DATENSCHUTZERKLÄRUNG – FREEMINDTRONIC SL

Website & Software – Version und Datum des Dokuments: V2.0 vom 28.02.2025

ARTIKEL 1 – EINLEITUNG

1.1. Identifizierung des für die Verarbeitung Verantwortlichen

Diese Datenschutzrichtlinie wird von **Freemindtronic SL herausgegeben**, einer Gesellschaft mit beschränkter Haftung, die nach dem Recht des Fürstentums Andorra registriert ist und ihren eingetragenen Sitz in:

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

Freemindtronic ist verantwortlich für die Verarbeitung von Daten, die durch die Nutzung seiner offiziellen Website https://freemindtronic.com sowie seiner Software, Anwendungen, Erweiterungen und eingebetteten Systeme erhoben oder verarbeitet werden.

1.2. Champ d'Application

Diese Datenschutzerklärung gilt für alle Dienste, Software, Anwendungen, Erweiterungen und eingebetteten Systeme, die von Freemindtronic entwickelt und betrieben werden.

Sie gilt nicht für Websites, Dienste oder Plattformen Dritter, auf die über die Dienste von Freemindtronic zugegriffen werden kann. Freemindtronic ist nicht verantwortlich für die Datenschutzpraktiken dieser Dienste von Drittanbietern.

1.3. Engagement: Zero Trust & Zero Knowledge

Freemindtronic hält sich an ein strenges **Zero Trust & Zero Knowledge-Framework**, das sicherstellt, dass Benutzerdaten überhaupt nicht abgerufen, gespeichert oder weitergegeben werden.

Alle von Freemindtronic entwickelten Softwares, Anwendungen, Erweiterungen und eingebetteten Systeme arbeiten **ohne einen Remote-Server, eine zentrale Datenbank, die Erstellung eines Benutzerkontos, die Benutzeridentifikation und die Datenübertragung**.

Alle Funktionen von Freemindtronic stellen sicher, dass Benutzerdaten nicht gespeichert oder an Remote-Server übertragen werden. Alle Verarbeitungen erfolgen ausschließlich lokal auf dem Gerät des Nutzers, ohne Interaktion mit einer externen Infrastruktur.

1.4. Einhaltung der Vorschriften

- Freemindtronic erfüllt die strengsten internationalen Datenschutz- und Cybersicherheitsvorschriften, darunter:
- Datenschutz-Grundverordnung (DSGVO – Verordnung (EU) 2016/679)
- Gesetz über die digitale Betriebsstabilität (DORA – Règlement (UE) 2022/2554)
- NIS2-Richtlinie (Richtlinie (EU) 2022/2555) über die Cybersicherheit kritischer Infrastrukturen
- California Consumer Privacy Act (SCCA – USA, Cal. Civ. Code § 1798.100 ff.)
- Allgemeines Datenschutzgesetz (LGPD – Brésil, Gesetz Nr. 13,709/2018)
- Gesetz 15/2003 über den Schutz personenbezogener Daten in Andorra, geändert durch das qualifizierte Gesetz 29/2021
- Verordnung (EU) 2021/821 vom 20. Mai 2021 zur Kontrolle der Ausfuhr von Gütern mit doppeltem Verwendungszweck
- ISO/IEC 27001-Standards und NIST (National Institute of Standards and Technology, USA) Best Practices für die Sicherheit

