INFORMATIVA SULLA PRIVACY – FREEMINDTRONIC SL

Sito web & Software – Versione e data del documento: V2.0 del 28/02/2025

ARTICOLO 1 – INTRODUZIONE

1.1. Identificazione del titolare del trattamento

La presente Informativa sulla privacy è emessa da **Freemindtronic SL,** una società a responsabilità limitata registrata ai sensi delle leggi del Principato di Andorra, con sede legale in:

Co-Prince de Gaulle, 13, Valira Building, piano terra, AD700 Escaldes – Engordany, Andorra.

Freemindtronic è responsabile del trattamento dei dati raccolti o elaborati attraverso l'uso del proprio sito Web ufficiale https://freemindtronic.com, nonché del software, delle applicazioni, delle estensioni e dei sistemi integrati.

1.2. Champ d'Application

La presente Informativa sulla privacy si applica a tutti i servizi, software, applicazioni, estensioni e sistemi integrati sviluppati e gestiti da Freemindtronic.

Non si applica a siti Web, servizi o piattaforme di terze parti accessibili tramite i servizi di Freemindtronic. Freemindtronic non è responsabile per le pratiche sulla privacy di questi servizi di terze parti.

1.3. Impegno: Zero Trust e Zero Knowledge

Freemindtronic aderisce a un rigoroso framework **Zero Trust & Zero Knowledge**, garantendo che i dati degli utenti non vengano acceduti, archiviati o condivisi affatto.

Tutti i software, le applicazioni, le estensioni e i sistemi integrati sviluppati da Freemindtronic funzionano **senza un server remoto, un database centralizzato, la creazione di un account utente, l'identificazione dell'utente e la trasmissione dei dati**.

Tutte le funzionalità di Freemindtronic garantiscono che i dati dell'utente non vengano memorizzati o trasmessi a server remoti. Tutti i trattamenti vengono effettuati esclusivamente localmente sul dispositivo dell'utente, senza interazione con un'infrastruttura esterna.

1.4. Conformità alle normative

- Freemindtronic è conforme alle più severe normative internazionali in materia di protezione dei dati e sicurezza informatica, tra cui:
- Regolamento generale sulla protezione dei dati (GDPR – Regolamento (UE) 2016/679)
- Legge sulla resilienza operativa digitale (DORA – Règlement (UE) 2022/2554)
- Direttiva NIS2 (direttiva (UE) 2022/2555) sulla cibersicurezza delle infrastrutture critiche
- Legge sulla privacy dei consumatori della California (SCCA – USA, Cal. Civ. Code § 1798.100 e seguenti)
- Legge generale sulla protezione dei dati (LGPD – Brésil, legge n. 13.709/2018)
- Legge 15/2003 sulla protezione dei dati personali in Andorra, modificata dalla Legge Qualificata 29/2021
- Regolamento (UE) 2021/821 del Consiglio, del 20 maggio 2021, relativo al controllo delle esportazioni di prodotti a duplice uso
- Standard ISO/IEC 27001 e best practice di sicurezza NIST (National Institute of Standards and Technology, USA)

1.5. DefinizioniNella presente informativa, i seguenti termini sono definiti come segue:

- **Dati personali** : qualsiasi informazione riguardante, direttamente o indirettamente, una persona fisica identificata o identificabile, in particolare con riferimento a un identificatore come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o a uno o più elementi specifici della sua identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale.
- **Dati sensibili** : qualsiasi informazione la cui divulgazione non autorizzata potrebbe comportare un rischio elevato per i diritti e le libertà degli interessati. Ciò include, a titolo esemplificativo ma non esaustivo:
    - Identificatori univoci (nomi utente, password, codici di autenticazione).
    - Chiavi di crittografia e autenticazione.
    - Informazioni di pagamento e coordinate bancarie.
    - Dati riservati di clienti e partner (strategie commerciali, brevetti, documenti protetti da segreti commerciali).
    - Qualsiasi dato personale che rientra nelle categorie speciali del GDPR (origine etnica, opinioni politiche, convinzioni religiose, salute, dati biometrici, vita sessuale).
- **Per trattamento** si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, limitazione, cancellazione o distruzione.
- **Titolare del trattamento** : la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
- **Responsabile del trattamento** : la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
- **Consenso** : qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale quest'ultimo acconsente, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano.
- **Pseudonimizzazione** : trattamento dei dati personali in modo tale che non possano più essere attribuiti a una determinata persona fisica senza ulteriori informazioni, che devono essere mantenute separate e protette da misure tecniche e organizzative adeguate.
- **Anonimizzazione** : trasformazione irreversibile dei dati personali in modo tale che non sia più possibile identificare direttamente o indirettamente l'interessato.
- **Violazione dei dati personali** : qualsiasi violazione della sicurezza che provochi accidentalmente o illegalmente la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali. Ciò include l'accesso non autorizzato a dati di accesso, password, chiavi di crittografia o altri dati sensibili protetti.

ARTICOLO 2 – RACCOLTA E TRATTAMENTO DEI DATI

2.1. Mancanza di una raccolta sistematica dei dati

Freemindtronic non raccoglie, archivia, condivide o vende dati personali o tecnici degli utenti, tranne nel caso di interazione diretta, tra cui:

- Un ordine tramite piattaforme ufficiali.
- Una richiesta di contatto relativa al servizio clienti o a una partnership ufficiale.

I dati vengono elaborati solo nell'ambito dell'esecuzione del contratto o del rapporto commerciale e non vengono mai utilizzati per altri scopi.

2.2. Dati che possono essere raccolti

Se un utente fornisce volontariamente informazioni, vengono trattati solo i dati strettamente necessari:

- Identità (cognome, nome)
- Dati di contatto (e-mail, telefono, indirizzo di fatturazione e consegna)
- Informazioni professionali
- Contenuti inviati volontariamente

I dati transazionali sono utilizzati esclusivamente per la gestione degli ordini e la loro consegna, senza trasmissione a terzi se non per obblighi di legge (fiscali e contabili).

2.2.1 – Dati memorizzati localmente sull'estensione o sull'applicazioneAlcune applicazioni ed estensioni Freemindtronic possono utilizzare localStorage o l'API Web Storage per memorizzare temporaneamente le impostazioni locali sul dispositivo dell'utente. Questi dati non vengono mai trasmessi a server remoti e sono accessibili solo all'interno del software utilizzato.

