	POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS	**Emissão** **29/09/2023** **Atualização em 02/12/2025**	**Classificação** **Uso interno e externo**
Código **PGPDP-01**		**Versão** **1.0**	**Aprovado por:** **Comitê Gestor de Dados Pessoais**

SUMÁRIO

INTRODUÇÃO 2

DIRETRIZES GERAIS 2

1. OBJETIVO 5

2. ABRANGÊNCIA 5

3. GOVERNANÇA E RESPONSABILIDADES 6

3.1. COMITÊ DE PROTEÇÃO DE DADOS PESSOAIS 6

3.2. ENCARREGADO DE PROTEÇÃO DE DADOS (DPO) 7

3.3. SEGURANÇA DA INFORMAÇÃO 7

3.4. USUÁRIOS DA INFORMAÇÃO 8

4. DIREITOS DOS TITULARES 9

5. TRATAMENTO E FINALIDADE DE DADOS 9

5.1. TRATAMENTO DE DADOS ON-CHAIN E METADADOS DE BLOCKCHAIN 10

5.2. COMPARTILHAMENTO DE DADOS PARA CUMPRIMENTO DA TRAVEL RULE 11

5.3. PROTEÇÃO DE CHAVES PRIVADAS E ACESSO AOS DADOS CRIPTOGRÁFICOS 11

5.4. RETENÇÃO E DESCARTE DE DADOS 11

5.5. RETENÇÃO DE LOGS E EVIDÊNCIAS 12

5.6. RESPOSTAS A INCIDENTES E NOTIFICAÇÃO RELACIONADA A ATIVOS VIRTUAIS 12

6. SANÇÕES 12

7. CASOS OMISSOS 13

8. GLOSSÁRIO: 13

9. REVISÕES 14

10. TERMO DE APROVAÇÃO 15

INTRODUÇÃO

A presente Política de Proteção de Dados tem por finalidade estabelecer os princípios, regras, controles e práticas adotadas pela instituição para garantir o tratamento adequado, lícito, transparente e seguro de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados (LGPD) e com os requisitos adicionais introduzidos pela Resolução BCB nº 520/2025, que disciplina, entre outros aspectos, os controles operacionais, tecnológicos e organizacionais relacionados às prestadoras de serviços de ativos virtuais.

A instituição, atuando simultaneamente como corretora de câmbio e como intermediadora de ativos virtuais, reconhece que o tratamento de dados pessoais é fundamental para a integridade de suas operações, devendo observar padrões elevados de governança, segurança da informação, rastreabilidade e proteção aos direitos dos titulares.

O GRUPO GUITTA entende que a privacidade é um direito fundamental da pessoa natural, bem como que, em seus processos de negócio ocorre o tratamento de dados pessoais, essa informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a proteção de dados pessoais e afetar negativamente a privacidade dos seus titulares.

Dessa forma, o GRUPO GUITTA estabelece sua POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS (PGPDP), como parte integrante do seu sistema de gestão corporativa, compatível com os requisitos da legislação brasileira, além de boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção para os dados pessoais tratados pela organização.

DIRETRIZES GERAIS

O objetivo da Proteção de Dados no GRUPO GUITTA é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à proteção de dados pessoais e dos direitos dos seus titulares, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a organização.

O Conselho de Administração, o Comitê Gestor de Proteção de Dados Pessoais e o DPO estão comprometidos com uma gestão efetiva da Proteção de Dados Pessoais no GRUPO GUITTA.

Desta forma, adotam todas medidas cabíveis para garantir que a presente política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades do GRUPO GUITTA.

Nesta política, apresentaremos os procedimentos que servirão de fundamentação para a proteção de dados pessoais pela Guitta Corretora como corretora de câmbio e intermediadora de ativos virtuais, seguindo estritamente as normativas vigentes do Banco Central do Brasil. Dentre as diretrizes gerais estão:

- Garantir a proteção de dados pessoais em todas as etapas do fluxo de tratamento;
- Manter controles compatíveis com a Resolução BCB 520/25, incluindo proteção de chaves privadas, trilhas de auditoria e segregação patrimonial;
- Implementar mecanismos de Travel Rule para compartilhamento de dados de originador e beneficiário;
- Realizar avaliações periódicas de riscos de proteção de dados;
- Manter registros de operações e incidentes pelo prazo mínimo de cinco anos;

