2025.2
V. 2

# Política

## Privacidade e Proteção de Dados


VRDEBANK

# 01. Objetivo

Através desta política, o VrdeBank busca Prevenir, detectar, reduzir, vulnerabilidades e responder aos eventuais incidentes de segurança da informação, bem como, com base na Lei Geral de Proteção de Dados, chama para a ação todos os colaboradores, independente do seu nível hierárquico, para proteger todos os dados contidos em ambientes computacionais de processamento em nuvem ou locais e todos os equipamentos da organização.

# 02. Escopo

Esta Política se aplica a toda organização, aos seus empregados, parceiros, sejam eles pessoas físicas ou jurídicas que atuam para ou em nome do VrdeBank em quaisquer operações que envolvam tratamento de dados pessoais que sejam realizadas em contrato com o banco, a terceiros que de qualquer forma se relacionem com o banco e que venham a ter contato com os dados da organização ou por esta tratada, bem como aos titulares de dados pessoais, cujos dados são tratados pelo VrdeBank.

Todos aqueles que possuem relações contratuais com esta organização comprometem-se em aderir ao programa de compliance, o que também inclui a observância desta política sabendo que todos os dados detidos, usados ou transmitidos pelo ou em nome do VrdeBank, em qualquer tipo de mídia, bem como todas as operações que envolvam o tratamento de dados pessoais e são realizadas no escopo do banco estão subordinadas a este normativo.

# 03. Definições e Conceitos

- Dados Pessoais: Informações que identificam ou podem identificar uma pessoa física, como nome, endereço, número de identificação, etc.
- Dados Sensíveis: Informações sobre raça, etnia, opiniões políticas, crenças religiosas, saúde, orientação sexual, etc., que merecem proteção especial.
- Titular dos Dados: Pessoa física ou jurídica a quem os dados se referem.
- Controlador: Pessoa física ou Jurídica que decide como e por que os dados pessoais são tratados.
- Operador: Pessoa física ou Jurídica que realiza o processamento de dados em nome do controlador.
- Encarregado de Proteção de Dados (DPO): Pessoa responsável por garantir a conformidade com as leis de proteção de dados dentro da organização
- Consentimento: Permissão concedida pelo titular dos dados para processar seus dados pessoais, baseada em informação clara e específica.
- Anonimização: Processo pelo qual os dados pessoais são irreversivelmente transformados para que não possam mais identificar um indivíduo específico.


- Cookies: Pequenos arquivos de texto armazenados no dispositivo do usuário que são usados para melhorar a experiência online, mas também podem coletar dados pessoais.
- Segurança da Informação: Medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, perda ou destruição.
- Cloud: Refere-se ao armazenamento e processamento de informações em servidores remotos, geralmente mantidos por provedores de serviços de computação em nuvem.
- Framework: Conjunto de diretrizes, princípios e procedimentos que o VRDE adota para garantir a conformidade com as leis de proteção de dados e para proteger a privacidade das informações dos usuários.

# 04. Princípios da Proteção de Dados

- Finalidade: O tratamento dos dados deve ter propósitos legítimos, específicos, explícitos e informados ao titular. O VRDE não usa os dados para finalidades incompatíveis com aquelas inicialmente comunicadas.
- Adequação: O tratamento deve ser compatível com as finalidades informadas ao titular, considerando o contexto em que os dados são coletados.
- Necessidade: O tratamento deve ser limitado ao mínimo necessário para atingir suas finalidades. O VRDE coleta apenas os dados pertinentes e proporcionais que precisam ser utilizados.
- Livre Acesso: Os titulares têm o direito de consultar as informações sobre como seus dados estão sendo tratados e sobre a integralidade destes. Através desta política o VRDE torna pública a forma que trata os dados.
- Qualidade dos Dados: Os dados devem ser mantidos atualizados, precisos, claros e relevantes para a finalidade do tratamento.
- Transparência: O VRDE garante aos titulares informações claras e acessíveis sobre o tratamento de seus dados pessoais, incluindo os agentes envolvidos, resguardando o segredo industrial e comercial.
- Segurança: O VRDE adota as melhores medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração ou divulgação indevida.