2.3. Archiviazione e sicurezza dei dati

Freemindtronic applica i più elevati standard di sicurezza, conformi alle normative **GDPR, DORA, NIS2, ISO/IEC 27001 e NIST**.

- **Archiviazione offline sicura** : i dati sono conservati su supporti crittografati a cui è possibile accedere solo tramite unità flash USB sicure EviKey NFC e/o supporti di archiviazione crittografati e/o dati crittografati.
- **Zero Trust & Zero Knowledge** : Mancanza di server remoti e database centralizzati per archiviare e/o gestire i dati sensibili per tutti i prodotti Freemindtronic.
- **Maggiore sicurezza per le comunicazioni sensibili**: lo scambio di dati sensibili avviene esclusivamente tramite strumenti **DataShielder** o un protocollo sicuro definito dal cliente.
- **Alternativa imposta se necessario** : se il servizio clienti non garantisce un livello di sicurezza sufficiente, Freemindtronic offre **DataShielder** come unico canale sicuro.

2.4. Protezione dei dati classificati e degli ambienti sensibili

Le soluzioni Freemindtronic, identificate come prodotti a duplice uso, civili e militari, sono progettate per proteggere le informazioni critiche e includono:

- **Isolamento fisico e partizionamento** : nessun dato viene archiviato su un server remoto.
- **Autenticazione forte** : NFC HSM e crittografia a chiave segmentata brevettata. L'uso della crittografia asimmetrica RSA-4096 consente di condividere in modo sicuro le chiavi CBC AES-256 tra i dispositivi HSM NFC, anche in remoto, senza trasmissione su infrastrutture centralizzate. Questo meccanismo elimina il rischio di esfiltrazione delle chiavi e fornisce una protezione avanzata per gli exchange crittografati.
- **Crittografia end-to-end:** AES-256 CBC, RSA-4096, PGP - Tutti i sistemi di crittografia simmetrica sicura sono ottenuti tramite chiavi segmentate e sistemi di controllo degli accessi

brevettati a livello internazionale. Questa architettura rende la crittografia resistente agli attacchi quantistici, garantendo la protezione a lungo termine dei dati sensibili.
- **Registrazione decentralizzata** : scatola nera locale accessibile solo in NFC da un amministratore autorizzato.
- **Stress test e sicurezza informatica proattiva** : valutazioni regolari contro attacchi APT, spionaggio industriale e minacce informatiche avanzate.

Se un'estensione o un'applicazione Freemindtronic accede a file locali su un dispositivo Windows o Mac (ad esempio, per archiviare chiavi di crittografia o proteggere i file), questi file vengono elaborati esclusivamente localmente e non sono mai accessibili da terze parti. L'utente mantiene il pieno controllo sui propri dati e non vengono condivisi con altri servizi.

2.5. Archiviazione, cancellazione e conservazione dei dati del cliente

- I dati forniti tramite un modulo di **contatto** vengono utilizzati solo per rispondere alla richiesta e cancellati immediatamente dopo l'elaborazione.
- I dati dei clienti risultanti dalle transazioni vengono conservati solo per il periodo legale necessario, in conformità con le normative applicabili nelle seguenti giurisdizioni:
    - **Andorra: Legge Qualificata 29/2021 – conservazione dei documenti fiscali per 5 anni**
    - **Unione Europea: Articolo 6 della Direttiva 2011/83/UE sulla protezione dei consumatori – conservazione dei dati delle transazioni per un massimo di 10 anni a seconda dei requisiti contabili locali**
    - **Francia: articolo L123-22 del Codice di commercio francese – conservazione obbligatoria dei documenti contabili per 10 anni**
    - **U.S.A.: Irs Publication 583 – 3-7 anni di conservazione dei dati sulle transazioni**
- **Non vengono memorizzati dati bancari:** le transazioni vengono elaborate tramite **fornitori terzi sicuri** (ad es. PayPal).

2.6. Trasferimenti internazionali di dati

Freemindtronic non trasferisce alcun dato al di fuori del SEE a meno che non venga applicato un quadro giuridico adeguato (**Clausole contrattuali standard - SCC**).

2.7. Procedura per violazione dei dati

In conformità con gli articoli 33 e 34 del **GDPR** e della **Legge Qualificata 29/2021**, Freemindtronic applica una **risposta proattiva** in caso di incidente:

- **Contenimento immediato** e **analisi dell'impatto**.
- **Notifica entro 72 ore** all'Agenzia per la protezione dei dati di Andorra (APDA), se necessario.
- **Informare gli utenti interessati** se viene identificato un rischio elevato.
- **Audit post-incidente** per rafforzare le misure di protezione.

2.8. Resilienza informatica e protezione contro catastrofi e attacchi informatici

Freemindtronic garantisce **l'integrità e la disponibilità** dei dati anche in caso di guasto, furto, disastro o massiccio attacco informatico.

2.8.1. Crittografia e backup sicuro

- **Crittografia avanzata** : AES-256 CBC, AES-256 CBC PGP, BitLocker con chiavi memorizzate **su NFC HSM PassCypher**.
- **Separazione di chiavi e dati**: le chiavi di **decrittografia** non vengono mai memorizzate sullo stesso supporto dei dati. Le chiavi di crittografia CBC AES-256 sono altamente sicure, condivisibili tramite NFC HSM DataShielder, funzionano senza contatto, senza server e senza database. Questo meccanismo garantisce la trasmissione sicura delle chiavi, anche da remoto, eliminando qualsiasi rischio di intercettazione da parte di terzi.
- **Backup crittografati e ridondanti**: dati replicati **su più supporti offline** e sicuri.

2.8.2. Protezione rafforzata contro gli attacchi informatici

- **Ransomware e crittografia eccessiva** : i backup offline crittografati e le chiavi esternalizzate fisicamente impediscono la manomissione o il ripristino fraudolento.
- **Attacchi informatici avanzati (APT, Zero-Day, Spionaggio):** l 'architettura **Zero Trust e Zero Knowledge** e la **separazione delle chiavi fisiche** impediscono l'esfiltrazione. L'architettura di sicurezza di Freemindtronic, che incorpora sistemi di crittografia segmentati brevettati e controllo degli accessi basato su hardware, garantisce che nessuna chiave privata o dato crittografato possa essere esfiltrato, anche in caso di vincoli fisici o logici. La combinazione della crittografia AES-256 CBC e RSA-4096 aumenta la resilienza agli attacchi avanzati, compresi quelli assistiti dall'intelligenza artificiale.
- **Resilienza senza cloud** : **nessuna dipendenza dai server remoti**, eliminando il rischio di attacchi centralizzati.

