POLÍTICA DE PRIVACIDADE – FREEMINDTRONIC SL

Website & Software – Versão e data do documento: V2.0 de 28/02/2025

ARTIGO 1 – INTRODUÇÃO

1.1. Identificação do Controlador de Dados

Esta Política de Privacidade é emitida pela **Freemindtronic SL,** uma sociedade de responsabilidade limitada registrada sob as leis do Principado de Andorra, com sede em:

Av. Co-Prince de Gaulle, 13, Edifício Valira, Rés-do-chão, AD700 Escaldes – Engordany, Andorra.

A Freemindtronic é responsável pelo processamento dos dados coletados ou processados por meio do uso de seu site oficial https://freemindtronic.com bem como de seus softwares, aplicativos, extensões e sistemas embarcados.

1.2. Campo de Aplicação

Esta Política de Privacidade se aplica a todos os serviços, softwares, aplicativos, extensões e sistemas embarcados desenvolvidos e operados pela Freemindtronic.

Não se aplica a sites, serviços ou plataformas de terceiros acessíveis através dos serviços da Freemindtronic. A Freemindtronic não é responsável pelas práticas de privacidade desses serviços de terceiros.

1.3. Engajamento: Zero Trust e Zero Knowledge

A Freemindtronic adere a uma estrutura estrita **de Zero Trust e Zero Knowledge**, garantindo que os dados do usuário não sejam acessados, armazenados ou compartilhados.

Todos os softwares, aplicativos, extensões e sistemas embarcados desenvolvidos pela Freemindtronic operam **sem um servidor remoto, um banco de dados centralizado, a criação de uma conta de usuário, identificação de usuário e transmissão de dados**.

Todos os recursos do Freemindtronic garantem que os dados do usuário não sejam armazenados ou transmitidos para servidores remotos. Todo o processamento é realizado exclusivamente localmente no dispositivo do usuário, sem interação com uma infraestrutura externa.

1.4. Conformidade com os regulamentos

- A Freemindtronic está em conformidade com os mais rígidos regulamentos internacionais de proteção de dados e segurança cibernética, incluindo:
- Regulamento Geral de Proteção de Dados (GDPR – Regulamento (UE) 2016/679)
- Regulamento Resiliência Operacional Digital (DORA – Regulamento (UE) 2022/2554)
- Diretiva NIS2 (Diretiva (UE) 2022/2555) relativa à cibersegurança das infraestruturas críticas
- Lei de Privacidade do Consumidor da Califórnia (SCCA – EUA, Cal. Civ. Code § 1798.100 et seq.)
- Lei Geral de Proteção de Dados (LGPD – Brésil, Lei nº 13.709/2018)
- Lei 15/2003 sobre a Proteção de Dados Pessoais em Andorra, alterada pela Lei Qualificada 29/2021
- Regulamento (UE) 2021/821, de 20 de maio de 2021, relativo ao controlo das exportações de produtos de dupla utilização
- Padrões ISO/IEC 27001 e melhores práticas de segurança do NIST (National Institute of Standards and Technology, EUA)

1.5. DefiniçõesNesta política, os seguintes termos são definidos da seguinte forma:

- **Dados pessoais** : qualquer informação relativa a uma pessoa singular identificada ou identificável, direta ou indiretamente, nomeadamente por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, um identificador por via eletrónica, ou a um ou mais elementos específicos da sua identidade física, fisiológica, genética, mental, económica, cultural ou social.
- **Dados sensíveis** : qualquer informação cuja divulgação não autorizada possa resultar em alto risco para os direitos e liberdades dos titulares dos dados. Isso inclui, mas não se limita a:
    - Identificadores exclusivos (nomes de usuário, senhas, códigos de autenticação).
    - Chaves de criptografia e autenticação.
    - Informações de pagamento e dados bancários.
    - Dados confidenciais de clientes e parceiros (estratégias comerciais, patentes, documentos protegidos por segredos comerciais).
    - Quaisquer dados pessoais que se enquadrem nas categorias especiais do GDPR (origem étnica, opiniões políticas, crenças religiosas, saúde, biometria, vida sexual).
- **Processamento** significa qualquer operação ou conjunto de operações realizadas sobre dados pessoais, por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou outra forma de disponibilização, alinhamento ou combinação, limitação, apagamento ou destruição.
- **Controlador de dados** : a pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, individualmente ou em conjunto com outros, determina as finalidades e os meios de processamento de dados pessoais.
- **Subcontratante** : a pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trata os dados pessoais em nome do responsável pelo tratamento.
- **Consentimento** : qualquer indicação livre, específica, informada e inequívoca da vontade do titular dos dados, pela qual este concorda, por declaração ou por ato positivo inequívoco, com o tratamento dos dados pessoais que lhe digam respeito.
- **Pseudonimização** : tratamento de dados pessoais de tal forma que já não possam ser atribuídos a uma pessoa singular específica sem informações adicionais, que devem ser mantidos separados e protegidos por medidas técnicas e organizativas adequadas.
- **Anonimização** : transformação irreversível dos dados pessoais de tal forma que não seja mais possível identificar direta ou indiretamente o titular dos dados.
- **Violação de Dados Pessoais** : Qualquer violação de segurança que resulte acidental ou ilegalmente na destruição, perda, alteração, divulgação não autorizada ou acesso a dados pessoais. Isso inclui acesso não autorizado a logins, senhas, chaves de criptografia ou outros dados confidenciais protegidos.

ARTIGO 2 – COLETA E PROCESSAMENTO DE DADOS

2.1. Falta de coleta sistemática de dados

A Freemindtronic não coleta, armazena, compartilha ou vende quaisquer dados pessoais ou técnicos dos usuários, exceto no caso de interação direta, incluindo:

- Um pedido através das plataformas oficiais.
- Uma solicitação de contato relacionada ao atendimento ao cliente ou a uma parceria oficial.

Os dados são tratados apenas no âmbito estrito da execução do contrato ou da relação comercial e nunca são utilizados para qualquer outra finalidade.

