POLÍTICA DE PRIVACITAT – FREEMINDTRONIC SL

Web i programari – Versió i data del document: V2.0 de 28/02/2025

ARTICLE 1 – INTRODUCCIÓ

1.1. Identificació del responsable del tractament

Aquesta Política de Privacitat és emesa per **Freemindtronic SL,** societat de responsabilitat limitada registrada sota les lleis del Principat d'Andorra, amb domicili social a:

Av. Co-Prince de Gaulle, 13, Edifici Valira, Planta baixa, AD700 Escaldes – Engordany, Andorra.

Freemindtronic és responsable del tractament de les dades recollides o tractades mitjançant l'ús del seu lloc web oficial https://freemindtronic.com així com del seu programari, aplicacions, extensions i sistemes incrustats.

1.2. Camp d'aplicació

Aquesta Política de Privacitat s'aplica a tots els serveis, programari, aplicacions, extensions i sistemes integrats desenvolupats i operats per Freemindtronic.

No s'aplica a llocs web, serveis o plataformes de tercers accessibles a través dels serveis de Freemindtronic. Freemindtronic no es fa responsable de les pràctiques de privadesa d'aquests serveis de tercers.

1.3. Compromís: Confiança Zero i Coneixement Zero

Freemindtronic s'adhereix a un estricte **marc Zero Trust i Zero Knowledge**, assegurant que les dades dels usuaris no s'accedeixin, s'emmagatzemin o es comparteixin en absolut.

Tot el programari, aplicacions, extensions i sistemes integrats desenvolupats per Freemindtronic funcionen **sense un servidor remot, una base de dades centralitzada, la creació d'un compte d'usuari, la identificació de l'usuari i la transmissió de dades**.

Totes les funcions de Freemindtronic garanteixen que les dades de l'usuari no s'emmagatzemin ni es transmetin a servidors remots. Tot el tractament es realitza exclusivament localment al dispositiu de l'usuari, sense interacció amb una infraestructura externa.

1.4. Compliment de la normativa

- Freemindtronic compleix amb les més estrictes normatives internacionals de protecció de dades i ciberseguretat, que inclouen:
- Reglament General de Protecció de Dades (RGPD – Reglament (UE) 2016/679)
- Llei de resiliència operativa digital (DORA – Règlement (UE) 2022/2554)
- Directiva NIS2 (Directiva (UE) 2022/2555) sobre ciberseguretat d'infraestructures crítiques
- Llei de privadesa del consumidor de Califòrnia (SCCA - EUA, Cal. Civ. Code § 1798.100 i següents)
- Llei General de Protecció de Dades (LGPD – Brésil, Llei núm. 13.709/2018)
- Llei 15/2003 de Protecció de Dades de Caràcter Personal a Andorra, modificada per la Llei Qualificada 29/2021
- Reglament (UE) 2021/821, de 20 de maig de 2021, relatiu al control de les exportacions de productes de doble ús
- Estàndards ISO/IEC 27001 i millors pràctiques de seguretat NIST (National Institute of Standards and Technology, EUA)

1.5. DefinicionsEn aquesta política, els termes següents es defineixen de la següent manera:

- **Dades personals** : qualsevol informació relativa a una persona física identificada o identificable, directament o indirectament, en particular per referència a un identificador com un nom, un número d'identificació, dades d'ubicació, un identificador en línia o a un o més elements específics de la seva identitat física, fisiològica, genètica, mental, econòmica, cultural o social.
- **Dades sensibles** : qualsevol informació la divulgació no autoritzada de la qual pugui suposar un alt risc per als drets i llibertats dels interessats. Això inclou, entre d'altres:
    - Identificadors únics (noms d'usuari, contrasenyes, codis d'autenticació).
    - Claus d'encriptació i autenticació.
    - Informació de pagament i dades bancàries.
    - Dades confidencials de clients i col·laboradors (estratègies comercials, patents, documents protegits per secrets empresarials).
    - Qualsevol dada personal que entri en les categories especials de l'RGPD (origen ètnic, opinions polítiques, creences religioses, salut, biometria, vida sexual).
- **Processament** significa qualsevol operació o conjunt d'operacions que es realitzen sobre dades personals, ja sigui per mitjans automatitzats o no, com ara la recopilació, l'enregistrament, l'organització, l'estructuració, l'emmagatzematge, l'adaptació o la modificació, la recuperació, la consulta, l'ús, la divulgació per transmissió, difusió o la posada a disposició d'una altra manera, l'alineació o la combinació, limitació, esborrament o destrucció.
- **Responsable del tractament** : la persona física o jurídica, autoritat pública, agència o un altre organisme que, sol o conjuntament amb altres, determina les finalitats i els mitjans del tractament de les dades personals.
- **Encarregat del tractament** : la persona física o jurídica, autoritat pública, agència o un altre organisme que tracta dades personals en nom del responsable.
- **Consentiment** : qualsevol indicació lliure, específica, informada i inequívoca de la voluntat de l'interessat per la qual accepta, mitjançant una declaració o una acció afirmativa clara, el tractament de les dades personals que li concerneixen.
- **Pseudonimització** : tractament de dades personals de manera que ja no es puguin atribuir a una persona física concreta sense informació addicional, que s'ha de mantenir separada i protegida mitjançant les mesures tècniques i organitzatives adequades.
- **Anonimització** : transformació irreversible de les dades personals de manera que ja no sigui possible identificar directament o indirectament l'interessat.
- **Violació de dades personals** : Qualsevol violació de seguretat que accidentalment o il·legalment resulti en la destrucció, pèrdua, alteració, divulgació no autoritzada o accés a dades personals. Això inclou l'accés no autoritzat a inicis de sessió, contrasenyes, claus de xifratge o altres dades sensibles protegides.

ARTICLE 2 – RECOLLIDA I TRACTAMENT DE DADES

2.1. Manca de recollida sistemàtica de dades

Freemindtronic no recopila, emmagatzema, comparteix ni ven cap dada personal o tècnica dels usuaris, excepte en el cas d'interacció directa, incloent-hi:

- Una comanda a través de plataformes oficials.
- Una sol·licitud de contacte relacionada amb el servei d'atenció al client o una col·laboració oficial.