É dever do GRUPO GUITTA:

- Assegurar ao titular a titularidade de seus dados pessoais, garantindo os direitos fundamentais de liberdade, intimidade e privacidade. Sendo direitos do titular: confirmar a existência de tratamento de seus dados pessoais; acessá-los; corrigi-los; anonimizá-los; bloqueá-los ou eliminá-los; realizar a portabilidade; obter informações sobre o compartilhamento; e revogar o consentimento dado;
- Garantir que o objetivo do tratamento de dados pessoais esteja em conformidade com a legislação vigente;
- Comunicar, de forma clara e objetiva, o tratamento de dados pessoais ao titular, antes do momento em que os dados são usados pela primeira vez para um novo propósito;
- Sempre que solicitado, fornecer ao titular explicações suficientes sobre o tratamento de seus dados pessoais, conforme previsto na legislação vigente;
- Limitar a coleta de dados pessoais estritamente ao que é permitido pela legislação vigente, e aos objetivos especificados durante a coleta de consentimento do titular dos dados pessoais, minimizando, quando possível, a quantidade de dados coletados;
- Limitar o uso, retenção, divulgação e transferência dos dados pessoais apenas ao necessário para o cumprimento dos objetivos específicos, explícitos e legítimos;

- Reter dados pessoais apenas pelo tempo necessário para cumprir os propósitos declarados e, posteriormente, destruí-los, bloqueá-los ou anonimizá-los com segurança;
- Bloquear o acesso aos dados pessoais e não realizar mais nenhum tratamento quando os propósitos declarados expirarem, mas a retenção dos dados pessoais for exigida pela legislação vigente;
- Garantir a precisão e qualidade dos dados pessoais tratados, excetuando-se os casos onde exista uma base legal para manter armazenados os dados desatualizados;
- Fornecer aos titulares dos dados pessoais tratados, informações claras e facilmente acessíveis sobre as políticas, procedimentos e boas práticas da organização com relação ao tratamento de dados pessoais, incluindo quais dados são efetivamente tratados, a finalidade desse tratamento e as informações de contato para obter maiores detalhes e/ou realizar reclamações;
- Notificar os titulares quando ocorrerem alterações significativas no tratamento dos seus dados, exceto para fins de newsletter e a finalidade específica, visto que é previamente autorizado junto ao Grupo Guitta;
- Garantir que os titulares tenham meios para acessar e revisar seus dados pessoais, desde que sua identidade seja autenticada com um nível apropriado de garantia, e que não exista nenhuma restrição legal a esse acesso ou a revisão dos dados pessoais;
- Garantir a rastreabilidade e prestação de contas durante todo o tratamento de dados pessoais, incluindo quando houver o compartilhamento dos dados pessoais com terceiros;
- Tratar integralmente as violações de dados, garantindo que sejam adequadamente registradas, classificadas, investigadas, corrigidas e documentadas;
- Garantir que, na ocorrência de uma violação de dados, todas as partes interessadas serão notificadas, conforme requisitos e prazos previstos na legislação vigente;
- Documentar e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados;
- Garantir a existência de um responsável por documentar, implementar e comunicar as políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados;
- Adotar controles de segurança da informação, tanto técnicos quanto administrativos, suficientes para garantir os níveis de proteção adequados para o tratamento de dados pessoais;
- Disponibilizar políticas, normas e procedimentos para proteção de dados pessoais a todas as partes interessadas e autorizadas, tais como: empregados, terceiros contratados e, quando pertinente, clientes;

- Garantir a educação e conscientização de empregados, terceiros contratados, parceiros e clientes, sobre as práticas de proteção de dados pessoais adotadas pelo GRUPO GUITTA;
- Melhorar continuamente a Gestão de Proteção de Dados Pessoais através da definição e revisão sistemática dos objetivos de privacidade e proteção de dados pessoais em todos os níveis da organização;
- Garantir a não discriminação no tratamento de dados pessoais, impossibilitando que estes sejam usados para fins discriminatórios, ilícitos ou abusivos;
- Garantir a conformidade e adequação integral quanto às leis e regulamentações de proteção de Dados Pessoais, em especial a Lei n° 13.709/2018 (LGPD).