2.2. Dados que podem ser coletados

Se um usuário fornecer informações voluntariamente, apenas os dados estritamente necessários serão processados:

- Identidade (sobrenome, nome)
- Dados de contacto (e-mail, telefone, morada de faturação e entrega)
- Informações profissionais
- Conteúdo enviado voluntariamente

Os dados transacionais são utilizados exclusivamente para a gestão de encomendas e a sua entrega, sem transmissão a terceiros, exceto por obrigações legais (fiscais e contabilísticas).

2.2.1 – Dados armazenados localmente na extensão ou aplicativoAlguns aplicativos e extensões Freemindtronic podem usar localStorage ou a API de armazenamento na Web para armazenar temporariamente as configurações locais no dispositivo do usuário. Esses dados nunca são transmitidos para servidores remotos e só podem ser acessados dentro do software usado.

2.3. Armazenamento e segurança de dados

A Freemindtronic aplica os mais altos padrões de segurança, em conformidade com os regulamentos **GDPR, DORA, NIS2, ISO/IEC 27001 e NIST**.

- **Armazenamento offline seguro** : Os dados são mantidos em mídia criptografada que só pode ser acessada por meio de unidades flash USB seguras EviKey NFC e/ou mídia de armazenamento criptografada e/ou dados criptografados.
- **Zero Trust e Zero Knowledge** : Falta de servidores remotos e bancos de dados centralizados para armazenar e/ou gerenciar dados confidenciais para todos os produtos Freemindtronic.
- **Segurança aprimorada para comunicações confidenciais**: A troca de dados confidenciais é realizada exclusivamente por meio de ferramentas **DataShielder** ou um protocolo seguro definido pelo cliente.
- **Alternativa imposta, se necessário**: Se o atendimento ao cliente não garantir um nível de segurança suficiente, a Freemindtronic oferece **o DataShielder** como o único canal seguro.

2.4. Proteção de Dados Classificados e Ambientes Sensíveis

As soluções Freemindtronic identificadas como um produto civil e militar de uso duplo são projetadas para proteger informações críticas e incluem:

- **Isolamento físico e particionamento** : nenhum dado é armazenado em um servidor remoto.
- **Autenticação forte** : NFC HSM e criptografia de chave segmentada patenteada. O uso da criptografia assimétrica RSA-4096 permite que as chaves CBC AES-256 sejam compartilhadas com segurança entre dispositivos HSM NFC, inclusive remotamente, sem transmissão por infraestruturas centralizadas. Esse mecanismo elimina o risco de exfiltração de chaves e fornece proteção avançada para trocas criptografadas.
- **Criptografia de ponta a ponta** : AES-256 CBC, RSA-4096, PGP - Todos os sistemas de criptografia simétrica seguros são obtidos por meio de chaves segmentadas e sistemas de

controle de acesso patenteados e entregues internacionalmente. Essa arquitetura torna a criptografia resistente a ataques quânticos, garantindo a proteção de longo prazo de dados confidenciais.

- **Registro descentralizado** : caixa preta local acessível apenas em NFC por um administrador autorizado.
- **Testes de estresse e segurança cibernética proativa** : avaliações regulares contra ataques APT, espionagem industrial e ameaças cibernéticas avançadas.

Se uma extensão ou aplicativo Freemindtronic acessar arquivos locais em um dispositivo Windows ou Mac (por exemplo, para armazenar chaves de criptografia ou arquivos seguros), esses arquivos serão processados exclusivamente localmente e nunca poderão ser acessados por terceiros. O usuário mantém o controle total sobre seus dados e não é compartilhado com outros serviços.

2.5. Armazenamento, Exclusão e Retenção de Dados do Cliente

- Os dados fornecidos por meio de um **formulário de contato** são usados apenas para responder à solicitação e excluídos imediatamente após o processamento.
- Os dados dos clientes resultantes das transações são mantidos apenas pelo período legal necessário, de acordo com os regulamentos aplicáveis nas seguintes jurisdições:
    - **Andorra: Lei Qualificada 29/2021 – retenção de documentos fiscais por 5 anos**
    - **União Europeia: Artigo 6 da Diretiva de Proteção ao Consumidor 2011/83/UE – retenção de dados de transações por até 10 anos, dependendo dos requisitos contábeis locais**
    - **França: Artigo L123-22 do Código Comercial Francês – retenção obrigatória de documentos contábeis por 10 anos**
    - **EUA: Publicação 583 do IRS – retenção de dados de transação de 3 a 7 anos**
- **Nenhum dado bancário é armazenado** : as transações são processadas por meio **de provedores terceirizados seguros** (por exemplo, PayPal).

2.6. Transferências internacionais de dados

A Freemindtronic não transfere nenhum dado para fora do EEE, a menos que seja aplicada uma estrutura legal adequada (**Cláusulas Contratuais Padrão - SCCs**).

2.7. Procedimento de violação de dados

De acordo com os artigos 33.º e 34.º do **RGPD** e a **Lei Qualificada 29/2021**, a Freemindtronic aplica uma **resposta proativa** em caso de incidente:

- **Contenção imediata** e **análise de impacto**.
- **Notificação dentro de 72 horas** à Agência de Proteção de Dados de Andorra (APDA), se necessário.
- **Informar os usuários afetados** se um alto risco for identificado.
- **Auditoria pós-incidente** para fortalecer as medidas de proteção.

2.8. Ciber-resiliência e proteção contra catástrofes e ciberataques

A Freemindtronic garante **a integridade e disponibilidade** dos dados, mesmo em caso de avaria, roubo, desastre ou ataque cibernético massivo.

2.8.1. Criptografia e Backup Seguro

- **Criptografia avançada** : AES-256 CBC, AES-256 CBC PGP, BitLocker com chaves armazenadas **no NFC HSM PassCypher**.
- **Separação de chaves e dados**: as chaves **de descriptografia** nunca são armazenadas na mesma mídia que os dados. As chaves de criptografia AES-256 CBC são altamente seguras e compartilháveis via NFC HSM DataShielder, operando sem contato, sem servidor e sem banco de dados. Este mecanismo garante a transmissão segura das chaves, mesmo remotamente, eliminando qualquer risco de interceção por terceiros.
- **Backups criptografados e redundantes**: dados replicados **em várias mídias offline** e seguras.