Les dades només es tracten en l'àmbit estricte de l'execució del contracte o relació comercial i mai s'utilitzen per a cap altra finalitat.

2.2. Dades que es poden recollir

Si un usuari proporciona informació voluntàriament, només es tracten les dades estrictament necessàries:

- Identitat (cognoms, noms)
- Dades de contacte (correu electrònic, telèfon, adreça de facturació i lliurament)
- Informació professional
- Contingut enviat voluntàriament

Les dades transaccionals s'utilitzen exclusivament per a la gestió de les comandes i el seu lliurament, sense transmissió a tercers excepte obligacions legals (fiscals i comptables).

2.2.1 – Dades emmagatzemades localment a l'extensió o aplicacióAlgunes aplicacions i extensions de Freemindtronic poden utilitzar localStorage o l'API d'emmagatzematge web per emmagatzemar temporalment la configuració local al dispositiu de l'usuari. Aquestes dades mai es transmeten a servidors remots i només són accessibles dins del programari utilitzat.

2.3. Emmagatzematge i seguretat de les dades

Freemindtronic aplica els més alts estàndards de seguretat, complint amb les regulacions **GDPR, DORA, NIS2, ISO/IEC 27001 i NIST**.

- **Emmagatzematge segur fora de línia** : les dades es guarden en suports xifrats als quals només es pot accedir mitjançant unitats flash USB segures EviKey NFC i/o suports d'emmagatzematge xifrats i/o dades xifrades.
- **Zero Trust & Zero Knowledge** : Manca de servidors remots i bases de dades centralitzades per emmagatzemar i/o gestionar dades sensibles per a tots els productes Freemindtronic.
- **Seguretat millorada per a les comunicacions sensibles**: L'intercanvi de dades sensibles es realitza exclusivament a través d'eines **DataShielder** o d'un protocol segur definit pel client.
- **Alternativa imposada si cal** : Si el servei del client no garanteix un nivell de seguretat suficient, Freemindtronic ofereix **DataShielder** com a únic canal segur.

2.4. Protecció de dades classificades i entorns sensibles

Les solucions Freemindtronic identificades com a producte civil i militar de doble ús estan dissenyades per protegir la informació crítica i inclouen:

- **Aïllament físic i partició:** no s'emmagatzemen dades en un servidor remot.
- **Autenticació** forta: HSM NFC i xifratge de claus segmentades patentat. L'ús del xifratge asimètric RSA-4096 permet compartir de manera segura les claus CBC AES-256 entre dispositius NFC HSM, fins i tot de forma remota, sense transmissió a través d'infraestructures centralitzades. Aquest mecanisme elimina el risc d'exfiltració de claus i proporciona una protecció avançada per als intercanvis xifrats.
- **Xifratge d'extrem a extrem** : AES-256 CBC, RSA-4096, PGP - Tots els sistemes de xifratge simètric segur s'aconsegueixen mitjançant claus segmentades i sistemes de control d'accés

patentats i lliurats internacionalment. Aquesta arquitectura fa que el xifratge sigui resistent als atacs quàntics, garantint la protecció a llarg termini de les dades sensibles.
- **Registre descentralitzat:** caixa negra local accessible només en NFC per un administrador autoritzat.
- **Proves d'estrès i ciberseguretat proactiva** : avaluacions periòdiques contra atacs APT, espionatge industrial i amenaces cibernètiques avançades.

Si una extensió o aplicació de Freemindtronic accedeix a fitxers locals en un dispositiu Windows o Mac (per exemple, per emmagatzemar claus de xifratge o fitxers segurs), aquests fitxers es processen exclusivament localment i mai són accessibles per tercers. L'usuari conserva el control total sobre les seves dades i no es comparteixen amb altres serveis.

2.5. Emmagatzematge, supressió i retenció de les dades del client

- Les dades proporcionades a través d'un **formulari de contacte** s'utilitzen només per respondre a la sol·licitud i s'eliminen immediatament després del processament.
- Les dades del client resultants de les transaccions es conserven únicament durant el període legal necessari, d'acord amb la normativa aplicable en les següents jurisdiccions:
    - **Andorra: Llei qualificada 29/2021 – conservació de documents fiscals durant 5 anys**
    - **Unió Europea: article 6 de la Directiva de protecció del consumidor 2011/83/UE: conservació de les dades de les transaccions fins a 10 anys en funció dels requisits comptables locals**
    - **França: Article L123-22 del Codi de Comerç francès – conservació obligatòria dels documents comptables durant 10 anys**
    - **EUA: Publicació 583 de l'IRS - Retenció de dades de transaccions de 3-7 anys**
- **No s'emmagatzemen dades bancàries** : les transaccions es processen a través **de proveïdors externs segurs** (per exemple, PayPal).

2.6. Transferències internacionals de dades

Freemindtronic no transfereix cap dada fora de l'EEE tret que s'apliqui un marc legal adequat (**Clàusules Contractuals Tipus - SCC**).

2.7. Procediment de violació de dades

D'acord amb els articles 33 i 34 del **RGPD** i la **Llei qualificada 29/2021**, Freemindtronic aplica una **resposta proactiva** en cas d'incidència:

- **Contenció immediata** i **anàlisi d'impacte**.
- **Notificació en un termini de 72 hores** a l'Agència Andorrana de Protecció de Dades (APDA) si fos necessari.
- **Informar els usuaris afectats** si s'identifica un risc elevat.
- **Auditoria postincident** per reforçar les mesures de protecció.

2.8. Ciberresiliència i protecció contra desastres i ciberatacs

Freemindtronic garanteix **la integritat i disponibilitat** de les dades fins i tot en cas d'avaria, robatori, desastre o ciberatac massiu.

2.8.1. Xifratge i còpia de seguretat segura

- **Xifratge avançat** : AES-256 CBC, AES-256 CBC PGP, BitLocker amb claus emmagatzemades **a NFC HSM PassCypher**.
- **Separació de claus i dades**: les claus de desxifrat mai s'emmagatzemen al mateix suport que les dades. Les claus de xifratge AES-256 CBC es poden compartir de manera altament segura mitjançant NFC HSM DataShielder, que funcionen sense contacte, sense servidor i sense bases de dades. Aquest mecanisme garanteix una transmissió segura de claus, fins i tot de forma remota, eliminant qualsevol risc d'intercepció per part de tercers.
- **Còpies de seguretat xifrades i redundants**: dades replicades **en diversos suports fora de línia** i segures.