2.8.3. Resilienza ai disastri fisici e alle perdite accidentali

I protocolli di Freemindtronic garantiscono sempre l'accesso ai dati criptati con le loro chiavi, anche in caso di:

- **Furto o smarrimento** di supporti crittografati: senza **chiavi esternalizzate**, i dati rimangono inutilizzabili.
- **Distruzione accidentale o disastro naturale** : **i backup duplicati** garantiscono il recupero dei dati sensibili.
- **Isolamento geografico dei backup**: i supporti crittografati vengono conservati in una varietà di posizioni sicure, prevenendo la compromissione totale.

2.9. Accordi di non divulgazione (NDA) e riservatezza degli scambi

Tutti i rapporti commerciali con Freemindtronic che comportano lo scambio di informazioni sensibili o riservate sono regolarmente coperti da un accordo di **non divulgazione (NDA).**

- **Applicazione rigorosa** : tutte le informazioni scambiate nell'ambito di partnership, collaborazioni tecniche o discussioni commerciali sono protette da clausole di riservatezza legalmente vincolanti. Tutti i documenti sensibili, crittografati o meno, scambiati con clienti e partner vengono sistematicamente firmati digitalmente tramite la funzione integrata in DataShielder HSM PGP. Questa firma digitale garantisce l'integrità e l'autenticità dei documenti, assicurando che non siano stati apportati danneggiamenti o alterazioni dopo la loro emissione. Inoltre, le comunicazioni e-mail che coinvolgono informazioni sensibili sono sempre protette tramite PGP, impedendo l'intercettazione o la manomissione dei messaggi.

- **Ambito di applicazione dell'NDA** : L'NDA copre **documenti, comunicazioni, scambi tecnici, innovazioni, dati interni**, nonché qualsiasi informazione riservata trasmessa da Freemindtronic o ricevuta da un partner.
- **Sanzioni per violazioni** : qualsiasi divulgazione non autorizzata di informazioni riservate è soggetta a **sanzioni contrattuali e legali** che possono includere azioni legali per violazione della riservatezza e dei segreti commerciali.
- **Durata della protezione** : Gli obblighi di non divulgazione rimangono in vigore **anche dopo la fine del rapporto contrattuale**, secondo il termine definito in ciascun accordo.

Questa clausola rafforza l'impegno di Freemindtronic a proteggere tutte le informazioni critiche scambiate nel corso della sua attività, garantendo un quadro giuridico rigoroso contro qualsiasi fuga di notizie o compromissione.

ARTICOLO 3 – UTILIZZO DEI SENSORI E ACCESSO AI DATI DI LOCALIZZAZIONE

Alcuni software, applicazioni o estensioni **Freemindtronic** potrebbero richiedere l'accesso ai sensori sui dispositivi degli utenti.

3.1 Questi sensori includono:

- **GPS** (posizione precisa)
- **Wi-Fi e reti mobili** (posizione approssimativa)
- **Bluetooth** (rilevamento locale senza trasmissione esterna)
- **Dati biometrici** (impronta digitale, riconoscimento facciale)
- **Microfono e fotocamera** (solo con esplicito consenso)
- **Sensori ambientali** (accelerometro, giroscopio, sensori di prossimità, luminosità)
- **Moduli di sicurezza** (NFC, HSM, HSM, PGP)

3.2 Tutti i dati generati da questi sensori:

- **Rimangono esclusivamente sul dispositivo dell'utente** e non vengono trasmessi in nessun caso a un server remoto o a un servizio di terze parti.
- **Non sono soggetti a archiviazione esterna o remota**.
- **Sono accessibili solo con il consenso esplicito dell'utente**, in particolare per i sensori sensibili come microfono e fotocamera.
- **Può essere gestito dall'utente**, che può modificare o revocare le autorizzazioni concesse in qualsiasi momento attraverso le impostazioni del proprio dispositivo.

I sensori dei dispositivi (fotocamera, microfono, NFC, GPS, Wi-Fi, Bluetooth) vengono utilizzati solo localmente e non trasmettono mai dati a server esterni, terze parti o altri servizi Freemindtronic. L'utente può controllare e disabilitare questo accesso tramite le impostazioni del proprio dispositivo.

3.4 Garantire che i dati dei sensori non vengano utilizzati per scopi di tracciamento comportamentale

Freemindtronic garantisce che **i dati raccolti tramite i sensori del dispositivo non vengano mai utilizzati per il tracciamento comportamentale, la pubblicità mirata o la profilazione degli utenti**.

L'accesso ai sensori è strettamente limitato alle funzionalità essenziali del software e solo dopo aver ottenuto il consenso esplicito dell'utente.

Sulla base di questi dati non viene effettuata alcuna analisi dei modelli di utilizzo e non vengono memorizzati o trasmessi a terzi.

ARTICOLO 4 – RISPETTO DELLE PIATTAFORME DI DISTRIBUZIONE

I software, le applicazioni e le estensioni sviluppate da **Freemindtronic** sono conformi ai requisiti delle seguenti piattaforme:

- **Google Play Console** (applicazioni Android)
- **Chrome Web Store** (estensioni del browser)
- **Componenti aggiuntivi di Microsoft Store ed Edge** (app di Windows ed estensioni del browser)
- **Apple macOS e iOS** (app distribuite su App Store)

Freemindtronic si impegna ad aderire alle linee guida sulla **sicurezza e sulla privacy** imposte da queste piattaforme.

- **L'architettura Zero Trust & Zero Knowledge è garantita** in modo che nessun dato dell'utente venga raccolto, trasmesso o archiviato al di fuori del dispositivo dell'utente.
- **Non vi è alcuna integrazione con servizi di terze parti** per mitigare i rischi associati al tracciamento o alla raccolta di dati personali.
- **I requisiti di ciascuna piattaforma vengono rivisti periodicamente** per garantire la continua conformità alle modifiche delle normative applicabili.