2.8.2. Proteção aprimorada contra ataques cibernéticos

- **Ransomware e criptografia excessiva** : backups off-line criptografados e chaves fisicamente terceirizadas off-line evitam adulteração ou recuperação fraudulenta.
- **Ataques cibernéticos avançados (APT, Zero-Day, Espionagem):** A arquitetura Zero Trust e Zero Knowledge e **a separação de chaves físicas** evitam a exfiltração. A arquitetura de segurança da Freemindtronic, incorporando sistemas de criptografia segmentados patenteados e controle de acesso baseado em hardware, garante que nenhuma chave privada ou dados criptografados possam ser exfiltrados, mesmo sob restrição física ou lógica. A combinação de criptografia AES-256 CBC e RSA-4096 aumenta a resiliência a ataques avançados, incluindo aqueles assistidos por inteligência artificial.
- **Resiliência sem nuvem** : **sem dependência de servidores remotos**, eliminando o risco de ataques centralizados.

2.8.3. Resiliência a desastres físicos e perdas acidentais

Os protocolos da Freemindtronic garantem sempre o acesso aos dados encriptados com as suas chaves, mesmo em caso de:

- **Roubo ou perda** de mídia criptografada: sem **chaves terceirizadas**, os dados permanecem inutilizáveis.
- **Destruição acidental ou desastre natural**: backups duplicados garantem que os dados confidenciais sejam recuperados.
- **Isolamento geográfico de backups**: a **mídia criptografada** é mantida em vários locais seguros, evitando o comprometimento total.

2.9. Acordos de confidencialidade e confidencialidade das trocas comerciais

Todas as relações comerciais com a Freemindtronic envolvendo a troca de informações sensíveis ou confidenciais são rotineiramente cobertas por um **Acordo de Confidencialidade (NDA).**

- **Aplicação estrita** : Qualquer informação trocada no contexto de parcerias, colaborações técnicas ou discussões comerciais é protegida por cláusulas de confidencialidade juridicamente vinculativas. Todos os documentos confidenciais, criptografados ou não, trocados com clientes e parceiros são sistematicamente assinados digitalmente por meio da função incorporada no DataShielder HSM PGP. Essa assinatura digital garante a integridade e autenticidade dos documentos, garantindo que nenhuma corrupção ou alteração tenha sido feita após a emissão. Além disso, as comunicações por e-mail envolvendo informações

confidenciais são sempre protegidas via PGP, evitando interceptação ou adulteração de mensagens.

- **Escopo do NDA** : O NDA abrange **documentos, comunicações, intercâmbios técnicos, inovações, dados internos**, bem como qualquer informação confidencial transmitida pela Freemindtronic ou recebida de um parceiro.
- **Penalidades por violações** : Qualquer divulgação não autorizada de informações confidenciais está sujeita a **penalidades contratuais e legais** que podem incluir ações legais por violação de confidencialidade e segredos comerciais.
- **Prazo de Proteção** : As obrigações de confidencialidade permanecem vigentes **mesmo após o término da relação contratual**, de acordo com o prazo definido em cada contrato.

Esta cláusula reforça o compromisso da Freemindtronic em proteger todas as informações críticas trocadas no decorrer de seus negócios, garantindo uma estrutura legal rígida contra qualquer vazamento ou comprometimento.

ARTIGO 3 – USO DE SENSORES E ACESSO A DADOS DE LOCALIZAÇÃO

Alguns softwares, aplicativos ou extensões **Freemindtronic** podem exigir acesso aos sensores nos dispositivos dos usuários.

3.1 Esses sensores incluem:

- **GPS** (localização precisa)
- **Wi-Fi e redes móveis** (localização aproximada)
- **Bluetooth** (detecção local sem transmissão externa)
- **Dados biométricos** (impressão digital, reconhecimento facial)
- **Microfone e câmera** (somente com consentimento explícito)
- **Sensores ambientais** (acelerômetro, giroscópio, sensores de proximidade, brilho)
- **Módulos de segurança** (NFC, HSM, HSM, PGP)

3.2 Todos os dados gerados por esses sensores:

- **Permanecem exclusivamente no dispositivo do usuário** e não são transmitidos para um servidor remoto ou serviço de terceiros em nenhuma circunstância.
- **Não estão sujeitos a armazenamento externo ou remoto**.
- **Só são acessíveis com o consentimento explícito do usuário**, especialmente para sensores sensíveis, como microfone e câmera.
- **Pode ser gerenciado pelo usuário**, que pode alterar ou revogar as permissões concedidas a qualquer momento por meio das configurações do dispositivo.

Os sensores dos dispositivos (câmera, microfone, NFC, GPS, Wi-Fi, Bluetooth) são usados apenas localmente e nunca transmitem dados para servidores externos, terceiros ou outros serviços Freemindtronic. O usuário pode controlar e desabilitar esse acesso por meio das configurações do dispositivo.

3.4 Garantir que os Dados do Sensor não sejam usados para fins de rastreamento comportamental

O Freemindtronic garante que **os dados coletados por meio de sensores de dispositivos nunca sejam usados para rastreamento comportamental, publicidade direcionada ou perfil de usuário**.

O acesso aos sensores é estritamente limitado aos recursos essenciais do software e somente após a obtenção do consentimento explícito do usuário.

Nenhuma análise dos padrões de uso é realizada com base nesses dados, e eles não são armazenados ou repassados a terceiros.

ARTIGO 4 – CONFORMIDADE COM AS PLATAFORMAS DE DISTRIBUIÇÃO

Os softwares, aplicativos e extensões desenvolvidos pela **Freemindtronic** atendem aos requisitos das seguintes plataformas:

- **Google Play Console** (aplicativos Android)
- **Chrome Web Store** (extensões do navegador)
- **Complementos da Microsoft Store e do Edge** (aplicativos do Windows e extensões de navegador)
- **Apple macOS e iOS** (aplicativos distribuídos na App Store)

A Freemindtronic está empenhada em aderir às diretrizes **de segurança e privacidade** impostas por essas plataformas.