1. OBJETIVO

- Estabelecer diretrizes de Proteção de Dados que permitam ao GRUPO GUITTA realizar o tratamento de dados pessoais, em conformidade com a legislação brasileira, em especial da Lei Geral de Proteção de Dados (LGPD);
- Orientar quanto à adoção de controles técnicos e administrativos para atendimento aos requisitos de proteção de dados pessoais, conforme a legislação vigente;
- Resguardar os direitos dos titulares dos dados pessoais que são tratados pelo GRUPO GUITTA, garantindo, principalmente, os direitos fundamentais de liberdade e da privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural;
- Prevenir possíveis causas de violações de dados pessoais e incidentes de segurança da informação relacionados ao tratamento de dados pessoais;
- Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio do GRUPO GUITTA, como resultado de violações de dados;
- Garantir o tratamento adequado e seguro de dados pessoais em todas as operações da empresa.
- Assegurar conformidade integral com a LGPD e Resolução BCB 520/25, especialmente no tratamento de dados associados a operações com ativos virtuais.
- Estabelecer práticas transparentes e mecanismos de governança para proteção dos titulares de dados.
- Definir controles relacionados à segurança cibernética, retenção, registro, rastreabilidade e segregação patrimonial.

2. ABRANGÊNCIA

Esta política se aplica a qualquer operação de tratamento de dados pessoais realizada pelo GRUPO GUITTA, independentemente do meio ou do país onde estejam localizados os dados, desde que:

- A operação de tratamento seja realizada em território nacional brasileiro;
- Tenha por objetivo a oferta ou o fornecimento de serviços ou o tratamento de dados de indivíduos localizados no território nacional;
- Os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

3. GOVERNANÇA E RESPONSABILIDADES

A instituição designa um Representante Responsável pela Proteção de Dados e Conformidade com a Resolução BCB 520/25, através de ata de nomeação, se trata de profissional com autonomia operacional e acesso à alta administração, responsável por supervisionar a adequação normativa, implementar controles específicos relativos ao tratamento de dados, garantir o alinhamento entre LGPD, Bacen, ANPD e demais órgãos reguladores, bem como coordenar ações envolvendo dados utilizados em processos de identificação, verificação, travel rule, segregação patrimonial e análise de riscos.

O Representante Responsável atuará de forma integrada ao DPO e à área de Segurança da Informação, garantindo que todos os tratamentos sejam compatíveis com a regulamentação setorial e com a natureza sensível dos dados aplicados às operações com ativos virtuais.

3.1. COMITÊ DE PROTEÇÃO DE DADOS PESSOAIS

O comitê gestor de proteção de dados pessoais, conta com a participação de pelo menos um representante da diretoria e um membro das seguintes áreas: Tecnologia da Informação, Recursos Humanos e Compliance. São responsabilidades do comitê:

- Analisar, revisar e aprovar políticas e normas relacionadas à proteção de dados pessoais;
- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Proteção de Dados Pessoais;
- Garantir que o tratamento de Dados Pessoais seja realizado em conformidade com esta POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS e com a legislação vigente (LGPD);
- Promover a divulgação da PGPDP e tomar as ações necessárias para disseminar uma cultura de proteção de Dados Pessoais no ambiente corporativo do GRUPO GUITTA.

- Avaliar riscos, revisar incidentes e supervisionar conformidade;
- Integrar discussões de segurança e regulamentação de ativos virtuais;

3.2. ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)

O Data Protection Officer se trata do Encarregado de Proteção de Dados, este profissional é responsável por garantir que a instituição esteja em conformidade com as leis de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados). É responsabilidade do Encarregado pelo Tratamento de Dados Pessoais:

- Atuar como ponto de contato com titulares, ANPD e Bacen.
- Acompanhar incidentes envolvendo dados pessoais e sistemas associados a operações com ativos virtuais.
- Aceitar reclamações e comunicações dos titulares de dados pessoais, prestar esclarecimentos e adotar as providências necessárias;
- Receber comunicações da ANPD - Autoridade Nacional de Proteção de Dados e adotar as providências necessárias;
- Orientar os empregados, terceiros contratados e demais partes do GRUPO GUITTA a respeito das boas práticas a serem adotadas em relação à proteção de dados pessoais;
- Atender as demais atribuições, conforme orientação da ANPD - Autoridade Nacional de Proteção de Dados, definidas em normas complementares publicadas pelo referido órgão;
- Atuar junto ao time de Segurança da Informação no ajuste das normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PGPDP;
- Identificar e avaliar as principais ameaças à proteção de dados, bem como propor e, se aprovado, apoiar a implantação de medidas corretivas para reduzir o risco;
- Tomar as ações cabíveis para se fazer cumprir os termos desta Política;
- Apoiar a gestão das violações de dados pessoais, garantindo tratamento adequado e comunicando, em prazo razoável, a ANPD e os titulares afetados pela violação sempre que esta representar risco ou dano relevante aos titulares;

3.3. SEGURANÇA DA INFORMAÇÃO

A instituição atua somente com a intermediária de ativos virtuais, entretanto, adota controles técnicos e administrativos rigorosos, compatíveis com o nível de complexidade das operações,

incluindo criptografia, autenticação multifatorial, segregação de ambientes, controle de privilégios, monitoramento contínuo, trilhas de auditoria imutáveis e políticas específicas para proteção de chaves privadas utilizadas em operações com ativos virtuais.

São implementadas práticas de hardening, backups redundantes, controle seguro de APIs, proteção contra engenharia social e mecanismos de prevenção a incidentes cibernéticos. Em caso de incidente de segurança envolvendo dados pessoais, a instituição notificará, quando aplicável, titulares, ANPD e Banco Central, conforme a gravidade e o impacto identificado.

É de responsabilidade do time de segurança da Informação:

- Implementar controles reforçados, incluindo autenticação multifatorial, gestão segura de chaves privadas, segregação de ambientes e registros auditáveis.
- Garantir resposta a incidentes envolvendo plataformas e APIs conectadas à blockchain.
- Garantir que as políticas, normas e procedimentos de Segurança da Informação sejam ajustados de forma a atender os requisitos da Política Geral de Proteção de Dados Pessoais;
- Adotar medidas de segurança, tanto técnicas quanto administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme padrões mínimos recomendados pela ANPD - Autoridade Nacional de Proteção de Dados.
- Realizar o tratamento de incidentes de segurança da informação que envolvam o tratamento de dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação dentro de um prazo razoável.
- Apoiar o Encarregado pelo tratamento de dados pessoais na comunicação à ANPD e ao titular dos dados pessoais em casos de ocorrência de incidente de segurança que possam acarretar risco ou dano relevante aos titulares.
- Criptografia, segregação de ambientes, trilhas de auditoria e controle de privilégios.
- Plano de resposta a incidentes com procedimentos específicos para chave privada, invasões e falhas operacionais.
- Monitoramento contínuo de riscos cibernéticos.

3.4. USUÁRIOS DA INFORMAÇÃO

É de responsabilidade dos usuários da informação, ou seja, colaboradores e prestadores de serviço:

- Ler, compreender e cumprir integralmente os termos da Política Geral de Proteção de Dados Pessoais de Ativos Virtuais, bem como as demais normas e procedimentos de proteção de dados pessoais aplicáveis;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Proteção de Dados Pessoais, suas normas e procedimentos ao Encarregado pelo Tratamento de Dados Pessoais ou, quando pertinente, ao Comitê Gestor de Proteção de Dados Pessoais;
- Comunicar ao Encarregado pelo Tratamento de Dados Pessoais qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco Dados Pessoais tratados pelo GRUPO GUITTA;
- Manter atualizado o Termo de Responsabilidade do Grupo Guitta junto aos seus colaboradores e prestadores de serviço, formalizando a ciência e o aceite integral das disposições da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu comprometimento;
- Responder pela inobservância da Política Geral de Proteção de Dados Pessoais, normas e procedimentos relacionados ao tratamento de Dados Pessoais, conforme definido no item sanções e punições.

4. DIREITOS DOS TITULARES

Os titulares de dados possuem direito de acesso, correção, anonimização, eliminação, portabilidade, informações sobre compartilhamento e revogação do consentimento, quando aplicável. A instituição adota procedimentos formalizados para atendimento das solicitações dos titulares, garantindo respostas tempestivas e transparentes.