2.8.2. Protecció millorada contra ciberatacs

- **Ransomware i sobrexifratge** : les còpies de seguretat xifrades fora de línia i les claus físicament subcontractades fora de línia eviten la manipulació o la recuperació fraudulenta.
- **Ciberatacs avançats (APT, Zero-Day, espionatge):** L'arquitectura **Zero Trust i Zero Knowledge** i **la separació de claus físiques** eviten l'exfiltració. L'arquitectura de seguretat de Freemindtronic, que incorpora sistemes de xifratge segmentats patentats i control d'accés basat en maquinari, garanteix que no es puguin exfiltrar claus privades o dades xifrades, fins i tot sota restricció física o lògica. La combinació del xifratge AES-256 CBC i RSA-4096 augmenta la resistència als atacs avançats, inclosos els assistits per intel·ligència artificial.
- **Resiliència sense núvol** : **sense dependència de servidors remots**, eliminant el risc d'atacs centralitzats.

2.8.3. Resiliència davant desastres físics i pèrdues accidentals

Els protocols de Freemindtronic sempre garanteixen l'accés a les dades xifrades amb les seves claus, fins i tot en cas de:

- **Robatori o pèrdua** de suports xifrats: sense **claus subcontractades**, les dades romanen inutilitzables.
- **Destrucció accidental o desastre natural:** les còpies de seguretat **duplicades** garanteixen que es recuperin les dades sensibles.
- **Aïllament geogràfic de les còpies de seguretat**: els **suports xifrats** es mantenen en una varietat d'ubicacions segures, evitant el compromís total.

2.9. Acords de confidencialitat (NDA) i confidencialitat del comerç

Totes les relacions comercials amb Freemindtronic que impliquen l'intercanvi d'informació sensible o confidencial estan cobertes rutinàriament per un **acord de confidencialitat (NDA).**

- **Aplicació estricta** : Qualsevol informació intercanviada en el context de col·laboracions, col·laboracions tècniques o discussions comercials està protegida per clàusules de confidencialitat legalment vinculants. Tots els documents sensibles, xifrats o no, intercanviats amb clients i socis es signen digitalment sistemàticament mitjançant la funció integrada en DataShielder HSM PGP. Aquesta signatura digital garanteix la integritat i autenticitat dels documents, assegurant que no s'hagin produït alteracions o alteracions després de la seva emissió. A més, les comunicacions per correu electrònic que involucren informació sensible sempre estan protegides mitjançant PGP, evitant la intercepció o la manipulació dels missatges.

- **Abast de l'NDA** : L'NDA cobreix **documents, comunicacions, intercanvis tècnics, innovacions, dades internes**, així com qualsevol informació confidencial transmesa per Freemindtronic o rebuda d'un soci.
- **Sancions per infraccions** : Qualsevol divulgació no autoritzada d'informació confidencial està subjecta a **sancions contractuals i legals** que poden incloure accions legals per violació de la confidencialitat i els secrets comercials.
- **Termini de protecció** : Les obligacions de confidencialitat es mantenen vigents **fins i tot després de la finalització de la relació contractual**, segons el termini definit en cada acord.

Aquesta clàusula reforça el compromís de Freemindtronic de protegir tota la informació crítica intercanviada en el curs del seu negoci, garantint un marc legal estricte contra qualsevol filtració o compromís.

ARTICLE 3 – ÚS DE SENSORS I ACCÉS A LES DADES D'UBICACIÓ

Alguns programes, aplicacions o extensions **de Freemindtronic** poden requerir accés als sensors dels dispositius dels usuaris.

3.1 Aquests sensors inclouen:

- **GPS** (ubicació precisa)
- **Wi-Fi i xarxes mòbils** (ubicació aproximada)
- **Bluetooth** (detecció local sense transmissió externa)
- **Dades biomètriques** (empremta digital, reconeixement facial)
- **Micròfon i càmera** (només amb consentiment explícit)
- **Sensors ambientals** (acceleròmetre, giroscopi, sensors de proximitat, brillantor)
- **Mòduls de seguretat** (NFC, HSM, HSM, PGP)

3.2 Totes les dades generades per aquests sensors:

- **Romanen exclusivament al dispositiu de l'usuari** i no es transmeten a un servidor remot o servei de tercers en cap cas.
- **No estan subjectes a emmagatzematge extern o remot**.
- **Només són accessibles amb el consentiment explícit de l'usuari**, especialment per a sensors sensibles com el micròfon i la càmera.
- **Pot ser gestionat per l'usuari**, que pot canviar o revocar els permisos atorgats en qualsevol moment a través de la configuració del seu dispositiu.

Els sensors dels dispositius (càmera, micròfon, NFC, GPS, Wi-Fi, Bluetooth) només s'utilitzen localment i mai transmeten dades a servidors externs, tercers o altres serveis de Freemindtronic. L'usuari pot controlar i desactivar aquest accés a través de la configuració del dispositiu.

3.4 Garantir que les dades del sensor no s'utilitzin amb finalitats de seguiment del comportament

Freemindtronic garanteix que **les dades recollides a través dels sensors del dispositiu no s'utilitzin mai per al seguiment del comportament, la publicitat dirigida o el perfil de l'usuari**.

L'accés als sensors està estrictament limitat a les funcions essencials del programari i només després d'obtenir el consentiment explícit de l'usuari.

A partir d'aquestes dades no es realitza cap anàlisi dels patrons d'ús i no s'emmagatzemen ni es transmeten a tercers.

ARTICLE 4 – COMPLIMENT DE LES PLATAFORMES DE DISTRIBUCIÓ

El programari, les aplicacions i les extensions desenvolupades per **Freemindtronic** compleixen amb els requisits de les plataformes següents:

- **Google Play Console** (aplicacions Android)
- **Chrome Web Store** (extensions del navegador)
- **Complements del Microsoft Store i Edge** (aplicacions del Windows i extensions del navegador)
- **Apple macOS i iOS** (apps distribuïdes a l'App Store)

Freemindtronic es compromet a complir les directrius **de seguretat i privadesa** imposades per aquestes plataformes.