- **A arquitetura Zero Trust & Zero Knowledge é garantida** para que nenhum dado do usuário seja coletado, transmitido ou armazenado além do dispositivo do usuário.
- **Não há integração com serviços de terceiros** para mitigar os riscos associados ao rastreamento ou coleta de dados pessoais.
- **Os requisitos de cada plataforma são revisados regularmente** para garantir a conformidade contínua com as mudanças nos regulamentos aplicáveis.

SEÇÃO 5 – CLÁUSULA DE NÃO DISCRIMINAÇÃO (CONFORMIDADE COM A CCPA)

De acordo com as disposições da **Lei de Privacidade do Consumidor da Califórnia (CCPA), a Freemindtronic garante que os usuários não serão discriminados** no exercício de seus direitos em relação à proteção de dados pessoais.

Não serão aplicadas restrições ou limitações aos utilizadores que pretendam exercer os seus direitos, nomeadamente no que diz respeito:

- Acesso aos seus dados pessoais.
- Retificação de informações imprecisas ou incompletas.
- Exclusão de dados fornecidos voluntariamente.
- Opor-se ou restringir o processamento de seus dados.

A Freemindtronic compromete-se a não aplicar taxas adicionais, ou alterações no acesso a funcionalidades, em resposta a um pedido de exercício de direitos por parte de um utilizador.

Qualquer usuário que deseje fazer valer seus direitos pode entrar em contato diretamente com a Freemindtronic usando os detalhes de contato fornecidos nesta Política de Privacidade.

De acordo com a CCPA, o exercício dos direitos de proteção de dados pessoais (acesso, exclusão, oposição) não resultará em qualquer modificação, restrição ou degradação dos serviços oferecidos pela Freemindtronic.

ARTIGO 6.º – PROIBIÇÃO DE DEFINIÇÃO DE PERFIS E IMPRESSÕES DIGITAIS

6.1. Ausência de Definição de Perfis e Decisões Automatizadas

A Freemindtronic não realiza nenhum perfil, rastreamento comportamental ou tomada de decisão automatizada que afete os usuários.

- Nenhuma análise de atividade do usuário é executada.
- Nenhum algoritmo de inteligência artificial é usado para classificar os usuários.
- Nenhum mecanismo para personalizar serviços com base nos dados do usuário é implementado.

6.2. Ausência de impressões digitais

A impressão digital é uma técnica que envolve a coleta de informações específicas sobre o hardware ou software de um dispositivo, como endereço IP, sistema operacional, resolução da tela e outros parâmetros, a fim de criar uma impressão digital exclusiva do usuário. Ao contrário dos cookies, esse método é difícil de detectar e bloquear, o que representa grandes preocupações com a privacidade.

Em dezembro de 2024, o **Google anunciou que, a partir de 16 de fevereiro de 2025, permitiria que os anunciantes usassem impressões digitais** para rastreamento de usuários, revertendo sua política de 2019 que proibia a prática. A medida atraiu críticas de reguladores como **o Information Commissioner's Office (ICO) do Reino Unido,** que chamou a mudança de "irresponsável" devido à redução na escolha e no controle que os indivíduos têm sobre a coleta de suas informações.

Na **Freemindtronic**, estamos fortemente comprometidos em respeitar a privacidade de nossos usuários. Assim, **não usamos nenhuma forma de impressão digital** em nossos produtos ou serviços. **O Google anunciou em dezembro de 2024 que permitiria a coleta de impressões digitais para anunciantes a partir de 16 de fevereiro de 2025** (fonte oficial - https://blog.google/products/ads-commerce/privacy-sandbox-fingerprinting-policy-change).

A medida levantou preocupações dos reguladores, incluindo **a ICO do Reino Unido**. A Freemindtronic rejeita essas práticas e garante que **nenhum rastreamento, identificação de dispositivo ou perfil comportamental** seja implementado.

Todos os sistemas de TI da Freemindtronic são **completamente isolados e independentes** uns dos outros. **Nenhum dado do usuário é registrado, armazenado ou rastreado** por meio de uma operação exclusivamente local e offline. **O uso de soluções de criptografia de hardware e autenticação NFC HSM** garante que nenhuma impressão digital possa ser associada aos usuários, inclusive por meio do uso da tecnologia EviBITB da Freemindtronic.

A Freemindtronic implementa uma **estratégia avançada de segurança cibernética** para proteção contra ataques assistidos por IA, fraude de CEO e outros roubos de identidade.

- Os **e-mails usados para comunicação externa** são **endereços de sandbox e e-mails sem resposta** para **reduzir o risco de falsificação e phishing**.

- Qualquer abertura de anexo está sujeita a uma **política de controle rígida** para evitar **qualquer risco de arquivos maliciosos**.
- Cada **solicitação do cliente** é verificada sistematicamente por **um segundo canal de comunicação** para **confirmar sua autenticidade** (remoção proativa de dúvidas).

A Freemindtronic garante **que nunca coletará, analisará ou usará impressões digitais do dispositivo** por meio de métodos de identificação indireta (por exemplo, resolução da tela, modelo do dispositivo, idioma do navegador).

ARTIGO 7.º – CUMPRIMENTO DA REGULAMENTAÇÃO EM MATÉRIA DE DUPLA UTILIZAÇÃO

7.1. Regulamentos e Autorização de Exportação

A Freemindtronic aplica rigorosamente os regulamentos para o gerenciamento e exportação de tecnologias de segurança cibernética, inclusive para **produtos de criptografia classificados como civis e militares de uso duplo**.

Os produtos DataShielder NFC HSM receberam uma **autorização de importação para a França do Principado de Andorra**, validada em **7 de dezembro de 2024** através da empresa **AMG Pro**, de acordo com o **Decreto nº 2001-1192 de 13 de dezembro de 2001**, alterado pelo **Decreto nº 2024-95 de 8 de fevereiro de 2024**.

Esta autorização foi obtida após a apresentação do processo à **ANSSI**, que, de acordo com a sua missão de verificar o **cumprimento dos requisitos regulamentares**, não recusou nos prazos previstos pela legislação em vigor.

Desde **7 de fevereiro de 2025,** os produtos **DataShielder NFC HSM** também estão **autorizados para reexportação** da França para os Estados Membros da União Europeia, em conformidade com o **Regulamento (UE) 2021/821 de 20 de maio de 2021** sobre itens de uso duplo.

