy notices of the business units, prior to their actual publication, with the preparation of the data controller;
c) carrying out general activities related to the Privacy Program;
d) reviewing the Program's policies/procedures;
e) applying disciplinary measures for non-compliance with policies/procedures related to the Program;
f) ensuring that internal investigations aimed at evaluating possible non-compliance with laws related to privacy/processing of personal data are carried out impartially and independently;
g) ensuring the recording and support of activities related to the Program; and
h) reporting to the Audit Committee on the Program's indicators and risks related to the topic.

6.2.4. Privacy Ambassadors

Privacy Ambassadors are focal points who can be assigned to departments of the Company to act as a direct contact for the Compliance Officer and the CRC department. Ambassadors are responsible for facilitating communications, training and gathering information relating to their departments.

These agents will be appointed by the CRC department and may or may not form an Ambassador Committee, which will be responsible for supervising compliance with the Program's guidelines, as well as making recommendations on the Processing of Personal Data, through prior alignment with the CRC area and, when necessary, with the Data Controller.

6.2.5. Audit Committee

The Audit Committee shall operate under the exact terms of its Internal Regulations and is responsible for supervising adherence to legal, statutory and regulatory standards, the adequacy of risk management processes and the effectiveness of the Privacy Program.

When necessary, the Audit Committee shall report to the Board of Directors under the terms of its Rules of Procedure and Bylaws.

In order to carry out its duties, the Audit Committee shall have operational autonomy and a budget, within the limits approved by the Board of Directors, under the terms of the Company's Bylaws.

6.3. BASIC GUIDELINES OF THE PRIVACY PROGRAM

a) All Personal Data Processing operations carried out by the SIMPAR Group must follow the principles set out in the LGPD, in its article 6, described in item 5 of this instrument;

b) Every Personal Data Processing operation must be based on one of the legal hypotheses provided for in the LGPD (article 7 for Simple Personal Data or article 11 for Sensitive Personal Data);

c) The Company shall keep a record of its personal data processing activities, preferably containing the following information that allows identification: (i) the flow of personal data at each stage of its life cycle; (ii) the profile of the data subject; (iii) the types of data processed; (iv) the purpose of processing; (v) those internally responsible for the activity; (vi) the volume of personal data involved; (vii) the applicable legal processing hypothesis; and (viii) other information necessary to ensure that the SIMPAR Group is in compliance with the applicable laws and/or to enable management and direct the strategic actions of the Privacy Program;

d) Operations involving the sharing of Personal Data with third parties must be recorded and adequately protected through the application of personal data protection clauses. These operations must follow the provisions of the SIMPAR Group's Policy for Sharing Personal Data with Third Parties;

e) All new products, projects and initiatives involving the processing of Personal Data must be analyzed under the terms of the Privacy by Design Procedure;

f) Personal Data processing operations that require consent must be guided by the instructions described in the Company's Policy for the Use and Management of Consent;

g) The Personal Data processed must have a set duly justified retention period, and may be deleted after the end of the predetermined period. The retention periods must take into account the Company's internal needs, and must be set out in a separate document that compiles all the minimum retention periods; and

h) Information on the processing of personal data must be disclosed by means of Privacy Notices and/or other means that provide the necessary transparency to the Data Subject.

6.4. RIGHTS OF DATA SUBJECTS

The Company is committed to complying with the LGPD, especially with regard to the rights of data subjects:

Data Subject's Rights	Description
Right to Confirmation of the Existence of Processing	Guarantees that Data Subjects are able to obtain, at any time and upon request, confirmation of the existence or not of the Processing of their Personal Data.
Right of Access to Personal Data	Guarantees that Data Subjects are able to verify the form and duration of the Processing, as well as on the completeness of their Personal Data, in a free and simple manner.
Right to Correct Incomplete, Inaccurate or Outdated Personal Data	Guarantees that the Personal Data of Data Subjects is accurate, clear, relevant and up-to-date, according to the need and for the fulfillment of the purpose of its Processing.
Right to Anonymization, Blocking or Deletion of Personal Data	Guarantees that Data Subjects have the right to anonymization, blocking or deletion of Personal Data that is unnecessary, excessive or processed in breach of the LGPD.
Right to Portability	Guarantees that Data Subjects may have their Personal Data transferred to another service or product provider, upon express request, in accordance with ANPD regulations, observing commercial and industrial secrets.
Right to Information	Guarantees that Data Subjects may have access to information, including on the public and private entities with which their Personal Data has been shared.
Right to Withhold Consent and Right to Revoke Consent	Guarantees that Data Subjects may be informed of the possibility of withholding consent and the consequences of withholding consent. It also covers the possibility of revoking

	consent when this is the applicable legal basis.
Right to Review an Automated Decision	Guarantees that Data Subjects have the right to review decisions made solely on the basis of automated processing of personal data affecting their interests, including decisions aimed at defining their personal, professional, consumer and credit profiles or aspects of their personality.

