POLITIQUE DE CONFIDENTIALITÉ – FREEMINDTRONIC SL

Site Internet & Logiciels – Version et date du document : V2.0 du 28/02/2025

ARTICLE 1 – INTRODUCTION

1.1. Identification du Responsable du Traitement

Cette Politique de Confidentialité est émise par **Freemindtronic SL**, une société à responsabilité limitée enregistrée sous les lois de la Principauté d'Andorre, ayant son siège social à :

Av. Co-Prince de Gaulle, 13, Valira Building, Rez-de-chaussée, AD700 Escaldes – Engordany, Andorre.

Freemindtronic est responsable du traitement des données collectées ou traitées via l'utilisation de son site officiel https://freemindtronic.com ainsi que ses logiciels, applications, extensions et systèmes embarqués.

1.2. Champ d'Application

Cette Politique de Confidentialité s'applique à tous les services, logiciels, applications, extensions et systèmes embarqués développés et exploités par Freemindtronic.

Elle ne s'applique pas aux sites web, services ou plateformes tiers accessibles via les services de Freemindtronic. Freemindtronic décline toute responsabilité quant aux pratiques de confidentialité de ces services tiers.

1.3. Engagement Zero Trust & Zero Knowledge

Freemindtronic adhère à un cadre strict **Zero Trust & Zero Knowledge**, garantissant l'absence totale d'accès, de stockage ou de partage des données des utilisateurs.

Tous les logiciels, applications, extensions et systèmes embarqués développés par Freemindtronic fonctionnent **sans serveur distant, sans base de données centralisée, sans création de compte utilisateur, sans identification de l'utilisateur et sans transmission de données**.

1.4. Conformité aux Réglementations

Freemindtronic respecte les réglementations internationales les plus strictes en matière de protection des données et de cybersécurité, notamment :

- Règlement Général sur la Protection des Données (RGPD – Règlement (UE) 2016/679)
- Digital Operational Resilience Act (DORA – Règlement (UE) 2022/2554)
- California Consumer Privacy Act (CCPA – États-Unis)
- Lei Geral de Proteção de Dados (LGPD – Brésil)
- Loi 15/2003 sur la Protection des Données Personnelles en Andorre
- Réglementations applicables aux solutions de cybersécurité et de résilience numérique
- Normes ISO/IEC 27001 et bonnes pratiques de sécurité du NIST

1.5. Définitions

Dans la présente politique, les termes suivants sont définis comme suit :

- **Données personnelles** : toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

- **Données sensibles** : toute information dont la divulgation non autorisée pourrait entraîner un risque élevé pour les droits et libertés des personnes concernées. Cela inclut, mais ne se limite pas à :
    - Les identifiants uniques (noms d'utilisateur, mots de passe, codes d'authentification).
    - Les clés de chiffrement et d'authentification.
    - Les informations de paiement et données bancaires.
    - Les données confidentielles des clients et partenaires (stratégies commerciales, brevets, documents protégés par le secret des affaires).
    - Toute donnée personnelle entrant dans les catégories spéciales du RGPD (origine ethnique, opinions politiques, convictions religieuses, santé, biométrie, vie sexuelle).
- **Traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
- **Responsable du traitement** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.
- **Sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles pour le compte du responsable du traitement.
- **Consentement** : toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données personnelles la concernant fassent l'objet d'un traitement.
- **Pseudonymisation** : traitement des données personnelles de manière à ce qu'elles ne puissent plus être attribuées à une personne physique spécifique sans information supplémentaire, qui doit être conservée séparément et protégée par des mesures techniques et organisationnelles appropriées.
- **Anonymisation** : transformation irréversible des données personnelles de telle sorte qu'il n'est plus possible d'identifier directement ou indirectement la personne concernée.
- **Violation de données personnelles** : toute violation de sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès à des données personnelles. Cela inclut les accès non autorisés aux identifiants, mots de passe, clés de chiffrement, ou autres données sensibles protégées.

ARTICLE 2 – COLLECTE ET TRAITEMENT DES DONNÉES

2.1. Absence de Collecte Systématique des Données

Freemindtronic ne collecte, ne stocke, ne partage ni ne vend aucune donnée personnelle ou technique des utilisateurs, sauf en cas d'interaction directe, notamment pour :

- Une commande via les plateformes officielles.
- Une demande de contact liée au service client ou à un partenariat officiel.

Les données sont uniquement traitées dans le cadre strict de l'exécution du contrat ou de la relation commerciale et ne sont jamais utilisées à d'autres fins.

2.2. Données Susceptibles d'Être Collectées

Si un utilisateur fournit volontairement des informations, seules les données strictement nécessaires sont traitées :

- Identité (nom, prénom)
- Coordonnées (email, téléphone, adresse de facturation et livraison)
- Informations professionnelles
- Contenu soumis volontairement

Les données transactionnelles sont utilisées exclusivement pour la gestion des commandes et leur livraison, sans transmission à des tiers hors obligations légales (fiscales et comptables).

