Política de Política de Privacidade e Proteção de Dados

1. OBJETIVO

O objetivo desta Política de Privacidade e Proteção de Dados (a "Política") é demonstrar o compromisso da Natura com a coleta, uso e cuidado responsáveis de dados pessoais de acordo com nossos valores éticos e as leis e regulamentos aplicáveis nas jurisdições em que opera. Devemos garantir que a privacidade e a proteção de dados sejam incorporadas como facilitadores fundamentais para o crescimento de nossos negócios e marcas.

2. ABRANGÊNCIA

A Política estabelece como rege a conduta de todos os colaboradores, incluindo os diretores de previdência da Natura ("Companhia", "nós" e "nossos") da LATAM, como parte de nossa missão de desenvolver relações de confiança por meio do uso de dados pessoais.

3. DEFINIÇÕES

Anonimização significa tratar informações de tal forma que impeça qualquer pessoa de identificar um indivíduo específico, inclusive por referência a fontes externas. Isso é feito removendo informações dos dados para que não possam mais ser usadas para identificar qualquer indivíduo.

Base legal significa os motivos com base nos quais os dados pessoais podem ser tratados legalmente. De acordo com as leis de privacidade, cada atividade de tratamento de dados deve ter uma base legal, tais como: obrigação legal, necessidade contratual, interesses legítimos, consentimento de um indivíduo.

Controlador de dados significa a pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, sozinho ou em conjunto com outros, determina as finalidades e os meios do tratamento de dados pessoais. Em nosso negócio, o controlador final de dados é a Natura & Co., nossa holding.

Dados pessoais são quaisquer informações relacionadas a um indivíduo vivo identificável (ou seja, um nome, um número de identificação, dados de localização, um identificador on-line ou a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa). Também pode incluir informações como cookies; endereços IP; IDs de dispositivo exclusivos; informação comportamental; dados biométricos; e videovigilância.

Dados pessoais sensíveis são quaisquer informações relacionadas com a origem racial ou étnica de um indivíduo, opiniões políticas, crenças religiosas ou outras, filiação sindical ou tratamento de dados genéticos ou dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa singular.

Operador de dados significa uma pessoa física ou jurídica, autoridade pública, agência ou outro órgão que trata dados pessoais em nome e sob as instruções do controlador de dados.

Tratamento significa a coleta, registro, organização, estruturação, adaptação ou alteração, uso, análise, recuperação, consulta, fornecimento ou bloqueio de acesso (incluindo acesso remoto) a, divulgação, disseminação, alinhamento, cópia, transferência, armazenamento, exclusão, hospedagem, combinação, destruição, descarte ou outro uso ou tratamento de dados pessoais.

Violação de dados pessoais significa uma violação de segurança que leva à destruição, perda, alteração, divulgação não autorizada ou acesso acidental ou ilegal a dados pessoais. Isso inclui violações que são o resultado de causas acidentais e deliberadas.

4. DESCRIÇÃO

O que é privacidade e proteção de dados?

Privacidade é a coleta, uso e cuidado responsável e transparente de dados pessoais ao longo de seu ciclo de vida. A privacidade dos indivíduos é o direito legal e fundamental:

• Ter controle e aviso sobre como seus dados pessoais são coletados, tratados e armazenados;
• Entender se ou como seus dados são usados e compartilhados com terceiros; e para ter seus dados alterados, acessados ou excluídos.

A proteção de dados atende aos requisitos legais e organizacionais para que as empresas protejam os dados sob seus cuidados e impeçam que sejam usados indevidamente, explorados ou manipulados indevidamente. Nossos colaboradores devem ser:

- **Consciente de** apenas coletar e tratar os dados pessoais necessários para nossos fins comerciais.
- **Transparente** sobre quais dados pessoais usamos e para qual finalidade.
- **Cuidado** para manter os dados pessoais seguros e confidenciais.
- **Precisão** ao ser tomar todas as medidas razoáveis para manter os dados pessoais atualizados.

Por que a privacidade e a proteção de dados são importantes para nós?