VRDEBANK

# 05. Direitos dos Titulares

São direitos dos titulares de dados:

- Confirmação da Existência de Tratamento: O titular dos dados tem o direito de confirmar se a VRDE realiza o tratamento de seus dados pessoais. Isso inclui atividades como coleta, armazenamento, uso e classificação.

- Acesso aos Dados: O titular pode solicitar acesso aos dados que a organização possui.

- Correção de Dados: O titular tem o direito de solicitar a correção de dados pessoais incompletos, inexatos ou desatualizados, bem como solicitar a retificação. O VRDE entende que os titulares devem informar sempre que seus dados forem alterados para que o banco mantenha seus dados atualizados.

- Anonimização, Bloqueio ou Eliminação de Dados: O titular pode requerer a anonimização, bloqueio ou eliminação de seus dados pessoais, especialmente quando o tratamento não estiver em conformidade com a lei.

- Compartilhamento de Dados: O titular tem o direito de saber com quais terceiros a organização compartilha seus dados pessoais.

- Portabilidade dos Dados: O titular tem o direito de receber seus dados pessoais em formato estruturado e de uso comum, possibilitando a transferência para outro serviço ou banco, respeitados o segredo comercial e industrial da Instituição, bem como os limites técnicos de sua infraestrutura.

- Eliminação dos Dados Tratados com Consentimento: Se o tratamento dos dados for baseado no consentimento do titular, ele pode revogar este consentimento e solicitar a exclusão dos dados, ressalvadas as exceções da legislação.

VRDEBANK

# 06. Coleta e Finalidade

Os dados pessoais poderão ser fornecidos pelo próprio titular ao Vrde ou coletados automaticamente por meios digitais. Além disso, poderão ser recebidos através de terceiros que mantenham algum relacionamento com o titular dos dados, bem como de bases disponibilizadas por autoridades públicas ou por terceiros, como bureaus de crédito.

Também podem ser obtidos de fontes públicas como a Internet, meios de comunicação, mídias sociais, registros públicos e outras possíveis fontes permitidas pela legislação aplicável. Os dados tornados públicos pelo próprio titular em sites ou redes sociais também podem ser coletados, sempre respeitando rigorosamente a Lei.

O Vrde realizará o tratamento de dados pessoais com finalidades específicas e em conformidade com a legislação da seguinte forma:

- Mediante o fornecimento de consentimento pelo titular;
- Para o cumprimento de obrigação legal ou regulatória;
- Para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, conforme estabelecido pela LGPD;
- Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular faça parte, a pedido deste;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Quando necessário para atender aos interesses legítimos do VRDE ou de terceiros, desde que não prevaleçam os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- Realizar análises de risco de crédito, conforme estipulado na legislação pertinente;
- Assegurar a adequada identificação, qualificação e autenticação do titular;
- Garantir maior segurança e prevenção contra fraudes, prevenindo atos relacionados à lavagem de dinheiro e outras atividades ilícitas;
- Aperfeiçoar o atendimento, assim como os produtos e serviços oferecidos;
- Ofertar produtos e serviços adequados e relevantes aos interesses e necessidades do titular, de acordo com seu perfil;
- Cumprir obrigações trabalhistas;
- Outras finalidades legítimas, sempre com estrita observância à Lei.

# 07. Segurança da Informação

Todos os dados pessoais fornecidos pelo titular ao Vrde, coletados automaticamente ou recebidos de fontes externas, serão armazenados em bases de dados ou meios físicos seguros, com acesso restrito apenas aos profissionais autorizados e qualificados necessários exclusivamente para o desempenho de suas funções.

O Vrde adotará os seguintes padrões de segurança para proteger os dados pessoais, além daqueles descritos nos outros itens desta política:

- Anonimização dos dados, sempre que necessário e possível;
- Restrição de acesso a bases de dados ou locais de armazenamento de dados pessoais somente a pessoas previamente autorizadas, comprometidas com o sigilo absoluto desses dados;
- Implementação de mecanismos de registro de acesso que permitam identificar o responsável pelo tratamento e acesso aos dados pessoais através de meios digitais;
- Manutenção de inventário indicando data, duração, identidade do colaborador ou responsável pelo acesso, e arquivamento dos dados pessoais com base nos registros de conexão e acesso aos sistemas;
- Em caso de transmissão de dados, assegurar que o procedimento seja realizado de forma segura, sem divulgação de dados pessoais que permitam a identificação de seus titulares.