- **L'arquitectura Zero Trust & Zero Knowledge està garantida** perquè no es recopilin, transmetin o emmagatzemin dades de l'usuari més enllà del dispositiu de l'usuari.
- **No hi ha integració amb serveis de tercers** per mitigar els riscos associats al seguiment o la recopilació de dades personals.
- **Els requisits de cada plataforma es revisen periòdicament** per garantir el compliment continu dels canvis en la normativa aplicable.

SECCIÓ 5 - CLÀUSULA DE NO DISCRIMINACIÓ (COMPLIMENT DE LA CCPA)

D'acord amb les disposicions de la **Llei de privadesa del consumidor de Califòrnia (CCPA), Freemindtronic garanteix que els usuaris no seran discriminats** en l'exercici dels seus drets en matèria de protecció de dades personals.

No s'aplicaran restriccions ni limitacions als usuaris que vulguin exercir els seus drets, en particular pel que fa a:

- Accés a les seves dades personals.
- Rectificació d'informació inexacta o incompleta.
- Supressió de les dades facilitades voluntàriament.
- Oposar-se o limitar el tractament de les seves dades.

Freemindtronic es compromet a no aplicar tarifes addicionals, ni canvis en l'accés a les funcions, en resposta a una sol·licitud d'exercici de drets per part d'un usuari.

Qualsevol usuari que vulgui fer valer els seus drets pot posar-se en contacte directament amb Freemindtronic utilitzant les dades de contacte facilitades en aquesta Política de Privacitat.

D'acord amb la CCPA, l'exercici dels drets de protecció de dades personals (accés, supressió, oposició) no comportarà cap modificació, restricció o degradació dels serveis oferts per Freemindtronic.

ARTICLE 6 - SENSE PERFILS I EMPREMTES DIGITALS

6.1. Absència de perfils i decisions automatitzades

Freemindtronic no realitza cap perfil, seguiment del comportament ni presa de decisions automatitzada que afecti els usuaris.

- No es realitza cap anàlisi de l'activitat de l'usuari.
- No s'utilitza cap algorisme d'intel·ligència artificial per classificar els usuaris.
- No s'ha establert cap mecanisme per personalitzar els serveis basats en les dades dels usuaris.

6.2. Absència de empremta digital

L'empremta digital és una tècnica que consisteix a recopilar informació específica sobre el maquinari o programari d'un dispositiu, com ara l'adreça IP, el sistema operatiu, la resolució de pantalla i altres paràmetres, per tal de crear una empremta digital única de l'usuari. A diferència de les galetes, aquest mètode és difícil de detectar i bloquejar, cosa que planteja grans problemes de privadesa.

El desembre de 2024, **Google va anunciar que a partir del 16 de febrer de 2025 permetria als anunciants utilitzar l'empremta digital** per al seguiment dels usuaris, revertint la seva política del 2019 que prohibia la pràctica. La mesura va provocar crítiques de reguladors com **l'Oficina del Comissionat d'Informació (ICO) del Regne Unit,** que va qualificar el canvi d'"irresponsable" a causa de la reducció de l'elecció i el control que tenen les persones sobre la recopilació de la seva informació.

A **Freemindtronic** estem fermament compromesos amb el respecte a la privacitat dels nostres usuaris. Per tant, **no utilitzem cap forma d'empremta digital** en els nostres productes o serveis. **Google va anunciar el desembre de 2024 que permetria la presa d'empremtes digitals per als anunciants a partir del 16 de febrer de 2025** (font oficial - https://blog.google/products/ads-commerce/privacy-sandbox-fingerprinting-policy-change).

La mesura va generar preocupacions dels reguladors, inclosa **l'ICO del Regne Unit**. Freemindtronic rebutja aquestes pràctiques i garanteix que **no s'implementa** cap seguiment, identificació de dispositius o perfils de comportament.

Tots els sistemes informàtics de Freemindtronic estan **completament aïllats i independents** els uns dels altres. **No es registren, emmagatzemen o rastregen dades d'usuari** a través d'una operació exclusivament local i fora de línia. **L'ús de solucions d'encriptació de maquinari i autenticació NFC HSM** garanteix que no es pugui associar cap empremta digital als usuaris, fins i tot mitjançant l'ús de la tecnologia EviBITB de Freemindtronic.

Freemindtronic implementa una **estratègia avançada de ciberseguretat** per protegir-se dels atacs assistits per IA, el frau del CEO i altres robatoris d'identitat.

- Els **correus electrònics utilitzats per a la comunicació externa** són **adreces sandbox i correus electrònics sense resposta** per **reduir el risc de suplantació d'identitat i pesca**.
- Qualsevol obertura de fitxers adjunts està subjecta a una **estricta política de control** per tal **d'evitar qualsevol risc de fitxers maliciosos**.
- Cada **sol·licitud del client** es verifica sistemàticament mitjançant **un segon canal de comunicació** per confirmar la **seva autenticitat** (eliminació proactiva de dubtes).

Freemindtronic garanteix **que mai recopilarà, analitzarà o utilitzarà empremtes dactilars del dispositiu** mitjançant mètodes d'identificació indirecta (per exemple, resolució de pantalla, model de dispositiu, idioma del navegador).

ARTICLE 7 – COMPLIMENT DE LA NORMATIVA DE DOBLE ÚS

7.1. Normativa i autorització d'exportació

Freemindtronic aplica estrictament les regulacions per a la gestió i exportació de tecnologies de ciberseguretat, inclosos els **productes de xifratge classificats com a civils i militars de doble ús**.

Els productes **DataShielder NFC HSM** han rebut una **autorització d'importació a França del Principat d'Andorra**, validada el **7 de desembre de 2024** a través de l'empresa **AMG Pro**, d'acord amb el **Decret 2001-1192 de 13 de desembre de 2001**, modificat pel **Decret 2024-95 de 8 de febrer de 2024**.

Aquesta autorització es va obtenir després de la presentació de l'expedient a l'**ANSSI,** que, d'acord amb la seva missió de **verificar el compliment dels requisits normatius**, no es va negar en els terminis previstos per la legislació vigent.