2.3. Stockage et Sécurisation des Données

Freemindtronic applique les standards de sécurité les plus stricts, conformes aux réglementations **RGPD, DORA, NIS2, ISO/IEC 27001 et NIST**.

- **Stockage hors ligne sécurisé** : Les données sont conservées sur des supports chiffrés accessibles uniquement via des clés USB sécurisé EviKey NFC et/ou support de stockage chiffré et/ou données chiffrées.
- **Zero Trust & Zero Knowledge** : Absence de serveurs distants et de bases de données centralisées pour stocker et/ou gérer des données sensibles pour tous les produits de Freemindtronic.
- **Sécurité renforcée des communications sensible** : L'échange de données sensibles est exclusivement réalisé via les outils **DataShielder** ou un protocole sécurisé défini par le client.
- **Alternative imposée si besoin** : Si le service du client ne garantit pas un niveau de sécurité suffisant, Freemindtronic propose **DataShielder** comme unique canal sécurisé.

2.4. Protection des Données Classifiées et Environnements Sensibles

Les solutions Freemindtronic identifie comme produit double usage civil et militaire sont conçues pour protéger les informations critiques et incluent :

- **Isolation physique et cloisonnement** : Aucune donnée n'est stockée sur un serveur distant.
- **Authentification forte** : NFC HSM et chiffrement à clés segmentées breveté. L'utilisation du chiffrement asymétrique RSA-4096 permet de partager en toute sécurité les clés AES-256 CBC entre dispositifs NFC HSM, y compris à distance, sans transmission via des infrastructures centralisées. Ce mécanisme élimine le risque d'exfiltration des clés et garantit une protection avancée des échanges chiffrés.
- **Chiffrement de bout en bout** : AES-256 CBC, RSA-4096, PGP - Tous les systèmes de chiffrement symétrique sécurisé sont réalisés via des clés segmentées et des systèmes de contrôle d'accès brevetés, délivrés à l'international. Cette architecture rend le chiffrement résistant aux attaques quantiques, garantissant une protection durable des données sensibles.
- **Journalisation décentralisée** : Boîte noire locale accessible uniquement en NFC par un administrateur autorisé.
- **Tests de résistance et cybersécurité proactive** : Évaluations régulières contre les attaques APT, espionnage industriel et menaces cybernétiques avancées.

2.5. Stockage, Suppression et Conservation des Données Clients

- Les données fournies via un **formulaire de contact** sont utilisées uniquement pour répondre à la demande et supprimées immédiatement après traitement.
- Les **données clients issus des transactions** sont conservées uniquement pour la durée légale nécessaire (fiscale et comptable).
- **Aucune donnée bancaire n'est stockée** : Les transactions sont traitées via des **prestataires tiers sécurisés** (ex. PayPal).

2.6. Transferts Internationaux de Données

Freemindtronic ne transfère aucune donnée en dehors de l'EEE, sauf si un cadre juridique adéquat est appliqué (**Clauses Contractuelles Types - CCT**).

2.7. Procédure en Cas de Violation de Données

Conformément aux articles 33 et 34 du **RGPD** et à la **Loi Qualifiée 29/2021**, Freemindtronic applique une **réponse proactive** en cas d'incident :

- **Confinement immédiat** et **analyse de l'impact**.
- **Notification sous 72h** à l'Agence Andorrane de Protection des Données (APDA) si nécessaire.
- **Information des utilisateurs concernés** si un risque élevé est identifié.
- **Audit post-incident** pour renforcer les mesures de protection.

2.8. Cyber-Résilience et Protection Contre les Sinistres et Cyberattaques

Freemindtronic garantit **l'intégrité et la disponibilité** des données même en cas de panne, vol, catastrophe ou cyberattaque massive.

2.8.1. Chiffrement et Sauvegarde Sécurisée

- **Chiffrement avancé** : AES-256 CBC, AES-256 CBC PGP, BitLocker avec clés stockées **sur NFC HSM PassCypher**.
- **Séparation des clés et des données** : Les **clés de déchiffrement** ne sont jamais stockées sur les mêmes supports que les données. Les clés de chiffrement AES-256 CBC sont partageables de manière ultra-sécurisée via NFC HSM DataShielder, fonctionnant sans contact, sans serveur et sans base de données. Ce mécanisme garantit une transmission sécurisée des clés, même à distance, en éliminant tout risque d'interception par des tiers.
- **Sauvegardes chiffrées et redondantes** : Données répliquées **sur plusieurs supports hors ligne** et sécurisés.

2.8.2. Protection Renforcée Contre les Cyberattaques

- **Ransomware & surchiffrement** : Les sauvegardes hors ligne chiffrées et les clés externalisées physiquement hors ligne empêchent toute altération ou récupération frauduleuse.
- **Cyberattaques avancées (APT, Zero-Day, espionnage)** : L'architecture **Zero Trust & Zero Knowledge** et la **séparation physique des clés** empêchent toute exfiltration. L'architecture de sécurité de Freemindtronic, intégrant des systèmes brevetés de chiffrement segmenté et un contrôle d'accès matériel, garantit qu'aucune clé privée ou donnée chiffrée ne puisse être

exfiltrée, même sous contrainte physique ou logique. La combinaison du chiffrement AES-256 CBC et du RSA-4096 renforce la résilience aux attaques avancées, y compris celles assistées par intelligence artificielle.