VRDEBANK

# 08. Uso de Cookies em nossas plataformas

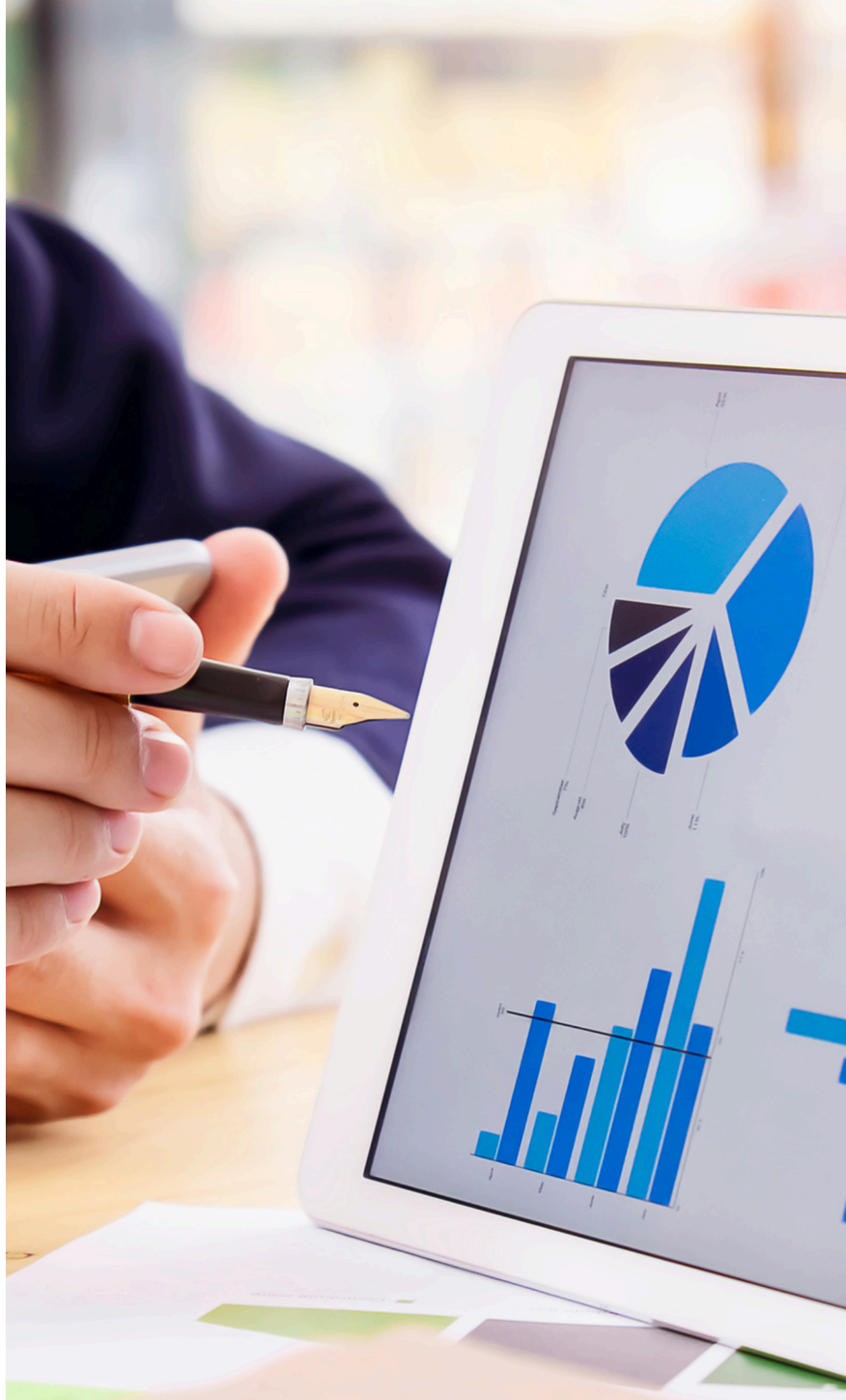
O Vrde utiliza cookies e outras tecnologias de identificação em nossas plataformas para permitir que você tenha uma navegação personalizada, garantindo assim mais eficiência no seu dia a dia como cliente Vrde.