Os dados pessoais são um facilitador crítico para a Companhia e para os indivíduos cujos dados coletamos e usamos. Portanto, devemos tratar os dados pessoais com cuidado e respeitar o direito à privacidade dos indivíduos. Além disso, temos uma tripla missão como organização que visa desenvolver relações de confiança de acordo com a legislação aplicável:

Capacitar os indivíduos e assegurar a sua compreensão dos dados:
- Proporcionar transparência e clareza através de uma comunicação simples - Dar aos nossos stakeholders escolha, poder e controle sobre seus dados, de acordo com a legislação aplicável.

Promover o impacto positivo e as relações de confiança:
- Não fazer mal a ninguém em nosso ecossistema, operando em uma base "sem surpresas" - Avanço do conceito de "uso de dados para o bem social"

Governar e proteger dados e informações dentro do nosso ecossistema: - Governar os dados do grupo da maneira que gostaríamos que nossos próprios dados fossem governados,
- Manter dados e informações seguros e renovar proativamente o consentimento, de acordo com a lei aplicável,
- Cultivar uma cultura de responsabilidade coletiva.

Nossa Missão e Princípios de Privacidade

Capacitar indivíduos e garantir sua compreensão dos dados

Legalidade, equidade e transparência
A coleta e o uso de dados pessoais devem ser legais. Os indivíduos precisam saber quais dados são coletados deles e como seus dados serão usados. Devemos ter uma base legal válida para coletar e usar dados pessoais e ser transparente sobre seu uso. Como resultado, devemos cumprir o seguinte:

Condições de Tratamento
Para coletar e usar dados pessoais, devemos identificar uma base legal válida (por exemplo, obrigação legal, necessidade contratual, interesses legítimos ou consentimento de um indivíduo) e cumprir com seus requisitos. Por exemplo, quando os dados de base legal são o consentimento (por exemplo, para enviar comunicações de marketing, para instalar cookies em um site), ele só é válido se for fornecido de forma genuína e livre. Só devemos usar dados pessoais sensíveis quando estritamente necessário e, geralmente, após a obtenção de consentimento individual explícito.

A Companhia verificará regularmente o Registro de Atividades de Tratamento e atualizará, se necessário, seus avisos de privacidade para garantir o cumprimento dessa obrigação. Consulte o **Padrão de Registros de Tratamento para obter mais orientações.**

Avisos de Privacidade

Os indivíduos precisam ser informados por nós, no momento da coleta de seus dados pessoais, como e por que seus dados serão tratados, e seus direitos em relação a esses dados. Por exemplo, se oferecermos aos indivíduos a oportunidade de optar por "opt-in" pelo marketing ou acessar e corrigir dados, essas oportunidades devem ser claras e fáceis de usar.

Direitos Individuais de Proteção de Dados
Os direitos de proteção de dados para os indivíduos são direitos relativos aos seus dados. Tais leis existem em quase todos os países em que operamos e ditam prazos rigorosos para a resposta. Os indivíduos têm frequentemente o direito de receber uma cópia dos seus dados (incluindo registos electrónicos e em papel). Muitas vezes, os indivíduos também têm o direito de entender como as decisões automatizadas são tomadas sobre eles. Um indivíduo também pode ter o direito de solicitar a exclusão de seus dados e solicitar a portabilidade de seus dados (ou seja, receber seus dados em um formato estruturado, comumente usado e legível por máquina). Consulte o

Procedimento de Direitos dos Titulares dos Dados para obter mais orientações.

Esses pedidos devem ser tratados com cuidado, coerência e rapidez. Devemos sempre responder às consultas e reclamações dentro de um prazo razoável, de acordo com os procedimentos da Companhia.

Promover impacto positivo e relações de confiança:

Limitação, minimização e precisão de propósito
Os dados pessoais só podem ser coletados para fins específicos e não podem ser utilizados de forma inconsistente com essas finalidades. Os dados pessoais coletados devem ser limitados à quantidade necessária para a finalidade da coleta, e qualquer decisão de coleta de dados pessoais sensíveis deve ser tomada com cuidado adicional.