SEZIONE 5 – CLAUSOLA DI NON DISCRIMINAZIONE (CONFORMITÀ CCPA)

In conformità con le disposizioni del **California Consumer Privacy Act (CCPA), Freemindtronic garantisce che gli utenti non saranno discriminati** nell'esercizio dei loro diritti in materia di protezione dei dati personali.

Nessuna restrizione o limitazione sarà applicata agli utenti che intendano esercitare i propri diritti, in particolare per quanto riguarda:

- Accesso ai propri dati personali.
- Rettifica di informazioni inesatte o incomplete.
- Cancellazione dei dati forniti volontariamente.
- Opporsi o limitare il trattamento dei propri dati.

Freemindtronic si impegna a non applicare costi aggiuntivi, o modifiche nell'accesso alle funzionalità, in risposta a una richiesta di esercizio dei diritti da parte di un utente.

Qualsiasi utente che desideri far valere i propri diritti può contattare direttamente Freemindtronic utilizzando i dettagli di contatto forniti nella presente Informativa sulla privacy.

In conformità con il CCPA, l'esercizio dei diritti di protezione dei dati personali (accesso, cancellazione, opposizione) non comporterà alcuna modifica, restrizione o degrado dei servizi offerti da Freemindtronic.

ARTICOLO 6 – DIVIETO DI PROFILAZIONE E RILEVAMENTO DELLE IMPRONTE DIGITALI

6.1. Assenza di profilazione e decisioni automatizzate

Freemindtronic non effettua alcuna profilazione, tracciamento comportamentale o processo decisionale automatizzato che interessa gli utenti.

- Non viene eseguita alcuna analisi dell'attività dell'utente.
- Nessun algoritmo di intelligenza artificiale viene utilizzato per classificare gli utenti.
- Non viene messo in atto alcun meccanismo per personalizzare i servizi in base ai dati degli utenti.

6.2. Assenza de Impronte digitali

Il fingerprinting è una tecnica che prevede la raccolta di informazioni specifiche sull'hardware o sul software di un dispositivo, come l'indirizzo IP, il sistema operativo, la risoluzione dello schermo e altri parametri, al fine di creare un'impronta digitale univoca dell'utente. A differenza dei cookie, questo metodo è difficile da rilevare e bloccare, il che pone gravi problemi di privacy.

Nel dicembre 2024, **Google ha annunciato che a partire dal 16 febbraio 2025 avrebbe consentito agli inserzionisti di utilizzare le impronte digitali** per il tracciamento degli utenti, invertendo la sua politica del 2019 che vietava la pratica. La mossa ha suscitato critiche da parte di autorità di regolamentazione come **l'Information Commissioner's Office (ICO) del Regno Unito,** che ha definito il cambiamento "irresponsabile" a causa della riduzione della scelta e del controllo che gli individui hanno sulla raccolta delle loro informazioni.

Noi di **Freemindtronic** ci impegniamo fortemente a rispettare la privacy dei nostri utenti. Pertanto, **non utilizziamo alcuna forma di rilevamento delle impronte digitali** nei nostri prodotti o servizi. **Google ha annunciato nel dicembre 2024 che avrebbe consentito il rilevamento delle impronte digitali per gli inserzionisti a partire dal 16 febbraio 2025** (fonte ufficiale - https://blog.google/products/ads-commerce/privacy-sandbox-fingerprinting-policy-change).

La mossa ha sollevato preoccupazioni da parte delle autorità di regolamentazione, tra cui **l'ICO del Regno Unito**. Freemindtronic rifiuta queste pratiche e garantisce che **non venga implementato** alcun tracciamento, identificazione del dispositivo o profilazione comportamentale.

Tutti i sistemi IT Freemindtronic sono **completamente isolati e indipendenti** l'uno dall'altro. **Nessun dato dell'utente viene registrato, archiviato o tracciato** attraverso un'operazione esclusivamente locale e offline. **L'utilizzo di soluzioni di crittografia hardware e autenticazione NFC HSM** garantisce che nessuna impronta digitale possa essere associata agli utenti, anche attraverso l'uso della tecnologia EviBITB di Freemindtronic.

Freemindtronic implementa una **strategia avanzata di sicurezza informatica** per proteggersi dagli attacchi assistiti dall'intelligenza artificiale, dalle frodi dei CEO e da altri furti di identità.

- Le **e-mail utilizzate per la comunicazione esterna** sono **indirizzi sandbox ed e-mail di mancata risposta** per **ridurre il rischio di spoofing e phishing**.
- Qualsiasi apertura di allegati è soggetta a una **rigorosa politica di controllo** al fine di evitare **qualsiasi rischio di file dannosi**.

- Ogni **richiesta del cliente** viene sistematicamente verificata da **un secondo canale di comunicazione** per **confermarne l'autenticità** (rimozione proattiva dei dubbi).

Freemindtronic garantisce che **non raccoglierà, analizzerà o utilizzerà mai le impronte digitali del dispositivo** tramite metodi di identificazione indiretta (ad es. risoluzione dello schermo, modello del dispositivo, lingua del browser).

ARTICOLO 7 – RISPETTO DELLA NORMATIVA SUI PRODOTTI A DUPLICE USO

7.1. Norme e autorizzazioni all'esportazione

Freemindtronic applica rigorosamente le normative per la gestione e l'esportazione delle tecnologie di sicurezza informatica, anche per i **prodotti di crittografia classificati come a duplice uso civile e militare**.

I prodotti DataShielder NFC HSM hanno ricevuto un'**autorizzazione all'importazione in Francia dal Principato di Andorra**, convalidata **il 7 dicembre 2024** tramite la società **AMG Pro**, in conformità con il **decreto n. 2001-1192 del 13 dicembre 2001**, modificato dal **decreto n. 2024-95 dell'8 febbraio 2024**.

Tale autorizzazione è stata ottenuta dopo la presentazione del fascicolo all'**ANSSI**, la quale, in conformità alla propria missione di verifica del **rispetto dei requisiti normativi**, non ha rifiutato entro i termini previsti dalla normativa vigente.

Dal **7 febbraio 2025**, i prodotti **DataShielder NFC HSM** sono **autorizzati anche per la riesportazione** dalla Francia agli Stati membri dell'Unione Europea, in conformità con il **Regolamento (UE) 2021/821 del 20 maggio 2021** sugli articoli a duplice uso.