Cookies são pequenos arquivos de texto criados quando você visita nosso site ou utiliza nosso aplicativo. Eles são amplamente usados para fazer com que os sites funcionem de maneira mais eficiente, além de fornecer informações úteis para melhorar a experiência do cliente.

Os cookies têm diversas finalidades, como:

1. lembrar as preferências e configurações do usuário;
2. determinar a popularidade de um conteúdo;
3. medir a eficácia de campanhas publicitárias;
4. analisar o tráfego do site;
5. entender os interesses das pessoas que interagem com nossos serviços.

VRDEBANK



# 08. Uso de Cookies em nossas plataformas

**Tipos de Cookies que usamos:**

- Cookies Necessários: Essenciais para o funcionamento do site e dos aplicativos. Eles permitem que você navegue e use suas funcionalidades, como acessar áreas seguras. Sem esses cookies, alguns serviços solicitados não podem ser fornecidos.

- Cookies de Desempenho: Coletam informações anônimas sobre a forma como os visitantes usam o site e o aplicativo. Esses cookies nos ajudam a entender como os visitantes interagem com o site, fornecendo informações sobre as áreas visitadas, tempo gasto e problemas encontrados, como mensagens de erro. Isso nos ajuda a melhorar a experiência do usuário.

- Cookies de Funcionalidade: Permitem que o site se lembre das escolhas que você faz (como seu nome de usuário, idioma ou região em que se encontra) e forneça recursos aprimorados e mais personalizados. Esses cookies também podem ser usados para lembrar alterações feitas no tamanho do texto, fontes e outras partes das páginas da web que você pode personalizar.

- Cookies de Publicidade e Marketing: Podem ser usados para fornecer anúncios mais relevantes para você e seus interesses. Eles também são usados para limitar o número de vezes que você vê um anúncio, além de ajudar a medir a eficácia das campanhas publicitárias. Sendo aceita a utilização desses cookies, os dados poderão ser compartilhados para fins de publicidade.

VRDEBANK

# 08. Uso de Cookies em nossas plataformas

**Gerenciamento de Cookies:**

- É possível controlar o uso de cookies através das configurações do navegador. A maioria dos navegadores permite o bloqueio e exclusão de cookies. Porém, é importante saber que ao fazer isso, partes do site podem não funcionar como esperado, o que prejudica a sua experiência conosco.
- Os cookies não essenciais são coletados apenas mediante consentimento do titular, conforme legislação de proteção de dados em vigor. Além disso, é possível gerenciar as preferências de cookies diretamente no site ou aplicativo, ajustando as configurações de consentimento de cookies.
- A política de cookies pode ser alterada a qualquer momento com base em mudanças legislativas, em decorrência de atualizações de ferramentas tecnológicas ou a critério do VRDE, porém sempre respeitando os direitos dos titulares e a transparência para sua tomada de decisão.


VRDEBANK

# 09. Compartilhamento de Dados Pessoais

O compartilhamento de dados pessoais coletados e tratados pelo VRDE é permitido em situações específicas, sempre garantindo os direitos dos titulares, quais sejam:

- Verificação de informações cadastrais do titular, bem como para fins de cobrança e segurança;
- Quando necessário para atividades comerciais, como propaganda, marketing e outras correlatas essenciais para a prestação de serviços e para melhorar a experiência do titular com os produtos e serviços oferecidos. Nesses casos, será firmado um acordo de confidencialidade com a empresa receptora dos dados para garantir o estrito sigilo das informações;
- Para proteção dos interesses da VRDE em casos de conflito, incluindo demandas judiciais;
- Em casos de transações e alterações societárias envolvendo a VRDE, quando a transferência dos dados for necessária para a continuidade dos serviços;
- Com outras instituições financeiras, quando necessário para processamento de transações ou outras atividades relacionadas à execução de contratos;
- Com bureaus de crédito, conforme previsto na legislação aplicável, incluindo o cumprimento da legislação do cadastro positivo em casos como negativação, entre outros;
- Para identificação, prevenção e investigação de possíveis infrações ou atos ilícitos, como fraude, lavagem de dinheiro e financiamento do terrorismo;
- Com órgãos reguladores, outras entidades públicas, instituições do sistema financeiro e terceiros, inclusive para cumprimento e execução de obrigações legais, regulatórias e contratuais, e para a proteção e exercício regular de direitos;
- Para cumprimento de requisições, solicitações e decisões de autoridades judiciais, administrativas ou arbitrais.