The rights of the Data Subjects will be addressed by an exclusive channel created for this purpose, which is exclusive and suitable for complying with the law.

a) In the context of responding to requests from Data Subjects, the Company shall take the following guidelines into consideration:
b) Maintain an appropriate channel available for receiving requests at any time of the day, with confirmation of receipt of the request, even if automated;
c) Ensure that evidence is generated at all stages of the process, from the moment the request is received to the moment the response is sent;
d) Ensure cooperation between the business departments involved, to enable a response and the adoption of measures;
e) Comply with the data subject's request in accordance with the applicable legal deadlines; and
f) Facilitate the response procedure, keeping the data stored in formats that make consultation easier.

6.5. PERSONAL DATA PROTECTION IMPACT REPORT - RIPD

The Personal Data Protection Impact Report (RIPD) is an important tool to help the Company comply with the LGPD, as it helps it properly assess the risks that a given activity poses to data subjects, in addition to defining and demonstrating the adoption of appropriate measures to mitigate the risks identified. Taking into account the nature, context and purpose of the Personal Data Processing operation, the RIPD will be carried out whenever a particular activity poses a high risk to the guarantee of one of the general principles listed in the LGPD and to the rights and freedoms of Data Subjects.

Without prejudice to other situations in which the Data Protection Officer deems it necessary, the RIPD must be drawn up when a processing activity is classified as “high” criticality, based on the criticality matrix in Exhibit I.

Such documents must not be published or made available to third parties without the express authorization of the data controller and the CRC department management. However, they must be stored in a tool/network approved by the Company, since they may be subject to requests from the ANPD and/or internal and external audits.

7. TRANSPARENCY HOTLINE

Any questions and/or requests for information on this policy and other policies and procedures of the Company's Privacy Program can be addressed through the Transparency Hotline, by the following means of communication: 0800 726 7250 or conformidade@simpar.com.br (or use the domain of the company you wish to speak about, for example: @jsl, @movida, @grupovamos, etc).

8. NON-COMPLIANCE WITH THE PRIVACY PROGRAM AND THE REPORTING CHANNEL

The Company undertakes to make every effort to adopt technical and administrative measures to protect and prevent the occurrence of damage as a result of the Processing of Personal Data. The Company has a Whistleblower Channel which shall be used to report non-compliance with applicable laws, as well as with the policies/procedures related to the Company's Privacy Program.

This channel follows the best governance practices in the market and operates 24 hours a day, 7 days a week, ensuring that whistleblowers coming forth in good faith remain anonymous. The Whistleblowing Channel is managed by a third-party company, hired for this specific purpose, and can be called at: 0800 726 7111 or contatoseguro.com.br/SIMPAR (or use the domain of the company you wish to speak to, for example: @jsl, @movida, @grupovamos, etc.).

Failure to comply with any provision of this Policy, other rules of the Privacy Program and/or any applicable legal provision shall result in the application of the appropriate sanctions, without prejudice to being subject to other relevant legal measures.

9. FINAL PROVISIONS

This Policy has been approved by SIMPAR's Board of Directors and will come into force on the date of its publication, revoking and replacing any similar and previous guidelines on the same matter.

EXHIBIT I - CRITICALITY MATRIX

Criticality level	Criteria
Low	- Processing of personal data that do not classify as “medium” or “high”.
Medium	- Processing of personal data classified under any of the criteria (general or specific) indicated for “high” criticality level; - Processing of personal financial data; - Processing of authentication data in systems; - Processing of data protected by legal, judicial or professional secrecy; and/or - Processing of data from public or private third-party sources.
High	Criticality will be considered high when at least 1 general criterion is present, plus at least 1 specific criterion: **General Criteria:** - Processing of personal data on a large scale; or - Processing of data that significantly affects the interests and rights of data subjects. + **Specific Criteria** - Data processing involving surveillance or control of publicly accessible areas and systematic monitoring, such as tracking the location of individuals; - Data processing aimed at forming a behavioral profile of an individual; - Automated data processing; - Data processing involving the use of emerging or innovative technologies; and/or - Processing of sensitive data or data involving children, teenagers and/or the elderly.