Des del **7 de febrer de 2025**, els productes **DataShielder NFC HSM** també estan **autoritzats per a la seva reexportació** des de França als Estats membres de la Unió Europea, de conformitat amb el **Reglament (UE) 2021/821 de 20 de maig de 2021** sobre articles de doble ús.

7.2. Textos de referència

Aquesta autorització s'expedeix d'acord amb els següents textos:

- **Decret nº 2001-1192, de 13 de desembre de 2001**, modificat pel **Decret de 8 de febrer de 2024**, sobre el control de l'exportació i transferència de béns i tecnologies de doble ús.
- **Reglament (UE) 2021/821, de 20 de maig de 2021**, pel qual s'estableix un règim de control de les exportacions d'articles de doble ús.

7.3. Compromís d'auditoria

Freemindtronic es compromet a garantir **auditories de compliment periòdiques** per garantir **el compliment continu dels requisits legals i reglamentaris**. Aquestes auditories internes es realitzen periòdicament d'acord amb els requisits normatius vigents.

ARTICLE 8 – CERTIFICACIONS I AUDITORIES

8.1. Sense requisit de certificació al núvol

Freemindtronic no requereix certificacions **SOC 2** o **ISO 27001** específiques per a infraestructures al núvol, ja que **no s'utilitzen servidors remots** per al processament o emmagatzematge de dades.

Els productes estan dissenyats amb un enfocament **100% air-gapped**, garantint l'**aïllament total de les dades dels usuaris** de qualsevol infraestructura de xarxa externa. Aquesta arquitectura justifica **l'absència de certes auditories** normalment aplicades als sistemes connectats.

8.2. Auditoria de seguretat i control de qualitat

Aquest enfocament **s'aplica al llarg de la cadena de valor**, des del **disseny del producte** fins a la **fabricació**. Totes les auditories realitzades tenen com a objectiu garantir la **resiliència, la manipulació i l'eliminació de fuites de dades dels** sistemes de Freemindtronic.

A més de les auditories internes per garantir el compliment del producte, Freemindtronic aplica **controls millorats sobre la gestió de pagaments** i **la protecció de transaccions financeres**.

- El sistema de gestió comptable i financera està aïllat i no es pot validar cap transacció sense autenticació forta mitjançant DataShielder NFC HSM Auth i DataShielder MAuth, garantint una autenticació forta i eliminant el risc de frau.
- L'accés als comptes bancaris i als sistemes de pagament està estrictament limitat als accionistes autoritzats, sense relació de subordinació, per limitar els riscos interns de frau.

ARTICLE 9 – DELEGAT DE PROTECCIÓ DE DADES (DPO)

9.1. Nomenament del DPO

D'acord amb els requisits del **Reglament General de Protecció de Dades (RGPD – Reglament (UE) 2016/679)** i altres normatives aplicables, Freemindtronic ha nomenat un **Delegat de Protecció de Dades (DPO)** responsable de vetllar pel compliment de la protecció de dades personals per part de l'empresa.

El **DPO de Freemindtronic** és:

- **Nom:** Jacques Gascuel
- **Càrrec:** CEO i DPO de Freemindtronic SL
- **Contacte:** dpo [at] freemindtronic.com

9.2. Missions del DPO

El DPO de Freemindtronic duu a terme diverses missions essencials, entre elles:

- Assegurar-se que **el tractament de dades compleix** amb la normativa aplicable (**RGPD, CCPA, LGPD, etc.**).
- Informar i assessorar Freemindtronic sobre **les seves obligacions de protecció de dades**.
- Supervisar l'aplicació **de les polítiques de seguretat i protecció de dades** establertes.
- Respondre a les sol·licituds dels usuaris sobre **els seus drets (accés, rectificació, supressió, oposició, etc.)**.
- Contactar amb **les autoritats de protecció de dades**, inclosa l'**Agència Andorrana de Protecció de Dades** i les autoritats europees o internacionals pertinents.

9.3. Contacte i queixes

Qualsevol usuari que desitgi obtenir informació sobre **el tractament de les seves dades personals** o exercir els seus drets pot posar-se en contacte amb **el DPO de Freemindtronic** a la següent adreça:

- **Correu electrònic :** dpo [a] freemindtronic.com
- **Adreça postal:**
  Freemindtronic SLAv. Co-Prince de Gaulle, 13, Edifici Valira, Planta baixa, AD700 Escaldes – Engordany, Andorra

Si no es dóna resposta en el termini **de 30 dies**, l'usuari pot remetre l'assumpte directament **a l'Agència Andorrana de Protecció de Dades (APDA)** per **incompliment de l'obligació legal de respondre en el termini de 30 dies**.

ARTICLE 10 – REQUISITS ESPECÍFICS PER A PLATAFORMES DE DISTRIBUCIÓ

10.1. Google Play Console (Android)

Les aplicacions Freemindtronic no recopilen, emmagatzemen ni transmeten cap dada personal. Alguns permisos d'Android (per exemple, NFC, emmagatzematge, càmera) només s'utilitzen per habilitar la funcionalitat del producte i no s'exploten amb finalitats de tercers. No es comparteixen dades amb tercers i totes les operacions es realitzen localment al dispositiu de l'usuari, d'acord amb les polítiques de privadesa de Google Play.

10.1.1. Compliment de les polítiques de Google Play sobre dades sensibles i permisosLes aplicacions de Freemindtronic que requereixen accés a funcions sensibles d'Android (NFC, emmagatzematge, càmera, micròfon, GPS, SMS, RCS, MMS) compleixen els requisits següents:

- **Consentiment exprés** : no hi ha permisos habilitats per defecte. L'usuari ha d'habilitar-los manualment a través de la configuració del dispositiu.
- **Ús perfecte** : l'accés a aquestes funcions es **limita estrictament** a les necessitats essencials de l'aplicació i les dades generades romanen **exclusivament al dispositiu**.
- **Sense abús de permisos** : Freemindtronic mai demana accés a funcions superflues i respecta la política de transparència de Google Play.