Quando dados forem necessários para cumprimento de obrigações legais, especialmente as previstas na Resolução nº 520/2025, alguns direitos poderão ser limitados em razão da exigência de retenção por parte do regulador ou da necessidade de manutenção de registros de operações.

5. TRATAMENTO E FINALIDADE DE DADOS

O tratamento de dados se trata de toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação,

avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Para atividades relacionadas à intermediação de ativos virtuais, são tratados dados de originadores, beneficiários, endereços de carteira, histórico de transações e demais informações necessárias à rastreabilidade plena das operações, inclusive para cumprimento da travel rule.

Serão utilizados sistemas especializados para análise on-chain, verificação de risco de carteiras e monitoramento de fluxos suspeitos. Todos os dados relacionados serão tratados de forma segura, com segregação patrimonial e controles equivalentes aos exigidos pelo Bacen. Considerando que se trata de produto recém implementado na instituição, sendo necessárias readequações após o início do processo estaremos atualizando as informações e manual.

A instituição coleta, utiliza e armazena dados pessoais exclusivamente para finalidades legítimas e necessárias, dentre as quais destacam-se: identificação de clientes, cumprimento de obrigações legais e regulatórias, prevenção à lavagem de dinheiro, execução de serviços contratados, análise de risco, rastreabilidade de operações com ativos virtuais, execução da Travel Rule e proteção contra fraudes.

O tratamento de dados observará constantemente os princípios de finalidade, adequação, necessidade, segurança, prevenção e responsabilização. Quanto ao tratamento de dados no contexto de ativos virtuais, contempla:

- Coleta e armazenamento seguro das informações de originador e beneficiário.
- Registro imutável e rastreável das transações relacionadas.
- Controle reforçado de acesso a carteiras, APIs e sistemas integrados.
- Due diligence ampliada para validação de carteiras, histórico on-chain e perfil do titular.

5.1. TRATAMENTO DE DADOS ON-CHAIN E METADADOS DE BLOCKCHAIN

Os dados derivados de transações on-chain, incluindo endereços de carteira, hashes de transações, metadados de roteamento de ativos virtuais e informações geradas por ferramentas de análise blockchain, serão tratados como dados pessoais sensíveis sempre que possibilitarem a identificação do titular. A Instituição adotará salvaguardas técnicas avançadas, como segregação lógica de ambientes, minimização de dados e pseudonimização,

além de controles específicos para impedir correlação indevida entre dados pessoais e dados públicos registrados em blockchain.

Considerando que se trata de produto recém implementado na instituição, sendo necessárias readequações após o início do processo estaremos atualizando as informações e manual.

5.2. COMPARTILHAMENTO DE DADOS PARA CUMPRIMENTO DA TRAVEL RULE

Para cumprir as obrigações estabelecidas pela Resolução 520/25, a Instituição poderá compartilhar dados pessoais com outros prestadores de serviços de ativos virtuais, instituições financeiras e autoridades competentes, exclusivamente para fins de identificação de originadores e beneficiários em transferências de ativos virtuais. O compartilhamento ocorre sob a base legal do art. 7º, II e VI, da LGPD (cumprimento de obrigação legal e exercício regular de direito), sendo vedado qualquer uso incompatível com essa finalidade.

Considerando que se trata de produto recém implementado na instituição, sendo necessárias readequações após o início do processo estaremos atualizando as informações e manual.

5.3. PROTEÇÃO DE CHAVES PRIVADAS E ACESSO AOS DADOS CRIPTOGRÁFICOS

As chaves privadas, seeds, credenciais de acesso a carteiras digitais, ambientes de custódia, módulos de segurança criptográfica (HSM) e demais segredos tecnológicos utilizados pela Instituição serão tratados como dados de segurança sensíveis, com acesso estritamente limitado, registro de logs imutáveis e segregação total entre ambientes de produção, teste e contingência. Qualquer acesso será autorizado exclusivamente sob o princípio do "menor privilégio" e monitorado em tempo real.

Considerando que se trata de produto recém implementado na instituição, sendo necessárias readequações após o início do processo estaremos atualizando as informações e manual.