- **Résilience sans cloud** : **Aucune dépendance aux serveurs distants**, éliminant les risques d'attaques centralisées.

2.8.3. Résilience aux Sinistres Physiques et Pertes Accidentelles

Les protocoles de Freemindtronic assurent toujours un accès aux données chiffrées avec leurs clés, même en cas de :

- **Vol ou perte** de supports chiffrés : Sans **les clés externalisées**, les données restent inexploitables.
- **Destruction accidentelle ou catastrophe naturelle** : La **duplication des sauvegardes** garantit la récupération des données sensibles.
- **Isolement géographique des sauvegardes** : Les **supports chiffrés** sont conservés en divers lieux sécurisés, évitant une compromission totale.

2.9. Accords de Non-Divulgation (NDA) et Confidentialité des Échanges

Toutes les relations professionnelles avec Freemindtronic impliquant des échanges d'informations sensibles ou confidentielles sont systématiquement couvertes par un **contrat de non-divulgation (NDA - Non-Disclosure Agreement)**.

- **Application stricte** : Toute information échangée dans le cadre de partenariats, de collaborations techniques ou de discussions commerciales est protégée par des clauses de **confidentialité juridiquement contraignantes**.

- **Portée du NDA** : Le NDA couvre les **documents, communications, échanges techniques, innovations, données internes**, ainsi que toute information confidentielle transmise par Freemindtronic ou reçue d'un partenaire.

- **Sanctions en cas de violation** : Toute divulgation non autorisée d'informations confidentielles est passible de **sanctions contractuelles et juridiques** pouvant inclure des actions en justice pour atteinte à la confidentialité et aux secrets industriels.

- **Durée de protection** : Les obligations de non-divulgation restent en vigueur **même après la fin de la relation contractuelle**, selon la durée définie dans chaque accord.

Cette clause renforce l'engagement de Freemindtronic à protéger toutes les informations critiques échangées dans le cadre de ses activités, en garantissant un cadre juridique strict contre toute fuite ou compromission.

ARTICLE 3 – UTILISATION DES CAPTEURS ET ACCÈS AUX DONNÉES DE LOCALISATION

Certains logiciels, applications ou extensions de **Freemindtronic** peuvent nécessiter l'accès aux capteurs des appareils des utilisateurs.

3.1 Ces capteurs incluent :

- **GPS** (localisation précise)

- **Wi-Fi et réseaux mobiles** (localisation approximative)

- **Bluetooth** (détection locale sans transmission externe)

- **Données biométriques** (empreinte digitale, reconnaissance faciale)
- **Microphone et caméra** (uniquement avec consentement explicite)
- **Capteurs environnementaux** (accéléromètre, gyroscope, capteurs de proximité, luminosité)
- **Modules de sécurité** (NFC, HSM, HSM PGP)

3.2 Toutes les données générées par ces capteurs :

- **Restent exclusivement sur l'appareil de l'utilisateur** et ne sont en aucun cas transmises à un serveur distant ou à un service tiers.
- **Ne font l'objet d'aucun stockage externe ou à distance**.
- **Ne sont accessibles qu'avec le consentement explicite de l'utilisateur**, notamment pour les capteurs sensibles tels que le microphone et la caméra.
- **Peuvent être gérées par l'utilisateur**, qui peut modifier ou révoquer les autorisations accordées à tout moment via les paramètres de son appareil.

3.2 Garantie de non-utilisation des données des capteurs à des fins de suivi comportemental

Freemindtronic garantit que **les données collectées via les capteurs des appareils ne sont jamais utilisées pour du suivi comportemental, de la publicité ciblée ou du profilage des utilisateurs**.

L'accès aux capteurs est strictement limité aux fonctionnalités essentielles des logiciels et uniquement après obtention du consentement explicite de l'utilisateur.

Aucune analyse des habitudes d'utilisation n'est effectuée à partir de ces données, et celles-ci ne sont ni stockées ni transmises à des tiers.

ARTICLE 4 – CONFORMITÉ AVEC LES PLATEFORMES DE DISTRIBUTION

Les logiciels, applications et extensions développés par **Freemindtronic** respectent les exigences des plateformes suivantes :

- **Google Play Console** (applications Android)
- **Chrome Web Store** (extensions de navigateur)
- **Microsoft Store et Edge Add-ons** (applications Windows et extensions de navigateur)
- **Apple macOS et iOS** (applications distribuées sur l'App Store)

Freemindtronic s'engage à respecter les directives de **sécurité et de confidentialité** imposées par ces plateformes.