10.1.2. Protecció de dades i emmagatzematge localTotes les dades romanen estrictament emmagatzemades al dispositiu de l'usuari i **només es pot accedir a la pròpia aplicació**. No s'emmagatzemen dades d'usuari en **servidors externs** ni es comparteixen amb **tercers**.

10.2 - Chrome Web Store (extensions de Chrome)

Les extensions de Freemindtronic no recopilen ni comparteixen cap dada d'usuari. Poden utilitzar localStorage per emmagatzemar temporalment la informació local necessària perquè l'extensió funcioni correctament.

No es realitza cap seguiment ocult, cap transmissió de dades a tercers i cap accés injustificat a cookies o historial de navegació.

10.2.1 Ús d'emmagatzematge localLes extensions de Freemindtronic utilitzen exclusivament l'API localStorage i Web Storage per emmagatzemar temporalment els paràmetres necessaris per al seu correcte funcionament.
Aquestes dades:

- **Mai es transmeten a servidors remots.**
- **Són accessibles només per a l'usuari i només en el context de l'extensió.**
- **Els paràmetres desats localment mitjançant localStorage i Web Storage no contenen dades personals o sensibles.**
- **Els usuaris poden esborrar manualment les dades locals desades mitjançant una opció "Suprimeix dades" integrada a l'extensió.**

10.3. Complements de Microsoft Store i Edge (Windows)

Les aplicacions i extensions de Freemindtronic compleixen els estàndards de privadesa de Microsoft.

Si una aplicació accedeix a fitxers locals (per exemple, emmagatzematge segur de claus de xifratge), aquests fitxers romanen aïllats i mai es comparteixen amb serveis de tercers.

Freemindtronic garanteix que no hi haurà empremtes digitals ni seguiment ocults, d'acord amb les polítiques de Microsoft Store.

10.3.1. Protecció d'accés a fitxers locals (Windows)
Algunes aplicacions Freemindtronic poden requerir accés a fitxers locals per **xifrar, protegir o autenticar dades** sensibles.
Aquests fitxers:

- **Mai es reenvien a un servidor remot.**
- **Romandre emmagatzemats i processats exclusivament en el dispositiu de l'usuari.**
- **Només són accessibles a les aplicacions instal·lades localment amb el consentiment de l'usuari.**

10.4. App Store d'Apple (macOS i iOS)

Les aplicacions de Freemindtronic no rastregen els usuaris, recopilen cap dada per a la creació de perfils publicitaris ni transmeten cap informació fora del dispositiu.

Si una aplicació accedeix a sensors iOS/macOS (per exemple, NFC, micròfon, GPS), aquest ús es limita estrictament a les funcions essencials i controlables per l'usuari.

Si s'utilitzen API de tercers (per exemple, pagament a través d'Apple Pay), el seu impacte en les dades de l'usuari compleix els requisits d'Apple i és totalment transparent per a l'usuari.

10.4.1. Compliment de la política de transparència de seguiment d'aplicacions (ATT)Freemindtronic garanteix **que no utilitza identificadors de publicitat** ni **eines de seguiment d'usuaris** amb finalitats de màrqueting o publicitat.
D'acord amb les directrius d'Apple:

- **No es recullen dades d'usuari per a la creació de perfils o la segmentació publicitària.**
- **No hi ha integració amb serveis de publicitat o anàlisi de tercers.**
- **No s'utilitza l'ID d'Apple (IDFA) per fer un seguiment de l'activitat dels usuaris en altres apps.**
- **Freemindtronic no recopila ni comparteix cap dada d'ubicació en segon pla o sense el consentiment explícit de l'usuari.**
- **Les aplicacions no transmeten cap dada fora del dispositiu tret que l'usuari realitzi voluntàriament una acció que requereixi l'intercanvi de dades.**

ARTICLE 11 – COMPLIMENT DE LA LEGISLACIÓ ANDORRANA DE PROTECCIÓ DE DADES

11.1. Aplicació de les lleis andorranes

Freemindtronic, com a empresa registrada al **Principat d'Andorra**, està subjecta a la normativa local **de protecció de dades**, que inclou:

- **Llei Orgànica 15/2003, de 18 de desembre**, de Protecció de Dades de Caràcter Personal
- **Llei qualificada 29/2021, de 28 d'octubre**, per la qual s'alinea Andorra amb els principis del **Reglament General de Protecció de Dades (RGPD – Reglament (UE) 2016/679)**

Aquestes lleis garanteixen un marc de **protecció de dades** equivalent als estàndards europeus, reconeguts com **a adequats** per la Unió Europea d'acord amb l'**article 45 del RGPD**.

A més de la normativa vigent, **Freemindtronic implementa mesures físiques i de programari avançades per garantir una protecció absoluta de les dades**. Això inclou **el xifratge complet dels mitjans digitals, l'autenticació multifactor NFC HSM i l'aïllament físic de les infraestructures de TI**.

Aquestes mesures garanteixen **el ple compliment dels articles 10 i 45 del RGPD**, garantint una protecció de dades equivalent als estàndards europeus més estrictes.

ARTICLE 12 – PRINCIPIS DE COMPLIMENT I SEGURETAT DE LES DADES

12.1. Privacitat des del disseny

Freemindtronic integra **la protecció de dades** en el **disseny del seu programari i serveis**, d'acord amb els principis de **privacitat des del disseny i privacitat per defecte**.

12.2. Sense emmagatzematge de dades

D'acord amb **l'enfocament Zero Trust & Zero Knowledge**, **Freemindtronic no emmagatzema ni processa cap dada personal**, excepte en el cas de subministrament voluntari per part de l'usuari (per exemple, formulari de contacte, suport tècnic).

12.3. Adopció de mesures de seguretat reforçades

Freemindtronic implementa mesures **de seguretat avançades** per garantir la **protecció de dades** i prevenir infraccions, com ara:

- **Xifrar sistemàticament** les comunicacions i transaccions dels usuaris mitjançant els seus sistemes patentats de xifratge de claus segmentades
- **Manca d'** identificadors únics que es puguin utilitzar per fer un seguiment de l'activitat dels usuaris
- **Auditabilitat interna periòdica** per garantir el compliment de la normativa vigent

Aquestes mesures s'ajusten a **l'article 10 de la Llei qualificada 29/2021** de protecció de dades personals a Andorra.