7.2. Testi di riferimento

La presente autorizzazione è rilasciata ai sensi dei seguenti disposti:

- **Decreto n. 2001-1192 del 13 dicembre 2001**, modificato dal **decreto dell'8 febbraio 2024**, relativo al controllo dell'esportazione e del trasferimento di beni e tecnologie a duplice uso.
- **Regolamento (UE) 2021/821, del 20 maggio 2021**, che istituisce un regime di controllo delle esportazioni di prodotti a duplice uso.

7.3. Impegno di audit

Freemindtronic si impegna a garantire **controlli di conformità regolari** per garantire **il rispetto continuo dei requisiti legali e normativi**. Tali audit interni sono effettuati periodicamente in conformità ai requisiti normativi vigenti.

ARTICOLO 8 – CERTIFICAZIONI E AUDIT

8.1. Nessun requisito di certificazione cloud

Freemindtronic non richiede certificazioni **SOC 2** o **ISO 27001** specifiche per le infrastrutture cloud, poiché **non vengono utilizzati server remoti** per l'elaborazione o l'archiviazione dei dati.

I prodotti sono progettati con un approccio **air-gapped al 100%,** garantendo **il totale isolamento dei dati dell'utente** da qualsiasi infrastruttura di rete esterna. Questa architettura giustifica **l'assenza di alcuni audit** normalmente applicati ai sistemi connessi.

8.2. Audit di sicurezza e controllo di qualità

Questo approccio **viene applicato in tutta la catena del valore**, dalla **progettazione del prodotto** alla **produzione**. Tutti gli audit condotti hanno lo scopo di garantire la **resilienza, la sicurezza e l'assenza di perdite di dati dei** sistemi Freemindtronic.

Oltre agli audit interni per garantire la conformità dei prodotti, Freemindtronic applica **controlli avanzati sulla gestione dei pagamenti** e sulla **protezione delle transazioni finanziarie**.

- Il sistema di gestione contabile e finanziaria è isolato e nessuna transazione può essere convalidata senza un'autenticazione forte tramite DataShielder NFC HSM Auth e DataShielder MAuth, garantendo un'autenticazione forte ed eliminando il rischio di frodi.
- L'accesso ai conti bancari e ai sistemi di pagamento è strettamente limitato agli azionisti autorizzati, senza un rapporto di subordinazione, per limitare i rischi interni di frode.

ARTICOLO 9 – RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

9.1. Nomina del DPO

In conformità con i requisiti del **Regolamento generale sulla protezione dei dati (GDPR – Regolamento (UE) 2016/679)** e di altre normative applicabili, Freemindtronic ha nominato un **Responsabile della protezione dei dati (DPO)** responsabile di garantire il rispetto da parte dell'azienda della protezione dei dati personali.

Il **DPO di Freemindtronic** è:

- **Nome:** Jacques Gascuel
- **Posizione:** CEO e DPO di Freemindtronic SL
- **Contatto :** dpo [at] freemindtronic.com

9.2. Missioni del DPO

Il DPO di Freemindtronic svolge diverse missioni essenziali, tra cui:

- Garantire che **il trattamento dei dati sia conforme** alle normative applicabili (**GDPR, CCPA, LGPD, ecc.**).
- Informare e consigliare Freemindtronic sui **suoi obblighi in materia di protezione dei dati**.
- Monitorare l'applicazione **delle politiche di sicurezza e protezione dei dati** messe in atto.
- Rispondere alle richieste degli utenti in merito ai **loro diritti (accesso, rettifica, cancellazione, opposizione, ecc.)**.
- Collaborare con **le autorità per la protezione dei dati**, tra cui l'Agenzia per la protezione dei **dati di Andorra** e le autorità europee o internazionali competenti.

9.3. Contatti e reclami

L'utente che desidera ottenere informazioni sulla **gestione dei propri dati personali** o esercitare i propri diritti può contattare **il DPO di Freemindtronic** al seguente indirizzo:

- **E-mail :** dpo [at] freemindtronic.com
- **Indirizzo postale:**
  Freemindtronic SLAv. Co-Prince de Gaulle, 13, Valira Building, piano terra, AD700 Escaldes – Engordany, Andorra

In caso di mancata risposta entro **30 giorni**, l'utente può rivolgersi direttamente all'**Agenzia per la protezione dei dati di Andorra (APDA)** per **il mancato rispetto dell'obbligo legale di rispondere entro 30 giorni**.

ARTICOLO 10 – REQUISITI SPECIFICI PER LE PIATTAFORME DI DISTRIBUZIONE

10.1. Google Play Console (Android)

Le app Freemindtronic non raccolgono, memorizzano o trasmettono alcun dato personale. Alcune autorizzazioni Android (ad es. NFC, archiviazione, fotocamera) vengono utilizzate solo per abilitare la funzionalità del prodotto e non vengono sfruttate per scopi di terze parti. Nessun dato viene condiviso con terze parti e tutte le operazioni vengono eseguite localmente sul dispositivo dell'utente, in conformità con le norme sulla privacy di Google Play.

10.1.1. Conformità alle norme di Google Play relative a dati sensibili e autorizzazioniLe applicazioni Freemindtronic che richiedono l'accesso a funzioni Android sensibili (NFC, archiviazione, fotocamera, microfono, GPS, SMS, RCS, MMS) sono conformi ai seguenti requisiti:

- **Consenso esplicito** : per impostazione predefinita non sono abilitate le autorizzazioni. L'utente deve abilitarli manualmente tramite le impostazioni del dispositivo.
- **Utilizzo senza interruzioni** : l'accesso a queste funzionalità è **strettamente limitato** alle esigenze essenziali dell'app e i dati generati rimangono **esclusivamente sul dispositivo**.
- **Nessun abuso di autorizzazioni** : Freemindtronic non chiede mai l'accesso a funzionalità superflue e rispetta la politica di trasparenza di Google Play.

10.1.2. Protezione dei dati e archiviazione localeTutti i dati rimangono rigorosamente memorizzati sul dispositivo dell'utente e **sono accessibili solo dall'app stessa**. Nessun dato dell'utente viene memorizzato su **server esterni** o condiviso con **terze parti**.