- **L'architecture Zero Trust & Zero Knowledge est garantie** afin qu'aucune donnée utilisateur ne soit collectée, transmise ou stockée au-delà de l'appareil de l'utilisateur.
- **Aucune intégration avec des services tiers** n'est effectuée afin de limiter les risques liés au suivi ou à la collecte de données personnelles.
- **Les exigences de chaque plateforme sont régulièrement revues** afin de garantir une conformité continue aux évolutions des règlements applicables.

ARTICLE 5 – CLAUSE DE NON-DISCRIMINATION (CONFORMITÉ CCPA)

Conformément aux dispositions du **California Consumer Privacy Act (CCPA)**, **Freemindtronic garantit que les utilisateurs ne seront pas discriminés** pour l'exercice de leurs droits en matière de protection des données personnelles.

Aucune restriction ou limitation ne sera appliquée aux utilisateurs souhaitant exercer leurs droits, notamment en ce qui concerne :

- L'accès aux données personnelles les concernant.
- La rectification d'informations inexactes ou incomplètes.
- La suppression des données fournies volontairement.
- L'opposition ou la limitation du traitement de leurs données.

Freemindtronic s'engage à ne pas appliquer de frais supplémentaires, ni de modifications dans l'accès aux fonctionnalités, en réponse à une demande d'exercice des droits par un utilisateur.

Tout utilisateur souhaitant faire valoir ses droits peut contacter directement Freemindtronic en utilisant les coordonnées fournies dans cette politique de confidentialité.

Conformément au CCPA, l'exercice des droits de protection des données personnelles (accès, suppression, opposition) n'entraînera aucune modification, restriction ou dégradation des services proposés par Freemindtronic.

ARTICLE 6 – ABSENCE DE PROFILAGE ET DE FINGERPRINTING

6.1. Absence de Profilage et de Décisions Automatisées

Freemindtronic ne réalise aucun profilage, suivi comportemental ou prise de décision automatisée affectant les utilisateurs.

- Aucune analyse d'activité des utilisateurs n'est effectuée.
- Aucun algorithme d'intelligence artificielle n'est utilisé pour classifier les utilisateurs.
- Aucun mécanisme de personnalisation des services basé sur des données utilisateurs n'est mis en place.

6.2. Absence de Fingerprinting

Le **fingerprinting** est une technique qui consiste à collecter des informations spécifiques sur le matériel ou les logiciels d'un appareil, telles que l'adresse IP, le système d'exploitation, la résolution d'écran, et d'autres paramètres, afin de créer une empreinte numérique unique de l'utilisateur. Contrairement aux cookies, cette méthode est difficile à détecter et à bloquer, ce qui pose des préoccupations majeures en matière de confidentialité.

En décembre 2024, **Google a annoncé qu'à partir du 16 février 2025, il autoriserait les annonceurs à utiliser le fingerprinting** pour le suivi des utilisateurs, revenant ainsi sur sa politique de 2019 qui interdisait cette pratique. Cette décision a suscité des critiques de la part de régulateurs tels que l'**Information Commissioner's Office (ICO) du Royaume-Uni**, qui a qualifié ce changement d'« irresponsable » en raison de la réduction du choix et du contrôle des individus sur la collecte de leurs informations.

Chez **Freemindtronic**, nous nous engageons fermement à respecter la vie privée de nos utilisateurs. Ainsi, nous **n'utilisons aucune forme de fingerprinting** dans nos produits ou services. **Google a annoncé en décembre 2024 qu'il autoriserait le fingerprinting pour les annonceurs à partir du 16**

février 2025 (source officielle - https://blog.google/products/ads-commerce/privacy-sandbox-fingerprinting-policy-change).

Cette décision a soulevé des inquiétudes de la part des régulateurs, notamment **l'ICO du Royaume-Uni**. Freemindtronic rejette ces pratiques et garantit qu'**aucun suivi, identification des appareils ou profilage comportemental** n'est mis en place.

Tous les systèmes informatiques de Freemindtronic sont **totalement isolés et indépendants** les uns des autres. **Aucune donnée utilisateur n'est enregistrée, stockée ou tracée** grâce à un fonctionnement exclusivement local et déconnecté. **L'utilisation de solutions de chiffrement matériel et d'authentification NFC HSM** garantit qu'aucune empreinte numérique ne peut être associée aux utilisateurs notamment par l'utilisation de la technologie EviBITB de Freemindtronic.

Freemindtronic met en œuvre une **stratégie avancée de cybersécurité** pour se prémunir contre les attaques assistées par IA, les fraudes au président et autres usurpations d'identité.

- Les **emails utilisés pour la communication externe** sont des **adresses sandbox (bacs à sable) et des emails no-reply** pour **réduire les risques d'usurpation et de phishing**.
- Toute ouverture de pièce jointe est soumise à une **politique stricte de contrôle** afin d'écarter **tout risque de fichier malveillant**.
- Chaque **demande client** est systématiquement vérifiée par **un second canal de communication** pour **confirmer son authenticité** (levée de doute proactive).