Por último, devem ser envidados esforços para garantir a exatidão dos dados e permitir a correção de dados inexatos. Os indivíduos devem ser encorajados a nos informar quando seus dados forem alterados. Por exemplo, os colaboradores devem ser incentivados a atualizar detalhes como endereço residencial quando necessário.

Privacidade por Design e Padrão (Privacy by Design and by Default) Temos de assegurar que, no planeamento e implementação de quaisquer novos sistemas, aplicações ou quaisquer outros projetos que impliquem a coleta ou o tratamento de dados pessoais, os princípios e salvaguardas da privacidade sejam abordados desde o início do projeto e durante todo o seu ciclo de vida. Isso significa que devemos garantir que as configurações de privacidade, acesso a dados e anonimização sejam consideradas, desde a fase de design de um projeto. Consulte o Procedimento Privacy by Design para obter mais orientações.

Retenção de registros
Quando os dados pessoais que nos são confiados deixam de ser necessários ou a finalidade para a qual foram coletados foi cumprida, devem ser eliminados ou anonimizados. Se mantido, ele deve estar em conformidade com as políticas e processos de gerenciamento de registros da Companhia e devemos deixar isso claro para o indivíduo.

Governar e proteger dados e informações dentro do nosso ecossistema:

Integridade, confidencialidade e limitação de armazenamento
Devemos tomar medidas apropriadas para proteger e proteger os dados pessoais (por exemplo, criptografia, senhas, uso de repositórios de dados aprovados), inclusive contra perda e

comprometimento e, sempre que possível, anonimizar os dados. A anonimização é particularmente relevante se estivermos testando sistemas em um domínio de teste público. Dados reais não devem ser usados em um ambiente de teste.

Além disso, os dados pessoais não devem ser armazenados por mais tempo do que o legalmente exigido ou do que o necessário para cumprir a finalidade para a qual foram coletados, de acordo com as políticas de retenção de dados da Companhia.

Segurança dos Dados Pessoais

Devemos implementar medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado aos riscos apresentados por uma atividade de tratamento de dados pessoais (por exemplo, anonimização, retenção limitada no ambiente de teste). Isso nos permite reduzir a probabilidade de sofrer um ataque cibernético, incluindo um que resulte no acesso não autorizado, divulgação ou perda de dados pessoais. Consulte a **Política de Segurança da Informação** para obter mais orientações.

Gerenciamento de riscos de privacidade de terceiros

Nossa Companhia deve ter controles legais e comerciais para demonstrar a governança de privacidade apropriada quando os dados pessoais são tratados em seu nome por terceiros. A Companhia deve manter um registro completo de terceiros que tratam dados pessoais. Terceiros que coletam e tratam dados pessoais para nossos negócios devem estar sob contrato. Além disso, todos os terceiros que tratam dados em nosso nome devem:

- Ter um acordo vinculativo com uma de nossas empresas incorporando requisitos mínimos de privacidade e segurança e due diligence documentada;
- Garantir a conformidade com o GDPR e qualquer outra lei de proteção de dados aplicável;
- Agir somente mediante instruções documentadas do(s) representante(s) autorizado(s);
- Impor obrigações de confidencialidade a todo o pessoal que trata os nossos dados;
- Garantir a segurança dos dados;
- Cumprir as regras de nomeação de quaisquer subprocessadores;
- Implementar medidas para nos ajudar em relação aos direitos dos titulares de dados individuais;
- Auxiliar-nos na obtenção de aprovação, quando necessário, das Autoridades de Proteção de Dados;
- Sob nossa discricionariedade, devolver ou destruir dados;
- Fornecer-nos oportunamente todas as informações necessárias para demonstrar a conformidade com o acima; e
- Comunicar imediatamente problemas de privacidade de dados ou violações conforme estabelecido em nossos documentos.

Podemos divulgar dados pessoais a terceiros quando exigido por lei para fazê-lo, como quando necessário para proteger nossos direitos legais, ou em uma emergência em que a saúde ou a segurança de um indivíduo esteja em perigo. Antes de tais divulgações, devemos sempre tomar medidas para confirmar que os dados pessoais são divulgados apenas às partes autorizadas. Consulte o **Procedimento de Gerenciamento de Risco de Privacidade de Terceiros** para colaboradores para obter mais orientações.