Freemindtronic aplica una estratègia integral de ciberseguretat que garanteix la protecció de les dades fins i tot en cas d'intrusió física a les instal·lacions:

Tots els sistemes informàtics (fixos, mòbils, servidors i dispositius d'emmagatzematge) estan totalment xifrats amb claus de ≥256 bits.

Tots els llocs connectats en línia o en una xarxa local utilitzen PassCypher NFC HSM i PassCypher HSM PGP amb TOTP/HOTP i/o DataShielder NFC HSM i DataShielder HSM PGP Cyber Defense.

No hi ha claus de xifratge emmagatzemades ni visibles a les eines de producció.

Els suports sensibles (memòries USB, discs durs) s'emmagatzemen en una caixa forta resistent al foc i a les intrusions.

Qualsevol extracció de dades sensibles és impossible, fins i tot en cas de robatori físic de servidors o exfiltració il·lícita d'arxius.

Aquestes mesures garanteixen que, fins i tot en cas d'intrusió a les instal·lacions de Freemindtronic, no es puguin explotar dades, fins i tot en cas d'una intrusió il·legal amb èxit.

12.4. Compromís amb la seguretat permanent

Freemindtronic situa **la protecció de dades** al centre de les seves activitats i es compromet a:

- **Millorar contínuament les seves mesures de seguretat** mantenint-se al dia amb les amenaces i les regulacions en evolució.

- **Adaptar els seus protocols de protecció** per garantir un nivell de seguretat d'acord amb els nous avenços tecnològics i les millors pràctiques de ciberseguretat.
- **Superviseu constantment** les amenaces cibernètiques, incloses les assistides per intel·ligència artificial (IA), per anticipar-vos a possibles intents d'intrusió i reforçar les defenses en conseqüència.

12.4.1 Protecció estratègica: Freemindtronic no revela públicament tots els detalls tècnics dels seus mecanismes de seguretat per no facilitar una anàlisi per part d'un atacant o intel·ligència artificial que busqui identificar una possible vulnerabilitat. No obstant això, totes les mesures implementades compleixen els estàndards **més estrictes** en matèria de ciberseguretat i protecció de dades.

12.5. Seguretat operativa i protecció de dades sensibles

Freemindtronic aplica un estricte model de seguretat que garanteix la **màxima protecció contra els riscos d'espionatge intern i extern**.

12.5.1 Aïllament de sistemes informàtics

- No hi ha connexions de xarxa entre sistemes interns i no es permet compartir fitxers o impressores.
- Cada sistema és completament independent, evitant vulnerabilitats relacionades amb connexions externes.

12.5.2 Transferències segures de dades sensibles

- Totes les transferències de fitxers sensibles es realitzen **exclusivament a través de** les unitats flash USB segures **EviKey NFC** de Freemindtronic.
- Aquestes claus tenen **autobloqueig automàtic** quan no s'utilitzen, evitant l'accés no autoritzat.
- A **la caixa negra de les claus NFC d'EviKey s'integra un registre de traçabilitat, que permet verificar cada desbloqueig i la seva geolocalització**.

12.5.3 Aïllament físic i seguretat de les eines de producció

- Els equips i eines de producció sensibles **mai estan connectats a Internet** i estan estrictament aïllats després del seu ús.
- Després del seu ús, aquestes eines es guarden **en una caixa forta especial resistent** al foc i a la intrusió física.

12.5.4 Generació i protecció de claus d'autenticació

- Les claus d'autenticació antifalsificació que també serveixen com a **claus segmentades** són generades **aleatòriament** per les eines de producció.
- Aquestes claus **no es mostren ni es guarden** a les eines de producció, garantint l'absència de qualsevol rastre utilitzable.

12.5.5 Control estricte d'accés i mitigació de riscos interns

- Només **dues persones autoritzades**, que també són **accionistes de l'empresa**, estan autoritzades a utilitzar les eines de producció.

- Aquesta restricció té com a objectiu **minimitzar els riscos associats a les relacions de subordinació** i garantir el control total sobre l'accés a infraestructures sensibles.

12.6. Control estricte d'accés i mitigació de riscos interns

12.6.1 Seguretat d'accés i xifratge sistemàtic

Freemindtronic aplica protocols avançats d'autenticació i xifratge per garantir que tots els accessos digitals i mitjans estiguin protegits contra qualsevol intent d'intrusió o robatori.

12.6.1.1 Protecció de l'accés a llocs i xarxesTots els sistemes de xarxa en línia i locals utilitzen només les següents tecnologies d'autenticació forta:

- 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 i/o DataShielder HSM PGP en versió Cyber Defense, combinant autenticació forta i xifratge d'accés avançat.
- Emuladors de teclat USB Bluetooth per assegurar l'entrada de dades sensibles eliminant qualsevol risc de registre de tecles.

12.6.1.2 Encriptació de dades i suports d'emmagatzematgeTots els sistemes informàtics (fixos, mòbils) i dispositius d'emmagatzematge que contenen dades sensibles estan xifrats amb claus d'encriptació iguals o superiors a 256 bits.

- Discs durs interns i externs totalment xifrats.
- Dispositius mòbils d'emmagatzematge i còpia de seguretat protegits per xifratge de maquinari i/o programari.

12.6.1.3 Resiliència a les intrusions físiques i digitalsTot està dissenyat per garantir que, en cas d'intrusió a les instal·lacions de Freemindtronic, robatori de suports digitals o extracció il·lícita de dades sensibles, cap dada sigui utilitzable o físicament accessible.

- Claus de xifratge segures en dispositius NFC HSM, evitant l'accés no autoritzat.
- Bloqueig automàtic de clau o bloqueig en cas d'intent de compromís amb la traçabilitat de la caixa negra.

12.6.1.4 Integració de productes mitjançant la tecnologia NFC EviKey

Els productes de Freemindtronic que incorporen la tecnologia **NFC EviKey** utilitzen exclusivament l' aplicació **Fullkey Plus** per a la seva gestió i seguretat. Aquesta tecnologia també està integrada en les següents solucions de ciberseguretat:

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

La integració d'EviKey NFC en aquestes solucions proporciona un control avançat d'accés als suports d'emmagatzematge i inclou les següents característiques:

- **Bloqueig automàtic quan està inactiu**
- **Gestió segura de claus**
- **Accediu a la traçabilitat a través d'una caixa negra**, accessible només sense contacte a través d'**un telèfon Android NFC**, gràcies a l' aplicació **Fullkey Plus**, **PassCypher NFC HSM** o **DataShielder NFC HSM**.