ARTICLE 7 – CONFORMITÉ AVEC LES RÉGLEMENTATIONS SUR LES PRODUITS À DOUBLE USAGE

7.1. Réglementation et Autorisation d'Exportation

Freemindtronic applique strictement les réglementations en matière de gestion et d'exportation des technologies de cybersécurité, y compris pour les **produits de chiffrement classés double usage civil et militaire**.

Les produits **DataShielder NFC HSM** ont reçu une **autorisation d'importation en France depuis la Principauté d'Andorre**, validée le **7 décembre 2024** via l'entreprise **AMG Pro**, conformément au **décret n° 2001-1192 du 13 décembre 2001**, modifié par le **décret n° 2024-95 du 8 février 2024**.

Cette autorisation a été obtenue après soumission du dossier à l'**ANSSI**, qui, conformément à sa mission de **vérification de la conformité aux exigences réglementaires**, n'a pas opposé de refus dans les délais prévus par la législation en vigueur.

Depuis le **7 février 2025**, les produits **DataShielder NFC HSM** sont également **autorisés à la réexportation** depuis la France vers les États membres de l'Union européenne, dans le respect du **Règlement (UE) 2021/821 du 20 mai 2021** sur les biens à double usage.

7.2. Textes de Référence

Cette autorisation est délivrée en application des textes suivants :

- **Décret n° 2001-1192 du 13 décembre 2001**, modifié par **l'arrêté du 8 février 2024**, relatif au contrôle à l'exportation et au transfert des biens et technologies à double usage.
- **Règlement (UE) 2021/821 du 20 mai 2021**, établissant un régime de contrôle des exportations des produits à double usage.

7.3. Engagement en Matière d'Audit

Freemindtronic s'engage à assurer des **audits de conformité réguliers** pour garantir **l'adhésion continue aux exigences légales et réglementaires**. Ces audits internes sont réalisés périodiquement selon les exigences réglementaires en vigueur.

ARTICLE 8 – CERTIFICATIONS ET AUDITS

8.1. Absence d'Exigence de Certifications Cloud

Freemindtronic ne requiert pas de certifications **SOC 2** ou **ISO 27001** spécifiques aux infrastructures cloud, car **aucun serveur distant n'est utilisé** pour le traitement ou le stockage des données.

Les produits sont conçus selon une approche **100% air-gapped**, garantissant **une isolation totale des données utilisateur** de toute infrastructure réseau externe. Cette architecture justifie **l'absence de certains audits** normalement appliqués aux systèmes connectés.

8.2. Audit de Sécurité et Contrôle Qualité

Cette approche **est appliquée dans toute la chaîne de valeur**, depuis la **conception** jusqu'à la **fabrication des produits**. Tous les audits réalisés visent à garantir la **résilience, l'inviolabilité et l'absence de fuites de données** des systèmes de Freemindtronic.

En plus des audits internes garantissant la conformité des produits, Freemindtronic applique des **contrôles renforcés sur la gestion des paiements** et la **protection des transactions financières**.

- Le système de gestion comptable et financier est isolé, et aucune transaction ne peut être validée sans authentification forte via DataShielder NFC HSM Auth et DataShielder MAuth, assurant une authentification forte et évacuant les risques de fraude.
- Les accès aux comptes bancaires et aux systèmes de paiement sont strictement limités aux actionnaires habilités, sans lien de subordination, pour limiter les risques interne de fraude.

ARTICLE 9 – RESPONSABLE DE LA PROTECTION DES DONNÉES (DPO)

9.1. Désignation du DPO

Conformément aux exigences du **Règlement Général sur la Protection des Données (RGPD – Règlement (UE) 2016/679)** et des autres réglementations applicables, Freemindtronic a désigné un **Délégué à la Protection des Données (DPO)** chargé de veiller à la conformité de l'entreprise en matière de protection des données personnelles.

Le **DPO de Freemindtronic** est :

- **Nom :** Jacques Gascuel
- **Fonction :** CEO et DPO de Freemindtronic SL
- **Contact :** dpo [at] freemindtronic.com

9.2. Missions du DPO

Le **DPO de Freemindtronic** assure plusieurs missions essentielles, notamment :

- Veiller à la **conformité des traitements de données** aux réglementations applicables (**RGPD, CCPA, LGPD, etc.**).

- Informer et conseiller Freemindtronic sur **ses obligations en matière de protection des données**.
- Contrôler l'application des **politiques de sécurité et de protection des données** mises en place.
- Répondre aux demandes des utilisateurs concernant **leurs droits (accès, rectification, suppression, opposition, etc.)**.
- Assurer la liaison avec les **autorités de protection des données**, notamment l'**Agence Andorrane de Protection des Données** et les autorités européennes ou internationales compétentes.