10.2 – Chrome Web Store (estensioni di Chrome)

Le estensioni Freemindtronic non raccolgono né condividono alcun dato dell'utente. Possono utilizzare localStorage per archiviare temporaneamente le informazioni locali necessarie per il corretto funzionamento dell'estensione.

Non viene effettuato alcun tracciamento nascosto, nessuna trasmissione di dati a terzi e nessun accesso ingiustificato ai cookie o alla cronologia di navigazione.

10.2.1 Utilizzo dell'archiviazione localeLe estensioni Freemindtronic utilizzano esclusivamente l'API localStorage e Web Storage per memorizzare temporaneamente le impostazioni necessarie per il loro corretto funzionamento.
Questi dati:

- **Non vengono mai trasmessi a server remoti.**
- **Sono accessibili solo all'utente e solo nel contesto dell'estensione.**
- **Le impostazioni salvate localmente tramite localStorage e Web Storage non contengono dati personali o sensibili.**
- **Gli utenti possono cancellare manualmente i dati locali salvati tramite un'opzione "Elimina dati" integrata nell'estensione.**

10.3. Componenti aggiuntivi di Microsoft Store e Edge (Windows)

Le app e le estensioni di Freemindtronic sono conformi agli standard sulla privacy di Microsoft.

Se un'applicazione accede ai file locali (ad esempio, l'archiviazione sicura delle chiavi di crittografia), questi file rimangono isolati e non vengono mai condivisi con servizi di terze parti.

Freemindtronic garantisce che non ci saranno impronte digitali o tracciamenti nascosti, in conformità con le politiche di Microsoft Store.

10.3.1. Protezione dell'accesso ai file locali (Windows)
Alcune applicazioni Freemindtronic potrebbero richiedere l'accesso ai file locali per **crittografare, proteggere o autenticare i dati sensibili**.
Questi file:

- **Non vengono mai inoltrati a un server remoto.**
- **Rimangono memorizzati ed elaborati esclusivamente sul dispositivo dell'utente.**
- **Sono accessibili solo alle applicazioni installate localmente con il consenso dell'utente.**

10.4. App Store di Apple (macOS e iOS)

Le app Freemindtronic non tracciano gli utenti, non raccolgono dati per la profilazione pubblicitaria e non trasmettono alcuna informazione al di fuori del dispositivo.

Se un'app accede a sensori iOS/macOS (ad es. NFC, microfono, GPS), questo utilizzo è strettamente limitato alle funzioni essenziali e controllabili dall'utente.

Se vengono utilizzate API di terze parti (ad es. pagamento tramite Apple Pay), il loro impatto sui dati dell'utente è conforme ai requisiti di Apple ed è completamente trasparente per l'utente.

10.4.1. Conformità alla politica di trasparenza del tracciamento delle app (ATT)Freemindtronic garantisce **di non utilizzare ID pubblicitari** o **strumenti di tracciamento degli utenti** per scopi di marketing o pubblicitari.
In conformità con le linee guida Apple:

- **Nessun dato dell'utente viene raccolto per la profilazione o il targeting pubblicitario.**
- **Non vi è alcuna integrazione con servizi pubblicitari o di analisi di terze parti.**
- **Nessun utilizzo dell'ID Apple (IDFA) per monitorare l'attività degli utenti su altre app.**
- **Freemindtronic non raccoglie né condivide alcun dato sulla posizione in background o senza il consenso esplicito dell'utente.**
- **Le app non trasmettono alcun dato dal dispositivo a meno che l'utente non esegua volontariamente un'azione che richiede lo scambio di dati.**

ARTICOLO 11 – CONFORMITÀ ALLA LEGISLAZIONE SULLA PROTEZIONE DEI DATI DI ANDORRA

11.1. Applicazione delle leggi di Andorra

Freemindtronic, in quanto società registrata nel **Principato di Andorra**, è soggetta alle normative locali sulla **protezione dei dati**, tra cui:

- **Legge qualificata 15/2003 del 18 dicembre 2003** sulla protezione dei dati personali
- **Legge qualificata 29/2021 del 28 ottobre 2021**, che allinea Andorra ai principi del **Regolamento generale sulla protezione dei dati (GDPR – Regolamento (UE) 2016/679)**

Tali leggi garantiscono un quadro **di protezione dei dati** equivalente agli standard europei, riconosciuto **come adeguato** dall'Unione Europea ai sensi **dell'articolo 45 del GDPR**.

Oltre alle normative vigenti, **Freemindtronic implementa misure fisiche e software avanzate per garantire l'assoluta protezione dei dati**. Ciò include **la crittografia completa dei media digitali, l'autenticazione a più fattori NFC HSM e l'isolamento fisico delle infrastrutture IT**. Tali misure assicurano **il pieno rispetto degli articoli 10 e 45 del GDPR,** garantendo una protezione dei dati equivalente ai più severi standard europei.

ARTICOLO 12 – PRINCIPI DI CONFORMITÀ E SICUREZZA DEI DATI

12.1. Privacy by Design

Freemindtronic integra la **protezione dei dati** nella **progettazione del suo software e dei suoi servizi**, in conformità con i principi della **privacy by design e della privacy by default**.

12.2. Nessuna memorizzazione dei dati

In conformità con **l'approccio Zero Trust & Zero Knowledge**, **Freemindtronic non memorizza né elabora alcun dato personale**, tranne nel caso di fornitura volontaria da parte dell'utente (ad es. modulo di contatto, supporto tecnico).

12.3. Adozione di misure di sicurezza rafforzate

Freemindtronic implementa misure **di sicurezza avanzate** per garantire la **protezione dei dati** e prevenire le violazioni, tra cui:

- **Crittografa sistematicamente** le comunicazioni e le transazioni degli utenti attraverso i suoi sistemi brevettati di crittografia a chiave segmentata
- **Mancanza di identificatori univoci** che possono essere utilizzati per tracciare l'attività dell'utente
- **Verifica interna periodica** per garantire la conformità alle normative vigenti

Queste misure sono conformi all **'articolo 10 della Legge Qualificata 29/2021** sulla protezione dei dati personali in Andorra.

Freemindtronic applica una strategia di sicurezza informatica completa che garantisce la protezione dei dati anche in caso di intrusione fisica nei locali:

Tutti i sistemi informatici (fissi, mobili, server e dispositivi di archiviazione) sono completamente crittografati con chiavi a ≥256 bit.