Em quaisquer das hipóteses, seus dados pessoais só serão compartilhados com terceiros para cumprir os objetivos descritos nesta política. O VRDE irá pseudonimizar seus dados sempre que possível antes de compartilhá-los, e pedirá que esses terceiros mantenham a confidencialidade e a segurança de suas informações.

# 10. Transferência Internacional de Dados

Para oferecer um serviço seguro, rápido e eficiente, utilizamos uma infraestrutura tecnológica robusta que inclui parceiros especializados em armazenamento de dados. Dessa forma, a base de dados do VRDE é armazenada em servidores de fornecedores especializados, que podem estar localizados no exterior.

Nesses casos de transferência internacional, o VRDE assegura o cumprimento integral da legislação brasileira. Seus Dados Pessoais somente serão enviados para países com um grau de proteção de dados reconhecido como adequado pela autoridade competente ou mediante a observância de todos os requisitos legais aplicáveis. Ressaltamos que nossa relação com esses fornecedores é formalizada por contratos que estabelecem obrigações de proteção de dados e segurança da informação compatíveis com a lei.

Esse tipo de infraestrutura e a contratação desses parceiros é essencial para garantir a disponibilidade e a proteção dos seus dados, permitindo que nossa equipe se concentre em oferecer a melhor experiência para você.

VRDEBANK

# 11. Política de “Mesa Limpa” e “Tela Limpa”

Esta política de Mesa Limpa e Tela Limpa é essencial para fortalecer a segurança da informação no Vrde, protegendo os dados confidenciais dos clientes e do próprio banco contra potenciais ameaças e violações. Cada colaborador é responsável por aplicar as práticas de “Mesa Limpa” e “Tela Limpa” em seu ambiente de trabalho diariamente através das seguintes diretrizes:

- Todos os colaboradores devem manter suas mesas organizadas e livres de documentos, papéis ou dispositivos que contenham informações sensíveis quando não estiverem presentes;
- Documentos físicos que contenham dados sensíveis devem ser guardados em armários seguros e trancados quando não estiverem em uso;
- Nenhum documento ou dispositivo eletrônico deve ser deixado em áreas acessíveis a pessoas que não possuem autorização para acessá-los ou sem supervisão adequada;
- Os colaboradores devem adotar a prática de bloquear as telas de computadores ou dispositivos móveis que contenham informações sensíveis, ao sair de perto deles, para evitar o acesso não autorizado a informações sensíveis;
- Todos os dispositivos móveis devem ser protegidos com senha, PIN ou biometria, e configurados para bloqueio automático após um curto período de inatividade;
- Ter cautela para que a tela do dispositivo não seja vista por pessoas que não possuem autorização para acessar os dados tratados no momento.

# 12. Papéis para o tratamento adequado e segurança de dados

**Dever de todos os colaboradores do Vrde e dos parceiros que possuem acesso ou precisam acessar dados pessoais:**

- Cumprir todas as normas, recomendações e orientações de segurança da informação contidas nesta política e em futuras comunicações oficiais do VRDE;
- Utilizar apenas dispositivos autorizados e seguros para acessar sistemas corporativos e dados sensíveis.
- Manter sistemas operacionais, aplicativos e antivírus atualizados para mitigar vulnerabilidades de segurança.
- Utilizar senhas fortes e únicas para cada conta, alterando-as regularmente.
- Sempre solicitar formalmente a autorização necessária para o tratamento, compartilhamento e eliminação de dados;
- Jamais acessar ou tentar acessar dados para os quais não tem permissão para tratar ou visualizar, sob pena de sanção administrativa;
- Nunca disponibilizar, permitir ou facilitar acesso a dados pessoais mantidos pelo VRDE para quaisquer pessoas não autorizadas ou competentes conforme as normas institucionais;
- Implementar a política de "mesa limpa" e “tela limpa” sempre que tratar dados pessoais;
- Todos os colaboradores devem utilizar exclusivamente serviços de armazenamento em nuvem autorizados pelo VRDE para armazenar e acessar documentos e dados corporativos.
- Utilizar apenas métodos e plataformas seguras e autorizadas pelo banco para o compartilhamento de informações;
- É estritamente proibido o download de arquivos ou documentos para dispositivos pessoais, incluindo computadores, tablets, smartphones ou qualquer outro dispositivo eletrônico não autorizado.
- Deve-se evitar fazer o download de arquivos em dispositivos de propriedade do VRDE, sendo preferível que o trabalho seja desempenhado com os arquivos em nuvem;
- Em caso de extravio (perda, furto ou roubo) de dispositivo contendo dados tratados pelo banco, é obrigatório informar imediatamente para que sejam adotadas as medidas adequadas de mitigação de riscos.