1.5. DefinitionenIn dieser Richtlinie werden die folgenden Begriffe wie folgt definiert:

- **Personenbezogene Daten** : alle Informationen, die sich direkt oder indirekt auf eine identifizierte oder identifizierbare natürliche Person beziehen, insbesondere durch Bezugnahme auf eine Kennung wie einen Namen, eine Identifikationsnummer, Standortdaten, eine Online-Kennung oder auf ein oder mehrere Elemente, die für ihre physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität spezifisch sind.
- **Sensible Daten** : alle Informationen, deren unbefugte Weitergabe ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen könnte. Dazu gehören unter anderem:
    - Eindeutige Identifikatoren (Benutzernamen, Passwörter, Authentifizierungscodes).
    - Verschlüsselungs- und Authentifizierungsschlüssel.
    - Zahlungsinformationen und Bankverbindung.
    - Vertrauliche Daten von Kunden und Partnern (Geschäftsstrategien, Patente, Dokumente, die durch Geschäftsgeheimnisse geschützt sind).
    - Alle personenbezogenen Daten, die in die besonderen Kategorien der DSGVO fallen (ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gesundheit, biometrische Daten, Sexualleben).
- **Verarbeitung**: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung; Einschränkung, Löschung oder Vernichtung.
- **Verantwortlicher für die Datenverarbeitung** : die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.
- **Auftragsverarbeiter** : die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- **Einwilligung** : jede freie, spezifische, informierte und unmissverständliche Willensbekundung der betroffenen Person, mit der sie durch eine Erklärung oder eine eindeutige bestätigende Handlung mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
- **Pseudonymisierung** : Verarbeitung personenbezogener Daten in einer Weise, dass sie ohne zusätzliche Informationen nicht mehr einer bestimmten natürlichen Person zugeordnet werden können, die getrennt aufbewahrt und durch geeignete technische und organisatorische Maßnahmen geschützt werden müssen.
- **Anonymisierung** : unwiderrufliche Umwandlung personenbezogener Daten in eine Weise, die es nicht mehr ermöglicht, die betroffene Person direkt oder indirekt zu identifizieren.
- **Verletzung des Schutzes personenbezogener Daten** : Jede Sicherheitsverletzung, die versehentlich oder unrechtmäßig zur Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf personenbezogene Daten führt. Dazu gehört auch der unbefugte Zugriff auf Logins, Passwörter, Verschlüsselungsschlüssel oder andere geschützte sensible Daten.

ARTIKEL 2 – DATENERHEBUNG UND -VERARBEITUNG

2.1. Fehlende systematische Datenerhebung

Freemindtronic sammelt, speichert, teilt oder verkauft keine persönlichen oder technischen Daten von Benutzern, außer im Falle einer direkten Interaktion, einschließlich:

- Eine Bestellung über offizielle Plattformen.
- Eine Kontaktanfrage im Zusammenhang mit dem Kundendienst oder einer offiziellen Partnerschaft.

Die Daten werden nur im engen Rahmen der Vertragserfüllung oder Geschäftsbeziehung verarbeitet und niemals für andere Zwecke verwendet.

2.2. Daten, die erhoben werden können

Wenn ein Nutzer freiwillig Angaben macht, werden nur die Daten verarbeitet, die unbedingt erforderlich sind:

- Identität (Name, Vorname)
- Kontaktdaten (E-Mail, Telefon, Rechnungs- und Lieferadresse)
- Berufliche Informationen
- Freiwillig eingereichte Inhalte

Die Transaktionsdaten werden ausschließlich für die Verwaltung von Bestellungen und deren Lieferung verwendet, ohne dass sie an Dritte weitergegeben werden, es sei denn, es besteht gesetzliche Verpflichtungen (Steuern und Buchhaltung).

2.2.1 – Lokal in der Erweiterung oder Anwendung gespeicherte DatenEinige Freemindtronic-Anwendungen und -Erweiterungen verwenden möglicherweise localStorage oder die Web Storage API, um lokale Einstellungen vorübergehend auf dem Gerät des Benutzers zu speichern. Diese Daten werden niemals an Remote-Server übertragen und sind nur innerhalb der verwendeten Software zugänglich.

2.3. Datenspeicherung und -sicherheit

Freemindtronic wendet die höchsten Sicherheitsstandards an, die den Vorschriften **DSGVO, DORA, NIS2, ISO/IEC 27001 und NIST** entsprechen.