Tutti i siti connessi online o su una rete locale utilizzano PassCypher NFC HSM e PassCypher HSM PGP con TOTP/HOTP e/o DataShielder NFC HSM e DataShielder HSM PGP Cyber Defense.

Nessuna chiave di crittografia è memorizzata o visibile sugli strumenti di produzione.

I supporti sensibili (chiavette USB, dischi rigidi) sono conservati in una cassaforte resistente agli incendi e alle intrusioni.

Qualsiasi estrazione di dati sensibili è impossibile, anche in caso di furto fisico dei server o di esfiltrazione illecita di file.

Queste misure garantiscono che, anche in caso di intrusione nei locali di Freemindtronic, nessun dato possa essere sfruttato anche in caso di intrusione illecita riuscita.

12.4. Impegno per la sicurezza continua

Freemindtronic pone la **protezione dei dati** al centro delle sue attività e si impegna a:

- **Migliorare continuamente le proprie misure di sicurezza** stando al passo con le minacce e le normative in evoluzione.
- **Adattare i propri protocolli di protezione** per garantire un livello di sicurezza in linea con i nuovi progressi tecnologici e le migliori pratiche di sicurezza informatica.
- **Monitora costantemente** le minacce informatiche, comprese quelle assistite dall'intelligenza artificiale (AI), per anticipare potenziali tentativi di intrusione e rafforzare le difese di conseguenza.

12.4.1 Protezione strategica: Freemindtronic non divulga pubblicamente tutti i dettagli tecnici dei suoi meccanismi di sicurezza in modo da non facilitare un'analisi da parte di un utente malintenzionato o di un'intelligenza artificiale che cerca di identificare una possibile vulnerabilità. Tuttavia, tutte le misure messe in atto rispettano gli **standard più severi** in termini di sicurezza informatica e protezione dei dati.

12.5. Sicurezza operativa e protezione dei dati sensibili

Freemindtronic applica un rigoroso modello di sicurezza che garantisce **la massima protezione contro i rischi di spionaggio interno ed esterno**.

12.5.1 Isolamento dei sistemi informatici

- Non è consentita alcuna connessione di rete tra sistemi interni e non è consentita la condivisione di file o stampanti.
- Ogni sistema è completamente indipendente, evitando vulnerabilità legate alle connessioni esterne.

12.5.2 Trasferimenti sicuri di dati sensibili

- Tutti i trasferimenti di file sensibili vengono eseguiti **esclusivamente** tramite le unità flash USB sicure **EviKey NFC** di Freemindtronic.
- Queste chiavi sono dotate **di autobloccaggio automatico** quando non vengono utilizzate, impedendo l'accesso non autorizzato.
- Nella **scatola nera delle chiavi NFC EviKey è integrato un registro di tracciabilità, che consente di verificare ogni sblocco e la sua geolocalizzazione**.

12.5.3 Isolamento fisico e messa in sicurezza degli strumenti di produzione

- Le apparecchiature e gli strumenti di produzione sensibili **non sono mai connessi a Internet** e sono rigorosamente isolati dopo l'uso.
- Dopo l'uso, questi strumenti vengono **conservati in una speciale cassaforte** resistente al fuoco e alle intrusioni fisiche.

12.5.4 Generazione e protezione delle chiavi di autenticazione

- Le chiavi di autenticazione anticontraffazione che fungono anche da **chiavi segmentate** vengono generate **in modo casuale** dagli strumenti di produzione.

- Queste chiavi **non vengono né visualizzate né salvate** negli strumenti di produzione, garantendo l'assenza di qualsiasi traccia utilizzabile.

12.5.5 Controllo rigoroso degli accessi e mitigazione dei rischi interni

- Solo **due persone autorizzate**, che sono anche **azionisti della società**, sono autorizzate all'utilizzo degli strumenti di produzione.
- Questa restrizione mira a **ridurre al minimo i rischi associati alle relazioni subordinate** e a garantire il pieno controllo dell'accesso alle infrastrutture sensibili.

12.6. Controllo rigoroso degli accessi e mitigazione dei rischi interni

12.6.1 Sicurezza dell'accesso e crittografia sistematica

Freemindtronic applica protocolli avanzati di autenticazione e crittografia per garantire che tutti gli accessi digitali e i media siano protetti da qualsiasi intrusione o tentativo di furto.

12.6.1.1 Protezione dell'accesso a siti e retiTutti i sistemi di rete online e locali utilizzano solo le seguenti tecnologie di autenticazione forte:

- 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 e/o DataShielder HSM PGP in versione Cyber Defense, che combinano l'autenticazione forte e la crittografia avanzata degli accessi.
- Emulatori di tastiera USB Bluetooth per proteggere l'input di dati sensibili eliminando qualsiasi rischio di keylogging.

12.6.1.2 Crittografia dei dati e dei supporti di memorizzazioneTutti i sistemi informatici (fissi, mobili) e i dispositivi di archiviazione contenenti dati sensibili sono crittografati con chiavi di crittografia pari o superiori a 256 bit.

- Dischi rigidi interni ed esterni completamente crittografati.
- Dispositivi mobili di archiviazione e backup protetti da crittografia hardware e/o software.

12.6.1.3 Resilienza alle intrusioni fisiche e digitaliTutto è progettato per garantire che, in caso di intrusione nei locali di Freemindtronic, furto di media digitali o estrazione illecita di dati sensibili, nessun dato sia utilizzabile o fisicamente accessibile.

- Proteggi le chiavi di crittografia nei dispositivi HSM NFC, impedendo l'accesso non autorizzato.
- Blocco automatico delle chiavi o blocco in caso di tentativo di compromissione con tracciabilità della scatola nera.

12.6.1.4 Integrazione dei prodotti utilizzando la tecnologia NFC EviKey

I prodotti Freemindtronic che incorporano la tecnologia **EviKey NFC** utilizzano esclusivamente l' app **Fullkey Plus** per la loro gestione e sicurezza. Questa tecnologia è integrata anche nelle seguenti soluzioni di sicurezza informatica:

- **PassCypher NFC HSM Master**
- **DataShielder NFC HSM Master e difesa**

L'integrazione di EviKey NFC in queste soluzioni fornisce un controllo avanzato degli accessi ai supporti di archiviazione e include le seguenti funzionalità:

- **Autobloccante quando inattivo**
- **Gestione sicura delle chiavi**
- **Accedi alla tracciabilità tramite una scatola nera**, accessibile solo senza contatto tramite **un telefono Android NFC**, grazie all' applicazione **Fullkey Plus**, **PassCypher NFC HSM** o **DataShielder NFC HSM**.