9.3. Contact et Réclamations

Tout utilisateur souhaitant obtenir des informations sur **la gestion de ses données personnelles** ou exercer ses droits peut contacter le **DPO de Freemindtronic** à l'adresse suivante :

- **Email :** dpo [at] freemindtronic.com
- **Adresse postale :**
  Freemindtronic SL
  Av. Co-Prince de Gaulle, 13, Valira Building, Rez-de-chaussée, AD700 Escaldes – Engordany, Andorre

Si aucune réponse n'est apportée dans un délai de **30 jours**, l'utilisateur peut saisir directement **l'Agence Andorrane de Protection des Données (APDA)** pour **non-respect de l'obligation légale de réponse sous 30 jours**.

ARTICLE 10 – CONFORMITÉ AVEC LA LÉGISLATION ANDORRANE SUR LA PROTECTION DES DONNÉES

10.1. Application des Lois Andorranes

Freemindtronic, en tant que société enregistrée en **Principauté d'Andorre**, est soumise aux réglementations locales en matière de **protection des données**, notamment :

- **Loi Qualifiée 15/2003 du 18 décembre 2003** sur la protection des données personnelles
- **Loi Qualifiée 29/2021 du 28 octobre 2021**, qui aligne Andorre sur les principes du **Règlement Général sur la Protection des Données (RGPD – Règlement (UE) 2016/679)**

Ces lois garantissent un cadre de **protection des données** équivalent aux standards européens, reconnu **adéquat** par l'Union Européenne conformément à **l'article 45 du RGPD**.

En complément des réglementations en vigueur, **Freemindtronic met en œuvre des mesures physiques et logicielles avancées pour garantir une protection absolue des données**. Cela inclut **le chiffrement intégral des supports numériques, l'authentification multifactorielle NFC HSM et l'isolement physique des infrastructures informatiques**. Ces dispositifs permettent d'assurer **une conformité totale aux articles 10 et 45 du RGPD**, en garantissant une protection des données équivalente aux standards européens les plus stricts.

ARTICLE 12 – PRINCIPES DE CONFORMITÉ ET SÉCURITÉ DES DONNÉES

12.1. Confidentialité dès la Conception

Freemindtronic intègre la **protection des données** dès la **conception de ses logiciels et services**, conformément aux principes de **privacy by design et privacy by default**.

12.2. Absence de Stockage des Données

En accord avec **l'approche Zero Trust & Zero Knowledge**, **Freemindtronic ne stocke ni ne traite aucune donnée personnelle**, sauf en cas de fourniture volontaire par l'utilisateur (ex. : formulaire de contact, assistance technique).

12.3. Adoption de Mesures de Sécurité Renforcées

Freemindtronic met en œuvre des mesures de **sécurité avancées** pour garantir la **protection des données** et prévenir toute violation, notamment :

- **Chiffrement systématique** des communications et transactions utilisateurs via ses systèmes brevetés de chiffrement à clés segmentés
- **Absence d'identifiants uniques** pouvant être exploités pour tracer l'activité des utilisateurs
- **Auditabilité régulière interne** pour assurer la conformité aux réglementations en vigueur

Ces mesures sont conformes à **l'article 10 de la Loi Qualifiée 29/2021** sur la protection des données personnelles en Andorre.

Freemindtronic applique une stratégie de cybersécurité complète garantissant la protection des données même en cas d'intrusion physique dans les locaux :

Tous les systèmes informatiques (fixes, mobiles, serveurs et périphériques de stockage) sont intégralement chiffrés avec des clés ≥256 bits.

Tous les sites connectés en ligne ou en réseau local utilisent PassCypher NFC HSM et PassCypher HSM PGP avec TOTP/HOTP et/ou DataShielder NFC HSM et DataShielder HSM PGP Cyber Defense.

Aucune clé de chiffrement n'est stockée ou visible sur les outils de production.

Les supports sensibles (clés USB, disques durs) sont stockés dans un coffre-fort résistant au feu et aux intrusions.

Toute extraction de données sensibles est impossible, même en cas de vol physique des serveurs ou d'exfiltration illicite de fichiers.

Ces mesures garantissent que même en cas d'intrusion dans les locaux de Freemindtronic, aucune donnée ne pourra être exploitée même en cas d'intrusion illicite réussi.

12.4. Engagement envers la Sécurité Continue

Freemindtronic place la **protection des données** au cœur de ses activités et s'engage à :

- **Améliorer continuellement ses mesures de sécurité** en suivant l'évolution des menaces et des réglementations.
- **Adapter ses protocoles de protection** pour garantir un niveau de sécurité conforme aux nouvelles avancées technologiques et aux meilleures pratiques en cybersécurité.
- **Effectuer une veille constante** sur les cybermenaces, y compris celles assistées par intelligence artificielle (IA), afin d'anticiper les potentielles tentatives d'intrusion et de renforcer les défenses en conséquence.

12.4.1 Protection stratégique :
Freemindtronic ne divulgue pas publiquement tous les détails techniques de ses mécanismes de

sécurité afin de ne pas faciliter une analyse par un attaquant ou une intelligence artificielle cherchant à identifier une éventuelle faille.
Cependant, toutes les mesures mises en place respectent les standards **les plus stricts** en matière de cybersécurité et de protection des données.