7.2. Textos de referência

Esta autorização é emitida de acordo com os seguintes textos:

- **Decreto n.º 2001-1192, de 13 de dezembro de 2001**, alterado pelo **Decreto de 8 de fevereiro de 2024**, relativo ao controlo da exportação e transferência de bens e tecnologias de dupla utilização.
- **Regulamento (UE) 2021/821, de 20 de maio de 2021**, que estabelece um regime de controlo das exportações de produtos de dupla utilização.

7.3. Compromisso de auditoria

A Freemindtronic está empenhada em garantir **auditorias regulares de conformidade** para garantir a **adesão contínua aos requisitos legais e regulamentares**. Estas auditorias internas são realizadas periodicamente de acordo com os requisitos regulamentares em vigor.

ARTIGO 8 – CERTIFICAÇÕES E AUDITORIAS

8.1. Nenhum requisito de certificação em nuvem

A Freemindtronic não requer certificações **SOC 2** ou **ISO 27001** específicas para infraestruturas em nuvem, pois **nenhum servidor remoto é usado** para processamento ou armazenamento de dados.

Os produtos são projetados com uma abordagem **100% isolada**, garantindo **o isolamento total dos dados do usuário** de qualquer infraestrutura de rede externa. Essa arquitetura justifica **a ausência de certas auditorias** normalmente aplicadas a sistemas conectados.

8.2. Auditoria de Segurança e Controle de Qualidade

Essa abordagem **é aplicada em toda a cadeia de valor**, desde o **design do produto** até a **fabricação**. Todas as auditorias realizadas visam garantir a **resiliência, inviolabilidade e vazamento de dados** dos sistemas da Freemindtronic.

Além das auditorias internas para garantir a conformidade do produto, a Freemindtronic aplica **controles aprimorados no gerenciamento de pagamentos** e **na proteção de transações financeiras**.

- O sistema de gestão contábil e financeira é isolado e nenhuma transação pode ser validada sem autenticação forte via DataShielder NFC HSM Auth e DataShielder MAuth, garantindo uma autenticação forte e eliminando o risco de fraude.
- O acesso a contas bancárias e sistemas de pagamento é estritamente limitado a acionistas autorizados, sem relação de subordinação, para limitar os riscos internos de fraude.

ARTIGO 9 – ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)

9.1. Nomeação do DPO

De acordo com os requisitos do **Regulamento Geral de Proteção de Dados (RGPD – Regulamento (UE) 2016/679)** e demais regulamentação aplicável, a Freemindtronic nomeou um **Encarregado de Proteção de Dados (DPO)** responsável por garantir a conformidade da empresa com a proteção de dados pessoais.

O **DPO da Freemindtronic** é:

- **Nome:** Jacques Gascuel
- **Cargo:** CEO e DPO da Freemindtronic SL
- **Contato:** dpo [at] freemindtronic.com

9.2. Missões do encarregado da proteção de dados

O DPO da Freemindtronic realiza várias missões essenciais, incluindo:

- Garantir que **o processamento de dados esteja em conformidade** com os regulamentos aplicáveis (**GDPR, CCPA, LGPD, etc.**).
- Informar e aconselhar a Freemindtronic sobre **as suas obrigações de proteção de dados**.
- Monitore a aplicação **das políticas de segurança e proteção de dados** implementadas.
- Responder às solicitações dos usuários sobre **seus direitos (acesso, retificação, exclusão, oposição, etc.)**.
- Estabelecer contato com **as autoridades de proteção de dados**, incluindo a **Agência de Proteção de Dados de Andorra** e as autoridades europeias ou internacionais relevantes.

9.3. Contato e Reclamações

Qualquer utilizador que pretenda obter informações sobre **a gestão dos seus dados pessoais** ou exercer os seus direitos pode contactar **o DPO da Freemindtronic** no seguinte endereço:

- **E-mail:** dpo [at] freemindtronic.com

- **Endereço para correspondência:**
  Freemindtronic SLAv. Co-Príncipe de Gaulle, 13, Edifício Valira, Rés-do-chão, AD700 Escaldes – Engordany, Andorra

Se não for dada resposta no prazo de **30 dias**, o utilizador pode remeter o assunto diretamente **para a Agência de Proteção de Dados de Andorra (APDA)** por **incumprimento da obrigação legal de resposta no prazo de 30 dias**.

ARTIGO 10.º – REQUISITOS ESPECÍFICOS APLICÁVEIS ÀS PLATAFORMAS DE DISTRIBUIÇÃO

10.1. Google Play Console (Android)

Os aplicativos Freemindtronic não coletam, armazenam ou transmitem nenhum dado pessoal. Algumas permissões do Android (por exemplo, NFC, armazenamento, câmera) são usadas apenas para ativar a funcionalidade do produto e não são exploradas para fins de terceiros. Nenhum dado é compartilhado com terceiros e todas as operações são realizadas localmente no dispositivo do usuário, de acordo com as políticas de privacidade do Google Play.

10.1.1. Conformidade com as políticas do Google Play em relação a dados confidenciais e permissõesOs aplicativos Freemindtronic que exigem acesso a recursos confidenciais do Android (NFC, armazenamento, câmera, microfone, GPS, SMS, RCS, MMS) atendem aos seguintes requisitos:

- **Consentimento expresso** : nenhuma permissão é habilitada por padrão. O usuário deve habilitá-los manualmente por meio das configurações do dispositivo.
- **Uso contínuo** : O acesso a esses recursos é **estritamente limitado** às necessidades essenciais do aplicativo, e os dados gerados permanecem **exclusivamente no dispositivo**.
- **Sem abuso de permissões** : Freemindtronic nunca pede acesso a recursos supérfluos e respeita a política de transparência do Google Play.

10.1.2. Proteção de dados e armazenamento localTodos os dados permanecem estritamente armazenados no dispositivo do usuário e **só podem ser acessados pelo próprio aplicativo**. Nenhum dado do usuário é armazenado em **servidores externos** ou compartilhado com **terceiros**.