Freemindtronic non corre rischi quando si tratta di sicurezza e non si lascia sorprendere: qui, **il calzolaio non è certo il peggior ferrato** ! 😉

Freemindtronic implementa **partizioni di sicurezza a tenuta stagna**, prevenendo qualsiasi forma di spionaggio, sia interno che **esterno**, e garantendo **la massima** protezione degli asset digitali e dei dati critici.

12.6.1.4 – Protezione contro l'IA e gli attacchi avanzati :

Freemindtronic implementa tecnologie e protocolli specifici per proteggersi dagli attacchi assistiti dall'intelligenza artificiale, tra cui deepfake e manipolazioni audio/video volte a compromettere l'identità digitale di dirigenti e utenti. Tali misure comprendono una maggiore verifica delle comunicazioni e l'analisi multifattoriale delle operazioni sensibili.

12.7 – Gestione delle violazioni dei dati :

In caso di compromissione dell'hardware o tentativo di violazione della sicurezza che interessa l'infrastruttura di Freemindtronic, le procedure di risposta agli incidenti vengono eseguite in modo proattivo, indipendentemente dall'assenza di un sistema di rilevamento automatizzato.

Freemindtronic riconosce che non è realistico garantire una protezione assoluta contro un aggressore determinato, anche con le migliori misure di sicurezza al mondo. Per questo motivo l'approccio adottato si basa su una strategia **proattiva e preventiva**, integrando innovazioni brevettate a livello internazionale sviluppate per anticipare le nuove forme di spionaggio, in particolare quelle assistite dall'**intelligenza artificiale**.

Le soluzioni di sicurezza informatica di Freemindtronic sono progettate per impedire lo sfruttamento dei dati, anche in caso di accesso fisico o digitale non autorizzato. Questo approccio si basa su meccanismi avanzati tra cui l'autoblocco hardware, la crittografia a chiave segmentata, l'isolamento dell'infrastruttura e l'uso esclusivo di supporti sicuri come EviKey NFC, PassCypher NFC HSM e DataShielder NFC HSM.

Nel caso in cui un incidente di sicurezza riguardi un cliente o un partner, Freemindtronic si impegna a **informarli il prima possibile**, in conformità con i requisiti delle normative applicabili in materia di protezione dei dati.

ARTICOLO 13 – DIRITTI DEGLI UTENTI AI SENSI DELLA LEGISLAZIONE ANDORRANA

Ai sensi **degli articoli da 16 a 21 della Legge 29/2021**, gli utenti hanno i seguenti diritti, in linea con il **GDPR e la legislazione di Andorra** :

- **Diritto di accesso** : per verificare quali informazioni sono state fornite volontariamente e trattate.
- **Diritto di rettifica** : per correggere eventuali dati inesatti o incompleti.
- **Diritto di opposizione** : Opporsi all'utilizzo dei propri dati.
- **Diritto alla cancellazione (diritto all'oblio):** richiedere la cancellazione permanente dei propri dati.

- **Diritto alla portabilità** : ricevere i propri dati in un formato leggibile (nuovo obbligo rafforzato dalla Legge 29/2021).
- **Diritto alla limitazione del trattamento** : Limitare il trattamento di determinate informazioni.

13.1. Tempi di elaborazione delle richieste

Freemindtronic garantisce che qualsiasi richiesta di esercizio dei diritti sarà **elaborata entro un periodo massimo di 30 giorni**, salvo circostanze eccezionali che richiedano una **proroga giustificata fino a 60 giorni**.

Le richieste possono essere inviate via e-mail a:
contact [at] freemindtronic.com o **dpo [at] freemindtronic.com**

ARTICOLO 14 – RICORSO IN CASO DI CONTROVERSIA

Se un utente ritiene che i **suoi diritti non siano stati rispettati**, può presentare un reclamo all'**Agenzia per la protezione dei dati di Andorra (APDA),** l'**autorità di controllo competente in Andorra**.

14.1. Procedura di reclamo

Ai sensi **dell'articolo 25 della legge 29/2021**, chiunque ritenga che il trattamento dei propri dati sia stato effettuato in **violazione delle leggi applicabili** può:

- **Riferire la questione all'Agenzia per la protezione dei dati di Andorra (APDA)** per un'indagine amministrativa.
  Contatto APDA : https://www.apda.ad
- **Presentare ricorso presso i tribunali competenti di Andorra** al fine di ottenere il risarcimento del danno subito.

Freemindtronic si impegna a **collaborare pienamente** con le autorità di protezione dei dati in caso di indagine.

ARTICOLO 15 – MODIFICHE ALL'INFORMATIVA SULLA PRIVACY

15.1. Impegno ad aggiornare

Freemindtronic si impegna ad aggiornare la presente informativa in caso di modifiche legislative o regolamentari che influiscano sulla protezione dei dati. Eventuali modifiche saranno pubblicate esplicitamente sul sito ufficiale di Freemindtronic.

15.2. Frequenza e trasparenza degli aggiornamenti

Freemindtronic rilascia regolarmente aggiornamenti al suo software, alle sue applicazioni e alle sue estensioni. Viene mantenuta una pagina di aggiornamenti dedicata, che descrive in modo esplicito:

- **Le modifiche apportate,**
- **Miglioramenti della sicurezza,**
- **Eventuali vulnerabilità identificate e corrette.**

La cronologia completa delle versioni del software, delle applicazioni e delle estensioni Freemindtronic è disponibile qui: Cronologia delle versioni di Freemindtronic

15.3. Notifica agli utenti

Gli utenti che desiderano essere avvisati degli aggiornamenti via e-mail devono farne espressa richiesta fornendo il proprio indirizzo e-mail a Freemindtronic.

15.4. Informazioni in caso di modifiche delle funzionalità

In caso di modifiche alle funzionalità che comportano l'elaborazione dei dati, Freemindtronic si impegna a informare gli utenti:

- **Tramite notifica sul sito ufficiale,**
- **Tramite le applicazioni interessate.**

ARTICOLO 16 – DATI DI CONTATTO

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

Fine del documento