# 12. Papéis para o tratamento adequado e segurança de dados

**Incumbe aos titulares de dados (parceiros de negócios, colaboradores e Clientes) manter condutas responsáveis quanto ao uso dos seus dados para mitigar riscos de incidentes. São fortemente recomendadas as seguintes condutas:**

- Utilizar senhas robustas para acesso à conta bancária digital. As senhas devem ser complexas, contendo letras maiúsculas, minúsculas, números e caracteres especiais;
- Verificar regularmente as transações e atividades na conta bancária digital para identificar qualquer atividade suspeita ou não autorizada. Relatar imediatamente ao VRDE qualquer transação desconhecida;
- Manter o sistema operacional, navegadores e aplicativos sempre atualizados com as versões mais recentes para proteger contra vulnerabilidades de segurança;
- Evitar realizar transações financeiras ou acessar informações sensíveis utilizando redes Wi-Fi públicas não seguras. Optar por redes VPN (Rede Virtual Privada) para criptografar a conexão e proteger os dados transmitidos;
- Ser cauteloso ao clicar em links suspeitos em e-mails, mensagens de texto ou mídias sociais que possam redirecionar para sites falsos projetados para roubar informações de login (phishing). O VRDE jamais irá solicitar informações pessoais ou financeiras por meios não oficiais;
- Configurar alertas através do aplicativo do VRDE para receber notificações imediatas sobre atividades ou transações;
- Proteger dispositivos móveis com senhas, PINs ou biometria. Usar aplicativos de segurança para dispositivos móveis que ofereçam recursos como localização remota e limpeza de dados em caso de perda ou roubo;
- Manter-se atualizado sobre as melhores práticas de segurança da informação através de recursos educacionais fornecidos pelo VRDE ou outras fontes confiáveis. Compartilhar essas práticas com familiares e amigos para manterem-se sempre atentos a possíveis golpes;
- Em caso de suspeita de fraude ou comprometimento da conta bancária digital, entrar em contato imediato com o VRDE para bloquear a conta e relatar o incidente. Isso pode ajudar a minimizar danos e iniciar procedimentos de recuperação o mais rápido possível.

# 12. Papéis para o tratamento adequado e segurança de dados

**É papel de todos os envolvidos reportar ao encarregado de dados (DPO) do VRDE toda e qualquer:**

- Operação de Tratamento de dados pessoais sem base legal ou contrária a legislação vigente;
- Operação que seja realizada em desconformidade com a política de privacidade e proteção de dados do VRDE e das demais normas institucionais;
- Eliminação ou destruição de dados pessoais não autorizada pelo VRDE;
- Qualquer incidente de segurança que resulte na violação, comprometimento ou acesso não autorizado a dados pessoais deve ser imediatamente reportado ao DPO. Isso pode incluir incidentes como perda ou roubo de dispositivos contendo dados pessoais, acesso indevido a sistemas ou compartilhamento não autorizado de informações;
- Solicitações de acesso, retificação, exclusão ou portabilidade de dados pessoais por parte dos titulares dos dados devem ser encaminhadas ao DPO para garantir que sejam tratadas de acordo com os requisitos legais e regulatórios;
- Questões relacionadas ao consentimento para o processamento de dados pessoais, incluindo solicitações de revogação de consentimento, devem ser comunicadas ao DPO para assegurar que o tratamento dos dados esteja em conformidade com a legislação de proteção de dados;
- Relatar quaisquer incidentes de segurança cibernética ou violações de dados que possam afetar a segurança dos dados pessoais dos titulares, garantindo uma resposta rápida e eficaz para mitigar danos;
- Dúvidas, preocupações e sugestões de melhoria relacionadas às políticas e procedimentos de proteção de dados adotados pelo VRDE podem ser discutidas com o DPO para garantir a conformidade e a eficácia das medidas de segurança da informação.