10.2 – Chrome Web Store (extensões do Chrome)

As extensões Freemindtronic não coletam ou compartilham nenhum dado do usuário. Eles podem usar localStorage para armazenar temporariamente informações locais necessárias para que a extensão funcione corretamente.

Nenhum rastreamento oculto, nenhuma transmissão de dados a terceiros e nenhum acesso injustificado a cookies ou histórico de navegação são realizados.

10.2.1 Usando o armazenamento localAs extensões Freemindtronic usam exclusivamente a API localStorage e Web Storage para armazenar temporariamente as configurações necessárias para seu funcionamento adequado.
Esses dados:

- **Nunca são transmitidos para servidores remotos.**
- **São acessíveis apenas ao usuário e somente no contexto da extensão.**
- **As configurações salvas localmente via localStorage e Web Storage não contêm dados pessoais ou confidenciais.**

- **Os usuários podem limpar manualmente os dados locais salvos por meio de uma opção "Excluir dados" incorporada à extensão.**

10.3. Complementos da Microsoft Store e Edge (Windows)

Os aplicativos e extensões Freemindtronic estão em conformidade com os padrões de privacidade da Microsoft.

Se um aplicativo acessar arquivos locais (por exemplo, armazenamento seguro de chaves de criptografia), esses arquivos permanecerão isolados e nunca serão compartilhados com serviços de terceiros.

A Freemindtronic garante que não haverá impressão digital ou rastreamento oculto, de acordo com as políticas da Microsoft Store.

10.3.1. Proteção de Acesso a Arquivos Locais (Windows)
Alguns aplicativos Freemindtronic podem exigir acesso a arquivos locais para **criptografar, proteger ou autenticar dados confidenciais**.
Esses arquivos:

- **Nunca são encaminhados para um servidor remoto.**
- **Permanecem exclusivamente armazenados e processados no dispositivo do usuário.**
- **Só podem ser acessados por aplicativos instalados localmente com o consentimento do usuário.**

10.4. Apple App Store (macOS e iOS)

Os aplicativos Freemindtronic não rastreiam usuários, coletam dados para perfis de publicidade ou transmitem informações para fora do dispositivo.

Se um aplicativo acessar sensores iOS/macOS (por exemplo, NFC, microfone, GPS), esse uso será estritamente limitado a recursos essenciais e controláveis pelo usuário.

Se forem usadas APIs de terceiros (por exemplo, pagamento via Apple Pay), seu impacto nos dados do usuário estará em conformidade com os requisitos da Apple e será totalmente transparente para o usuário.

10.4.1. Conformidade com a Política de Transparência de Rastreamento de Aplicativos (ATT) A Freemindtronic
garante **que não usa IDs de publicidade** ou **ferramentas de rastreamento de usuários** para fins de marketing ou publicidade.
De acordo com as diretrizes da Apple:

- **Nenhum dado do usuário é coletado para criação de perfil ou direcionamento de publicidade.**
- **Não há integração com serviços de publicidade ou análise de terceiros.**
- **Não é permitido o uso do ID Apple (IDFA) para rastrear a atividade do usuário em outros apps.**
- **O Freemindtronic não coleta ou compartilha nenhum dado de localização em segundo plano ou sem o consentimento explícito do usuário.**

- **Os aplicativos não transmitem nenhum dado do dispositivo, a menos que o usuário execute voluntariamente uma ação que exija troca de dados.**

ARTIGO 11 – CONFORMIDADE COM A LEGISLAÇÃO DE PROTEÇÃO DE DADOS DE ANDORRA

11.1. Aplicação das leis andorranas

A Freemindtronic, como empresa registrada no **Principado de Andorra**, está sujeita aos regulamentos locais de **proteção de dados**, incluindo:

- **Lei Qualificada 15/2003, de 18 de dezembro** , sobre a Proteção de Dados Pessoais
- **Lei Qualificada 29/2021 de 28 de outubro de 2021**, que alinha Andorra com os princípios do **Regulamento Geral de Proteção de Dados (RGPD – Regulamento (UE) 2016/679)**

Essas leis garantem uma estrutura de **proteção de dados** equivalente aos padrões europeus, reconhecidos **como adequados** pela União Europeia de acordo com **o Artigo 45 do GDPR.**

Além dos regulamentos atuais, a **Freemindtronic implementa medidas físicas e de software avançadas para garantir a proteção absoluta dos dados**. Isso inclui **criptografia completa de mídia digital, autenticação multifator NFC HSM e isolamento físico de infraestruturas de TI**. Estas medidas asseguram **o cumprimento integral dos artigos 10.º e 45.º do RGPD**, garantindo uma proteção de dados equivalente às mais rigorosas normas europeias.

ARTIGO 12 – PRINCÍPIOS DE CONFORMIDADE E SEGURANÇA DE DADOS

12.1. Privacidade desde a conceção

A Freemindtronic integra **a proteção de dados** no **design de seu software e serviços**, de acordo com os princípios de **privacidade por design e privacidade por padrão**.

12.2. Sem armazenamento de dados

De acordo com **a abordagem Zero Trust & Zero Knowledge**, a **Freemindtronic não armazena ou processa quaisquer dados pessoais**, exceto no caso de fornecimento voluntário pelo utilizador (por exemplo, formulário de contacto, suporte técnico).

12.3. Adoção de medidas de segurança reforçadas

A Freemindtronic implementa medidas **de segurança avançadas** para garantir a **proteção de dados** e evitar violações, incluindo:

- **Criptografe sistematicamente** as comunicações e transações do usuário por meio de seus sistemas patenteados de criptografia de chave segmentada
- **Falta de** identificadores exclusivos que possam ser usados para rastrear a atividade do usuário
- **Auditabilidade interna regular** para garantir a conformidade com os regulamentos atuais

Estas medidas estão de acordo com **o artigo 10.º da Lei Qualificada 29/2021** sobre a Proteção de Dados Pessoais em Andorra.

A Freemindtronic aplica uma estratégia abrangente de segurança cibernética que garante a proteção dos dados mesmo em caso de intrusão física nas instalações:

Todos os sistemas de computador (fixos, móveis, servidores e dispositivos de armazenamento) são totalmente criptografados com chaves de ≥256 bits.