12.5. Sécurité Opérationnelle et Protection des Données Sensibles

Freemindtronic applique un modèle de sécurité strict garantissant une **protection maximale contre les risques d'espionnage interne et externe**.

12.5.1 Isolation des Systèmes Informatiques

- Aucune connexion réseau entre les systèmes internes et aucun partage de fichiers ou d'imprimantes n'est autorisé.
- Chaque système est entièrement indépendant, évitant ainsi toute vulnérabilité liée à des connexions externes.

12.5.2 Transferts Sécurisés des Données Sensibles

- Tous les transferts de fichiers sensibles sont réalisés **exclusivement** via des clés USB sécurisées **EviKey NFC** de Freemindtronic.
- Ces clés disposent d'un **auto-verrouillage automatique** lorsqu'elles ne sont pas utilisées, empêchant tout accès non autorisé.
- Un **journal de traçabilité** est intégré dans la boîte noire des clés EviKey NFC, permettant de vérifier chaque déverrouillage et sa **géolocalisation**.

12.5.3 Isolation Physique et Sécurisation des Outils de Production

- Les équipements de production et les outils sensibles **ne sont jamais connectés à Internet** et sont strictement isolés après usage.
- Après utilisation, ces outils sont **conservés dans un coffre-fort spécial** résistant aux incendies et aux intrusions physiques.

12.5.4 Génération et Sécurisation des Clés d'Authentification

- Les clés d'authentification anti-contrefaçon servant également de **clés segmentées** sont générées **aléatoirement** par les outils de production.
- Ces clés **ne sont ni affichées ni sauvegardées** dans les outils de production, garantissant l'absence de toute trace exploitable.

12.5.5 Contrôle d'Accès Strict et Limitation des Risques Internes

- Seules **deux personnes habilitées**, également **actionnaires de l'entreprise**, sont autorisées à utiliser les outils de production.
- Cette restriction vise à **minimiser les risques liés aux relations de subordination** et à garantir un contrôle total sur les accès aux infrastructures sensibles.

12.6. Contrôle d'Accès Strict et Limitation des Risques Internes

12.6.1 Sécurisation des Accès et Chiffrement Systématique

Freemindtronic applique des protocoles avancés d'authentification et de chiffrement garantissant que tous les accès et supports numériques sont protégés contre toute tentative d'intrusion ou de vol.

12.6.1.1 Protection des Accès aux Sites et Réseaux
Tous les systèmes en ligne et en réseau local utilisent exclusivement les technologies d'authentification forte suivantes :

- PassCypher NFC HSM et/ou PassCypher HSM PGP, intégrant des protocoles TOTP (Time-Based One-Time Password) et HOTP (HMAC-Based One-Time Password).
- DataShielder NFC HSM et/ou DataShielder HSM PGP en version Cyber Defense, combinant authentification forte et chiffrement avancé des accès.
- Émulateurs de clavier Bluetooth USB pour sécuriser les entrées de données sensibles en éliminant tout risque de keylogging.

12.6.1.2 Chiffrement des Données et des Supports de Stockage
Tous les systèmes informatiques (fixes, mobiles) ainsi que tous les périphériques de stockage contenant des données sensibles sont chiffrés avec des clés de chiffrement égales ou supérieures à 256 bits.

- Disques durs internes et externes entièrement chiffrés.
- Stockage mobile et périphériques de sauvegarde protégés par chiffrement matériel et/ou logiciel.

12.6.1.3 Résilience face aux Intrusions Physiques et Numériques
Tout est conçu pour que, en cas d'intrusion dans les locaux de Freemindtronic, de vol de support numérique ou d'extraction illicite de données sensibles, aucune donnée ne soit exploitable ni physiquement accessible.

- Clés de chiffrement sécurisées dans des dispositifs NFC HSM, empêchant tout accès non autorisé.
- Blocage automatique des clés ou verrouillage en cas de tentative de compromission avec traçabilité par boite noire.

12.6.1.4 Intégration des Produits utilisant la Technologie EviKey NFC

Les produits de Freemindtronic intégrant la technologie **EviKey NFC** utilisent exclusivement l'application **Fullkey Plus** pour leur gestion et leur sécurisation. Cette technologie est également intégrée aux solutions de cybersécurité suivantes :

- **PassCypher NFC HSM Master**
- **DataShielder NFC HSM Master & Defense**

L'intégration d'EviKey NFC dans ces solutions offre un contrôle avancé des accès aux supports de stockage et inclut les fonctionnalités suivantes :

- **Auto-verrouillage en cas d'inactivité**
- **Gestion sécurisée des clés**
- **Traçabilité des accès via une boîte noire**, accessible uniquement sans contact via un téléphone **Android NFC**, grâce à l'application **Fullkey Plus**, **PassCypher NFC HSM**, ou **DataShielder NFC HSM**.

Freemindtronic ne prend aucun risque en matière de sécurité et ne se laisse pas surprendre : ici, **le cordonnier n'est surtout pas le plus mal chaussé** ! 😉

Freemindtronic met en œuvre des **cloisons de sécurité étanches**, empêchant toute forme d'espionnage, qu'il soit **interne ou externe**, et garantissant une protection **maximale** des actifs numériques et des données critiques.