A Companhia implementou controles para identificar, gerenciar, resolver, documentar e relatar adequadamente violações de dados pessoais e estes devem ser sempre respeitados. Qualquer aquisição, uso ou acesso não autorizado conhecido ou suspeito a dados pessoais deve ser relatado imediatamente através do nosso Formulário de Relatório de Violação de Dados: https://avon.ethicspointvp.com/custom/avon/iir/form_data.asp

Isso garante que a organização use seus procedimentos para lidar com incidentes de privacidade de forma correta e rápida para reduzir o risco para os indivíduos, possíveis avisos regulatórios, investigações e aplicação, interrupção da continuidade dos negócios e danos à reputação. Consulte o **Procedimento de Gestão de Violação de Dados Pessoais** e a **Política de Segurança de Informações** para obter mais orientações.

Transferências transfronteiriças de dados

Qualquer atividade de tratamento que realizemos que possa envolver uma transferência

transfronteiriça de dados pessoais (por exemplo, transferências da União Europeia - UE para mercados na América Latina) deve ser avaliada para determinar se está em conformidade com a regulamentação aplicável e se são necessárias salvaguardas. Usamos cláusulas contratuais padrão da UE ou cláusulas semelhantes para apoiar transferências de dados.

Responsabilidade
Nossa Companhia deve ser capaz de demonstrar conformidade com esta Política, pois somos obrigados a assumir a responsabilidade pelo que fazemos com dados pessoais. Como resultado, devemos ter medidas e registros apropriados em vigor para poder demonstrar a conformidade adequada com o tratamento de dados pessoais.

Registro de Atividades de Tratamento (ROPA)
Devemos manter um registro dos dados pessoais da Companhia, descrevendo os sistemas em vigor e as atividades de tratamento que realizamos. Nosso ROPA cobre todos os requisitos relevantes (por exemplo, categorias de titulares de dados, finalidades, bases legais) e é revisado regularmente para precisão.

Avaliação de impacto sobre a proteção de dados
Quando necessário, a Companhia realiza uma avaliação de impacto à proteção de dados se houver um grande projeto envolvendo dados pessoais ou se a atividade de tratamento for suscetível de resultar em um "alto risco" para os indivíduos. Isso inclui certos tipos de tratamento, como avaliação ou pontuação de indivíduos, qualquer uso de inteligência artificial, tomada de decisão automatizada, monitoramento sistemático, tratamento de dados sensíveis, tratamento de dados em larga escala, soluções tecnológicas ou organizacionais inovadoras e combinação, comparação ou correspondência de dados de várias fontes.

Essas avaliações nos permitem identificar precocemente os riscos colaboradores ao tratamento de dados e implementar controles apropriados. A função Privacidade de Dados determinará onde eles são necessários e orientará as partes interessadas a concluí-los conforme necessário.

Treinamento & Conscientização
Para garantir o cumprimento desta Política, a Companhia fornece treinamento global para todos os nossos colaboradores e treinamento direcionado aos colaboradores que coletam ou usam dados pessoais. A Companhia monitora sua conclusão e os materiais de conscientização são compartilhados periodicamente.

Auditoria e Monitoramento
A função de auditoria interna do Grupo auditará de forma independente a implementação e a adesão a esta Política globalmente como parte de seu plano anual de auditoria em colaboração com o Encarregado pela Proteção de Dados da Natura e a função de Privacidade de Dados. As conclusões serão fornecidas às Unidades de Negócio, ao Conselho de Administração e/ou aos comitês relevantes.

Violações
O não cumprimento desta Política pode ter sérias consequências para a Companhia e seus colaboradores, incluindo penalidades civis e criminais e danos à reputação. Se você tiver algum motivo para acreditar que alguma ação não está em conformidade com esta Política, você deve denunciá-la imediatamente ao Encarregado pela Proteção de Dados da Natura e/ou à equipe de privacidade de dados: privacy@natura.net

Perguntas
Dúvidas relacionadas a esta Política podem ser direcionadas para a função Privacidade de Dados em: privacy@natura.net