Todos os sites conectados online ou em uma rede local usam PassCypher NFC HSM e PassCypher HSM PGP com TOTP/HOTP e/ou DataShielder NFC HSM e DataShielder HSM PGP Cyber Defense.

Nenhuma chave de criptografia é armazenada ou visível nas ferramentas de produção.

Mídias sensíveis (pen drives, discos rígidos) são armazenadas em um cofre resistente a incêndios e invasões.

Qualquer extração de dados confidenciais é impossível, mesmo em caso de roubo físico de servidores ou exfiltração ilícita de arquivos.

Essas medidas garantem que, mesmo no caso de uma intrusão nas instalações da Freemindtronic, nenhum dado possa ser explorado, mesmo no caso de uma intrusão ilegal bem-sucedida.

12.4. Compromisso com a segurança contínua

A Freemindtronic coloca **a proteção de dados** no centro de suas atividades e se compromete a:

- **Melhorar continuamente suas medidas de segurança** , acompanhando a evolução das ameaças e regulamentações.
- **Adaptar seus protocolos de proteção** para garantir um nível de segurança alinhado com os novos avanços tecnológicos e as melhores práticas de segurança cibernética.
- **Monitore constantemente** as ameaças cibernéticas, incluindo aquelas assistidas por inteligência artificial (IA), para antecipar possíveis tentativas de intrusão e fortalecer as defesas de acordo.

12.4.1 Proteção Estratégica: A Freemindtronic não divulga publicamente todos os detalhes técnicos de seus mecanismos de segurança para não facilitar uma análise por um invasor ou inteligência artificial buscando identificar uma possível vulnerabilidade. No entanto, todas as medidas implementadas cumprem os **padrões mais rigorosos** em termos de segurança cibernética e proteção de dados.

12.5. Segurança operacional e proteção de dados sensíveis

A Freemindtronic aplica um modelo de segurança rigoroso que garante **a máxima proteção contra os riscos de espionagem interna e externa**.

12.5.1 Isolamento de sistemas de computador

- Não são permitidas conexões de rede entre sistemas internos e nenhum compartilhamento de arquivos ou impressoras.
- Cada sistema é completamente independente, evitando vulnerabilidades relacionadas a conexões externas.

12.5.2 Transferências seguras de dados confidenciais

- Todas as transferências de arquivos confidenciais são realizadas **exclusivamente** por meio das unidades flash USB seguras **EviKey NFC** da Freemindtronic.
- Essas chaves possuem **travamento automático** quando não estão em uso, impedindo o acesso não autorizado.
- Um **registro de rastreabilidade** é integrado à caixa preta das chaves EviKey NFC, permitindo que cada desbloqueio e sua geolocalização sejam verificados.

12.5.3 Isolamento físico e proteção de ferramentas de produção

- Equipamentos e ferramentas de produção sensíveis **nunca são conectados à Internet** e são estritamente isolados após o uso.
- Após o uso, essas ferramentas são **mantidas em um cofre especial resistente** ao fogo e à intrusão física.

12.5.4 Gerando e protegendo chaves de autenticação

- As chaves de autenticação antifalsificação que também servem como **chaves segmentadas** são geradas **aleatoriamente** pelas ferramentas de produção.
- Essas chaves **não são exibidas nem salvas** nas ferramentas de produção, garantindo a ausência de qualquer vestígio utilizável.

12.5.5 Controle de Acesso Rigoroso e Mitigação de Riscos Internos

- Apenas **duas pessoas autorizadas**, que também são **acionistas da empresa**, estão autorizadas a usar as ferramentas de produção.
- Esta restrição visa **minimizar os riscos associados às relações de subordinação** e garantir o controlo total sobre o acesso a infraestruturas sensíveis.

12.6. Controle de Acesso Rigoroso e Mitigação de Riscos Internos

12.6.1 Segurança de acesso e criptografia sistemática

A Freemindtronic aplica protocolos avançados de autenticação e criptografia para garantir que todo o acesso digital e mídia estejam protegidos contra qualquer intrusão ou tentativa de roubo.

12.6.1.1 Proteção de acesso a sites e redesTodos os sistemas de rede online e local usam apenas as seguintes tecnologias de autenticação forte:

- PassCypher NFC HSM e/ou PassCypher HSM PGP, intégrant des protocoles TOTP (Time-Based One-Time Password) et HOTP (HMAC-Based One-Time Password).
- DataShielder NFC HSM e/ou DataShielder HSM PGP na versão Cyber Defense, combinando autenticação forte e criptografia de acesso avançada.
- Emuladores de teclado USB Bluetooth para proteger a entrada de dados confidenciais, eliminando qualquer risco de keylogging.

12.6.1.2 Criptografia de dados e mídia de armazenamentoTodos os sistemas de computador (fixos, móveis) e dispositivos de armazenamento que contêm dados confidenciais são criptografados com chaves de criptografia iguais ou superiores a 256 bits.

- Discos rígidos internos e externos totalmente criptografados.
- Dispositivos móveis de armazenamento e backup protegidos por criptografia de hardware e/ou software.

12.6.1.3 Resiliência a intrusões físicas e digitaisTudo é projetado para garantir que, em caso de intrusão nas instalações da Freemindtronic, roubo de mídia digital ou extração ilícita de dados confidenciais, nenhum dado seja utilizável ou fisicamente acessível.

- Chaves de criptografia seguras em dispositivos NFC HSM, impedindo o acesso não autorizado.
- Bloqueio automático de chaves ou travamento em caso de tentativa de comprometimento com rastreabilidade de caixa preta.

12.6.1.4 Integração de Produtos usando a Tecnologia EviKey NFC

Os produtos da Freemindtronic que incorporam a tecnologia **EviKey NFC** usam exclusivamente o aplicativo **Fullkey Plus** para seu gerenciamento e segurança. Essa tecnologia também está integrada às seguintes soluções de segurança cibernética:

- **PassCypher NFC HSM Mestre**
- **DataShielder NFC HSM Mestre & Defesa**

A integração do EviKey NFC nessas soluções fornece controle de acesso avançado à mídia de armazenamento e inclui os seguintes recursos:

- **Travamento automático quando inativo**
- **Gerenciamento seguro de chaves**
- **Acesse a rastreabilidade por meio de uma caixa preta**, acessível apenas sem contato por meio de **um telefone Android NFC**, graças ao aplicativo **Fullkey Plus**, **PassCypher NFC HSM** ou **DataShielder NFC HSM**.