12.6.1.4 – Protection contre l'IA et les attaques avancées :

Freemindtronic met en œuvre des technologies et des protocoles spécifiques pour se prémunir contre les attaques assistées par intelligence artificielle, y compris les deepfakes et les manipulations audio/vidéo visant à compromettre l'identité numérique des dirigeants et des utilisateurs. Ces mesures incluent une vérification renforcée des communications et une analyse multi-facteurs des échanges sensibles.

Article 12.7 – Gestion des Violations de Données :

En cas de compromission matérielle ou de tentative de violation de sécurité affectant les infrastructures de Freemindtronic, des procédures de réponse aux incidents sont réalisées de manière proactive, indépendamment de l'absence d'un système de détection automatisé.

Freemindtronic reconnaît qu'il est illusoire de garantir une protection absolue contre un attaquant déterminé, même avec les meilleures mesures de sécurité au monde. C'est pourquoi l'approche adoptée repose sur une stratégie **proactive et préventive**, intégrant des innovations brevetées à l'international et développées pour anticiper les nouvelles formes d'espionnage, notamment celles assistées par **intelligence artificielle**.

L'ensemble des solutions de cybersécurité de Freemindtronic est conçu pour empêcher toute exploitation des données, même en cas d'accès physique ou numérique non autorisé. Cette approche repose sur des mécanismes avancés incluant l'auto-verrouillage matériel, le chiffrement à clés segmentées, l'isolation des infrastructures et l'usage exclusif de supports sécurisés tels que EviKey NFC, PassCypher NFC HSM et DataShielder NFC HSM.

Dans l'éventualité où un incident de sécurité concernerait un client ou un partenaire, Freemindtronic s'engage à **les informer dans les meilleurs délais**, conformément aux exigences des réglementations applicables en matière de protection des données.

ARTICLE 13 – DROITS DES UTILISATEURS SOUS LA LÉGISLATION ANDORRANE

Conformément aux **articles 16 à 21 de la Loi 29/2021**, les utilisateurs disposent des droits suivants, alignés avec le **RGPD et la législation andorrane** :

- **Droit d'Accès** : Vérifier quelles informations ont été fournies volontairement et traitées.
- **Droit de Rectification** : Corriger toute donnée inexacte ou incomplète.
- **Droit d'Opposition** : Contester l'utilisation de leurs données.
- **Droit de Suppression (Droit à l'Oubli)** : Exiger la suppression définitive de leurs données.
- **Droit à la Portabilité** : Recevoir leurs données dans un format lisible (nouvelle obligation renforcée par la loi 29/2021).
- **Droit à la Limitation du Traitement** : Restreindre le traitement de certaines informations.

13.1. Délai de Traitement des Demandes

Freemindtronic garantit que toute demande d'exercice des droits sera **traitée sous un délai maximal de 30 jours**, sauf circonstances exceptionnelles nécessitant une **prolongation justifiée de 60 jours maximum**.

Les demandes peuvent être adressées par e-mail à :
contact [at] freemindtronic.com ou **dpo [at] freemindtronic.com**

ARTICLE 14 – RECOURS EN CAS DE LITIGE

Si un utilisateur estime que **ses droits n'ont pas été respectés**, il peut déposer une réclamation auprès de l'**Agence Andorrane de Protection des Données (APDA)**, **autorité de contrôle compétente en Andorre**.

14.1. Procédure de Réclamation

Conformément à **l'article 25 de la Loi 29/2021**, toute personne estimant que le traitement de ses données a été effectué en **violation des lois applicables** peut :

- **Saisir l'Agence Andorrane de Protection des Données (APDA)** pour une enquête administrative.
  Contact de l'APDA : https://www.apda.ad
- **Introduire un recours devant les tribunaux compétents en Andorre** afin d'obtenir réparation du préjudice subi.

Freemindtronic s'engage à **collaborer pleinement** avec les autorités de protection des données en cas d'investigation.

ARTICLE 15 – MODIFICATIONS DE LA POLITIQUE DE CONFIDENTIALITÉ

Freemindtronic s'engage à mettre à jour cette politique en cas d'évolution législative ou réglementaire affectant la protection des données.

Toute modification sera publiée explicitement sur le site web officiel de Freemindtronic.

Les utilisateurs qui souhaitent être informés des mises à jour par e-mail devront en faire expressément la demande en fournissant leur adresse e-mail à Freemindtronic.

En cas d'évolution des fonctionnalités impliquant un traitement de données, Freemindtronic s'engage à informer les utilisateurs par notification sur le site ou dans les applications concernées.

ARTICLE 16 – COORDONNÉES DE CONTACT

Freemindtronic SL
Email : **contact [at] freemindtronic.com**
Téléphone : **+376 804 500**
Politique des cookies : https://freemindtronic.com/cookie-policy/

Fin du document