Freemindtronic no corre cap risc pel que fa a la seguretat i no es deixa sorprendre: aquí, **el sabater no és certament el pitjor calçat** ! 😉

Freemindtronic implementa **particions de seguretat estances**, evitant qualsevol forma d'espionatge, ja sigui **intern o extern**, i garantint la **màxima** protecció dels actius digitals i les dades crítiques.

12.6.1.4 – Protecció contra IA i atacs avançats :

Freemindtronic implementa tecnologies i protocols específics per protegir-se dels atacs assistits per IA, inclosos deepfakes i manipulacions d'àudio/vídeo destinades a comprometre la identitat digital d'executius i usuaris. Aquestes mesures inclouen la verificació millorada de les comunicacions i l'anàlisi multifactorial del comerç sensible.

12.7 – Gestió de violacions de dades :

En cas de compromís de maquinari o intent de violació de seguretat que afecti la infraestructura de Freemindtronic, els procediments de resposta a incidents es duen a terme de manera proactiva, independentment de l'absència d'un sistema de detecció automatitzat.

Freemindtronic reconeix que no és realista garantir una protecció absoluta contra un atacant determinat, fins i tot amb les millors mesures de seguretat del món. Per això, l'enfocament adoptat es basa en una estratègia **proactiva i preventiva**, integrant innovacions patentades internacionalment desenvolupades per anticipar-se a noves formes d'espionatge, especialment les assistides per **la intel·ligència artificial**.

Les solucions de ciberseguretat de Freemindtronic estan dissenyades per evitar l'explotació de dades, fins i tot en cas d'accés físic o digital no autoritzat. Aquest enfocament es basa en mecanismes avançats que inclouen l'autobloqueig de maquinari, el xifratge de claus segmentades, l'aïllament de la infraestructura i l'ús exclusiu de suports segurs com EviKey NFC, PassCypher NFC HSM i DataShielder NFC HSM.

En cas que un incident de seguretat afecti a un client o col·laborador, Freemindtronic es compromet a **informar-lo el més aviat possible**, d'acord amb els requisits de la normativa de protecció de dades aplicable.

ARTICLE 13 – DRETS DELS USUARIS SOTA LA LEGISLACIÓ ANDORRANA

D'acord amb **els articles 16 a 21 de la Llei 29/2021**, els usuaris tenen els següents drets, alineats amb l' **RGPD i la legislació andorrana** :

- **Dret d'accés** : Verificar quina informació s'ha facilitat voluntàriament i tractat.
- **Dret de rectificació** : Corregir les dades inexactes o incompletes.
- **Dret d'oposició** : Impugnar l'ús de les seves dades.
- **Dret a la supressió (dret a l'oblit):** Exigir la supressió definitiva de les seves dades.
- **Dret a la portabilitat** : Rebre les seves dades en un format llegible (nova obligació reforçada per la Llei 29/2021).
- **Dret a la restricció del tractament** : Restringir el tractament de determinada informació.

13.1. Temps de tramitació de les sol·licituds

Freemindtronic garanteix que qualsevol sol·licitud d'exercici de drets serà **tramitada en un termini màxim de 30 dies**, excepte en circumstàncies excepcionals que requereixin una **pròrroga justificada de fins a 60 dies**.

Les sol·licituds es poden enviar per correu electrònic a:
contact [at] freemindtronic.com o **dpo [at] freemindtronic.com**

ARTICLE 14 – RECURS EN CAS DE CONTROVÈRSIA

Si un usuari creu que **no s'han respectat els seus drets**, pot presentar una reclamació davant l'**Agència Andorrana de Protecció de Dades (APDA), l'autoritat de control competent a Andorra**.

14.1. Procediment de reclamacions

D'acord amb **l'article 25 de la Llei 29/2021**, qualsevol persona que consideri que el tractament de les seves dades s'ha dut a terme en **violació de la legislació aplicable** podrà:

- **Remetre l'assumpte a l'Agència Andorrana de Protecció de Dades (APDA)** per a una investigació administrativa.
  Contacte APDA : https://www.apda.ad
- **Interposar un recurs davant els tribunals competents d'Andorra** per obtenir la indemnització del dany sofert.

Freemindtronic es compromet a cooperar plenament amb les autoritats de protecció de dades en cas d'investigació.

ARTICLE 15 – CANVIS EN LA POLÍTICA DE PRIVACITAT

15.1. Compromís d'actualització

Freemindtronic es compromet a actualitzar aquesta política en cas de canvis legislatius o normatius que afectin la protecció de dades. Qualsevol canvi es publicarà explícitament al lloc web oficial de Freemindtronic.

15.2. Freqüència i transparència de les actualitzacions

Freemindtronic publica regularment actualitzacions del seu programari, aplicacions i extensions. Es manté una pàgina d'actualitzacions dedicada, que detalla explícitament:

- **Els canvis realitzats,**
- **Millores de seguretat,**
- **Qualsevol vulnerabilitat identificada i corregida.**

L'historial complet de versions del programari, les aplicacions i les extensions de Freemindtronic es pot trobar aquí: Historial de versions de Freemindtronic

15.3. Notificació als usuaris

Els usuaris que desitgin ser notificats d'actualitzacions per correu electrònic han de fer una sol·licitud expressa proporcionant la seva adreça de correu electrònic a Freemindtronic.

15.4. Informació en cas de canvis en les funcionalitats

En cas de canvis en les funcionalitats que impliquin el tractament de dades, Freemindtronic es compromet a informar els usuaris:

- **Per notificació a la web oficial,**
- **A través de les aplicacions corresponents.**

ARTICLE 16 – DADES DE CONTACTE

Freemindtronic SL
Correu electrònic : **contacte [at] freemindtronic.com**
Telèfon : **+376 804 500Política de cookies :** https://freemindtronic.com/cookie-policy/

Fi del document