A Freemindtronic não corre riscos no que toca à segurança e não se deixa surpreender: aqui, **o sapateiro certamente não é o pior calçado** ! 😉

A Freemindtronic implementa **partições de segurança estanques**, evitando qualquer forma de espionagem, seja **interna ou externa**, e garantindo a **máxima** proteção de ativos digitais e dados críticos.

12.6.1.4 – Proteção contra IA e ataques avançados :

A Freemindtronic implementa tecnologias e protocolos específicos para proteção contra ataques assistidos por IA, incluindo deepfakes e manipulações de áudio/vídeo destinadas a comprometer a identidade digital de executivos e usuários. Essas medidas incluem verificação aprimorada de comunicações e análise multifatorial de comércio sensível.

12.7 – Gerenciamento de violação de dados :

No caso de um comprometimento de hardware ou tentativa de violação de segurança que afete a infraestrutura da Freemindtronic, os procedimentos de resposta a incidentes são realizados de forma proativa, independentemente da ausência de um sistema de detecção automatizado.

A Freemindtronic reconhece que não é realista garantir proteção absoluta contra um determinado invasor, mesmo com as melhores medidas de segurança do mundo. É por isso que a abordagem adotada assenta numa estratégia **proativa e preventiva**, integrando inovações patenteadas internacionalmente desenvolvidas para antecipar novas formas de espionagem, nomeadamente as assistidas por **inteligência artificial**.

As soluções de segurança cibernética da Freemindtronic são projetadas para impedir que os dados sejam explorados, mesmo em caso de acesso físico ou digital não autorizado. Essa abordagem é baseada em mecanismos avançados, incluindo autobloqueio de hardware, criptografia de chave segmentada, isolamento de infraestrutura e uso exclusivo de mídia segura, como EviKey NFC, PassCypher NFC HSM e DataShielder NFC HSM.

No caso de um incidente de segurança envolver um cliente ou parceiro, a Freemindtronic compromete-se a **informá-lo o mais rápido possível**, de acordo com os requisitos dos regulamentos de proteção de dados aplicáveis.

ARTIGO 13.º – DIREITOS DOS UTILIZADORES AO ABRIGO DA LEGISLAÇÃO DE ANDORRA

De acordo com **os artigos 16.º a 21.º da Lei 29/2021**, os utilizadores têm os seguintes direitos, alinhados com o **RGPD e a legislação andorrana** :

- **Direito de acesso** : Para verificar quais informações foram fornecidas voluntariamente e processadas.
- **Direito de retificação** : Para corrigir quaisquer dados imprecisos ou incompletos.
- **Direito de oposição** : Contestar o uso de seus dados.
- **Direito ao Apagamento (Direito ao Esquecimento):** Exigir o apagamento definitivo dos seus dados.
- **Direito à Portabilidade** : Receber os seus dados em formato legível (nova obrigação reforçada pela Lei 29/2021).
- **Direito à Restrição de Processamento** : Restringir o processamento de certas informações.

13.1. Tempo de processamento para solicitações

A Freemindtronic garante que qualquer pedido de exercício de direitos será **processado no prazo máximo de 30 dias**, salvo em circunstâncias excecionais que exijam uma **prorrogação justificada até 60 dias**.

Os pedidos podem ser enviados por e-mail para:
contacto [at] freemindtronic.com ou **dpo [at] freemindtronic.com**

ARTIGO 14.º – RECURSO EM CASO DE LITÍGIO

Se um usuário acreditar que **seus direitos não foram respeitados**, ele pode registrar uma reclamação junto à **Agência de Proteção de Dados de Andorra (APDA),** a **autoridade supervisora competente em Andorra**.

14.1. Procedimento de reclamações

De acordo com **o artigo 25.º da Lei 29/2021**, qualquer pessoa que considere que o tratamento dos seus dados foi realizado em **violação da legislação aplicável** pode:

- **Encaminhe o assunto para a Agência de Proteção de Dados de Andorra (APDA)** para uma investigação administrativa.
  Contato APDA : https://www.apda.ad
- **Interpor recurso para os tribunais competentes de Andorra** para obter a reparação dos danos sofridos.

A Freemindtronic está empenhada **em cooperar plenamente** com as autoridades de proteção de dados em caso de investigação.

ARTIGO 15 – ALTERAÇÕES À POLÍTICA DE PRIVACIDADE

15.1. Compromisso de atualização

A Freemindtronic compromete-se a atualizar esta política em caso de alterações legislativas ou regulamentares que afetem a proteção de dados. Quaisquer alterações serão publicadas explicitamente no site oficial do Freemindtronic.

15.2. Frequência e transparência das atualizações

O Freemindtronic lança regularmente atualizações para seu software, aplicativos e extensões. Uma página de atualizações dedicada é mantida, detalhando explicitamente:

- **As mudanças feitas,**
- **Melhorias de segurança,**
- **Quaisquer vulnerabilidades identificadas e corrigidas.**

O histórico completo de versões do software, aplicativos e extensões Freemindtronic pode ser encontrado aqui: Freemindtronic Histórico de versões

15.3. Notificação de Usuários

Os usuários que desejam ser notificados sobre atualizações por e-mail devem fazer uma solicitação expressa, fornecendo seu endereço de e-mail para Freemindtronic.

15.4. Informações em caso de alterações nas funcionalidades

Em caso de alterações nas funcionalidades que envolvam o processamento de dados, a Freemindtronic compromete-se a informar os utilizadores:

- **Por notificação no site oficial,**
- **Através dos aplicativos em questão.**

ARTIGO 16 – DADOS DE CONTATO

Freemindtronic SL
E-mail: **contato [at] freemindtronic.com**
Telefone: **+376 804 500Politique des cookies:** https://freemindtronic.com/cookie-policy/

Fim do documento