# 13. Relação com Parceiros Comerciais e Fornecedores

A LGPD estabelece que a responsabilidade por danos patrimoniais, morais, individuais ou coletivos decorrentes de violações à legislação de proteção de dados pessoais é de todos os agentes da cadeia envolvidos no tratamento de dados pessoais.

Por este motivo, o Vrde não se exime de sua responsabilidade como também exige que todos os seus parceiros e fornecedores estejam preparados e em conformidade com a legislação para realizar o tratamento de dados pessoais, na medida do que lhes couber dada as especificidades de suas operações.

Portanto, todos os contratos firmados com terceiros terão cláusulas específicas que abordem a proteção de dados pessoais, delineando claramente os deveres e responsabilidades pertinentes ao assunto, e demonstrando o compromisso desses terceiros em cumprir com as leis de proteção de dados aplicáveis e a aderir ao programa de compliance do VRDE e a esta política de privacidade e proteção de dados.

Por fim, as cláusulas contratuais referentes a Privacidade e Proteção de Dados serão cuidadosamente revisadas e sujeitas à aprovação pelo Encarregado de Proteção de Dados (DPO) do VRDE e sua equipe técnica, em conformidade com o atual quadro normativo.

VRDEBANK

# 14. Eliminação dos Dados

Os dados tratados pelo VRDE poderão ser eliminados, seguindo a legislação e tomando as medidas técnicas que evitem sua recuperação por meios razoáveis ou garantindo sua anonimização, nos seguintes casos:

- Quando a finalidade para a qual o dado foi coletado for alcançada, ou quando o dado deixar de ser necessário ou pertinente para o alcance desta finalidade;
- Em caso de revogação do consentimento pelo titular, salvo quando houver obrigação legal ou regulatório para o seu armazenamento;
- Por determinação de autoridade competente para tal fim.

# 15. Treinamento

Todos os colaboradores do VRDE são compelidos a participar de treinamentos periódicos sobre privacidade e proteção de dados. Esses treinamentos têm como objetivo aumentar a conscientização e garantir o cumprimento das políticas de segurança da informação estabelecidas pela instituição. A participação nestes treinamentos é mandatória e constará nos registros de treinamento e desenvolvimento de cada indivíduo.

VRDEBANK

# 16. Monitoramento e Revisão

O VRDEBANK está comprometido em manter sua política de privacidade e proteção de dados sempre atualizada e em conformidade com as melhores práticas e regulamentações vigentes. Reconhecemos a importância de proteger os dados pessoais dos nossos clientes, colaboradores e parceiros comerciais, e trabalhamos para assegurar que todas as informações sejam tratadas com a devida segurança.

Para garantir a eficácia e a relevância contínua de nossas políticas, realizamos revisões regulares com base nas mudanças da legislação, nas tecnologias emergentes e nas práticas recomendadas. Nossos especialistas em segurança da informação e Compliance trabalham em conjunto para monitorar e adaptar nossas políticas de acordo com o arcabouço normativo atualizado.

As alterações nesta política poderão acontecer a qualquer tempo e, sempre que impactar nos direitos dos titulares, o VRDE empreenderá esforços para comunicar essas atualizações de forma transparente, inclusive, se necessário, solicitar novo consentimento a respeito de determinado tratamento.

Além disso, o programa de compliance do VRDE trabalha para assegurar que todas as diretrizes e normas estabelecidas sejam rigorosamente seguidas em todas as áreas da organização. Isso inclui a realização de auditorias internas, avaliações de risco, revisão constante dos processos internos relacionados à proteção de dados e treinamentos periódicos sobre o tema.

# 17. Encarregado de Proteção de Dados - DPO

O Encarregado pelo tratamento de dados pessoais (DPO) tem a responsabilidade de receber e analisar suas reclamações e comunicações, receber notificações da Autoridade Nacional de Proteção de Dados (ANPD), orientar os funcionários do VRDE sobre as melhores práticas de proteção de dados pessoais de forma que garanta o bom cumprimento desta política.

Nosso DPO pode ser acionado sempre que preciso através do e-mail dpo@vrdebank.com.

VRDEBANK

# Política

## Privacidade e Proteção de Dados

2025.2