5.4. RETENÇÃO E DESCARTE DE DADOS

Os dados pessoais serão retidos pelo prazo necessário ao cumprimento de obrigações legais, regulatórias e contratuais, respeitando-se o prazo mínimo de cinco anos exigido pela Resolução BCB 520/25 para registros relacionados a operações financeiras e com ativos virtuais. Após o término do prazo, os dados serão eliminados, anonimizados ou arquivados conforme determinação legal.

Considerando que se trata de produto recém implementado na instituição, sendo necessárias readequações após o início do processo estaremos atualizando as informações e manual.

5.5. RETENÇÃO DE LOGS E EVIDÊNCIAS

A Instituição manterá logs de acesso, registros de validação de Travel Rule, dossiês de onboarding, relatórios de análise on-chain e evidências de monitoramento por prazo mínimo de 5 anos após o término da relação comercial, ou por período superior quando necessário para atender investigações, auditorias ou determinações do Banco Central. O armazenamento será realizado em ambiente seguro, com mecanismos de integridade, redundância e criptografia.

Considerando que se trata de produto recém implementado na instituição, sendo necessárias readequações após o início do processo estaremos atualizando as informações e manual.

5.6. RESPOSTAS A INCIDENTES E NOTIFICAÇÃO RELACIONADA A ATIVOS VIRTUAIS

A Instituição manterá plano de resposta a incidentes especificamente aplicável a operações com ativos virtuais, incluindo vazamento de chaves privadas, falhas de integridade, ataques cibernéticos, acessos não autorizados, clonagem de credenciais ou qualquer fato que comprometa a segurança das operações. Em tais situações, a Instituição notificará imediatamente o Encarregado de Dados, a autoridade supervisora competente e, quando aplicável, os titulares afetados, conforme previsto na LGPD e regulamentações do Banco Central.

6. SANÇÕES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de proteção de dados pessoais, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Proteção de Dados Pessoais, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho,

podendo o CGPDP, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

No caso de terceiros contratados ou prestadores de serviço, o CGPDP deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em riscos aos titulares de dados pessoais, ou dano ao GRUPO GUITTA, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 6.1, 6.2 e 6.3 desta política.

7. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê Gestor de Proteção de Dados Pessoais para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de proteção de dados pessoais, não se esgotam em razão da contínua evolução tecnológica, da legislação vigente e constante surgimento de novas ameaças e requisitos. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do GRUPO GUITTA adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção de dados pessoais tratados pelo GRUPO GUITTA.

8. GLOSSÁRIO:

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
Autoridade Nacional de Proteção de Dados Pessoais - ANPD: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (lei nº 13.709, de 14 de agosto de 2018) em todo território nacional brasileiro;
Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Comitê Gestor de Proteção de Dados Pessoais – CGPDP: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do GRUPO GUITTA, que tem por finalidade tratar questões ligadas à Proteção de Dados Pessoais;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Dado Anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do GRUPO GUITTA.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Tratamento de dados pessoais: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Usuário da informação: Empregados com vínculo empregatício de qualquer área das empresas que compõem o GRUPO GUITTA ou terceiros alocados na prestação de serviços ao GRUPO GUITTA, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do GRUPO GUITTA para o desempenho de suas atividades profissionais;

Violação de dados pessoais: situação em que dados pessoais são processados violando um ou mais requisitos relevantes de proteção da privacidade.

9. REVISÕES

Esta Política será revisada anualmente ou sempre que houver atualização regulatória relevante.

10. TERMO DE APROVAÇÃO

Pelo presente termo, há necessidade de aprovação pelo Comitê Gestor de Proteção de Dados Pessoais, Diretoria do Grupo Guitta e a gerente de compliance para aprovação deste documento. Por fim, informam que leram e aprovaram todo o conteúdo constante na Política Geral de Proteção de Dados Pessoais – Ativos Virtuais, emitido em 02/12/2025, assumindo também o compromisso de manter atualizada dando total apoio para que as normas vigentes sejam aplicadas nesta instituição da melhor maneira possível.

Eduardo Satiro dos Santos – Sócio diretor

Clézio Corneta – Sócio diretor

Julio Cesar Letra – Sócio diretor

Juarez Aparecido Kamimura – Diretor T.I.

Andréa Cristina – Gestora RH

Camila Graziele Zani – Gestora Compliance

Lucas Silveira Lopes – D.P.O.