- **Sichere Offline-Speicherung** : Die Daten werden auf verschlüsselten Medien gespeichert, auf die nur über EviKey NFC Secure USB-Flash-Laufwerke und/oder verschlüsselte Speichermedien und/oder verschlüsselte Daten zugegriffen werden kann.
- **Zero Trust & Zero Knowledge** : Mangel an Remote-Servern und zentralisierten Datenbanken zum Speichern und/oder Verwalten sensibler Daten für alle Freemindtronic-Produkte.
- **Erhöhte Sicherheit für sensible Kommunikation**: Der Austausch sensibler Daten erfolgt ausschließlich über **DataShielder-Tools** oder ein vom Kunden definiertes sicheres Protokoll.
- **Ggf. auferlegte Alternative** : Wenn der Service des Kunden kein ausreichendes Sicherheitsniveau gewährleistet, bietet Freemindtronic **DataShielder** als einzigen sicheren Kanal an.

2.4. Schutz von Verschlusssachen und sensiblen Umgebungen

Die Lösungen von Freemindtronic, die als ziviles und militärisches Produkt mit doppeltem Verwendungszweck gekennzeichnet sind, wurden entwickelt, um kritische Informationen zu schützen, und umfassen:

- **Physische Isolierung und Partitionierung** : Es werden keine Daten auf einem Remote-Server gespeichert.
- **Starke Authentifizierung** : NFC HSM und patentierte segmentierte Schlüsselverschlüsselung. Die Verwendung der asymmetrischen RSA-4096-Verschlüsselung ermöglicht den sicheren Austausch von AES-256-CBC-Schlüsseln zwischen HSM-NFC-Geräten, auch aus der Ferne, ohne Übertragung über zentralisierte Infrastrukturen. Dieser Mechanismus eliminiert das Risiko einer Schlüsselexfiltration und bietet erweiterten Schutz für verschlüsselten Austausch.
- **Ende-zu-Ende-Verschlüsselung** : AES-256 CBC, RSA-4096, PGP - Alle sicheren symmetrischen Verschlüsselungssysteme werden über segmentierte Schlüssel und patentierte, international ausgelieferte Zutrittskontrollsysteme erreicht. Diese Architektur macht die Verschlüsselung resistent gegen Quantenangriffe und gewährleistet einen langfristigen Schutz sensibler Daten.
- **Dezentrale Protokollierung** : Lokale Blackbox, auf die nur ein autorisierter Administrator in NFC zugreifen kann.
- **Stresstests und proaktive Cybersicherheit** : Regelmäßige Bewertungen gegen APT-Angriffe, Industriespionage und fortschrittliche Cyberbedrohungen.

Wenn eine Freemindtronic-Erweiterung oder -Anwendung auf lokale Dateien auf einem Windows- oder Mac-Gerät zugreift (z. B. um Verschlüsselungsschlüssel oder sichere Dateien zu speichern), werden diese Dateien ausschließlich lokal verarbeitet und sind für Dritte niemals zugänglich. Der Benutzer behält die volle Kontrolle über seine Daten und diese werden nicht mit anderen Diensten geteilt.

2.5. Speicherung, Löschung und Aufbewahrung von Kundendaten

- Die über ein Kontaktformular angegebenen Daten werden nur zur Beantwortung der Anfrage verwendet und nach der Bearbeitung sofort gelöscht.
- Kundendaten, die sich aus Transaktionen ergeben, werden nur so lange aufbewahrt, wie es gesetzlich vorgeschrieben ist, in Übereinstimmung mit den in den folgenden Rechtsordnungen geltenden Vorschriften:
    - **Andorra: Qualifiziertes Gesetz 29/2021 – Aufbewahrung von Steuerunterlagen für 5 Jahre**
    - **Europäische Union: Artikel 6 der Verbraucherschutzrichtlinie 2011/83/EU – Aufbewahrung von Transaktionsdaten für bis zu 10 Jahre, abhängig von den lokalen Rechnungslegungsanforderungen**
    - **Frankreich: Artikel L123-22 des französischen Handelsgesetzbuches – obligatorische Aufbewahrung von Buchhaltungsunterlagen für 10 Jahre**
    - **USA: IRS-Veröffentlichung 583 – Aufbewahrung von Transaktionsdaten für 3-7 Jahre**
- **Es werden keine Bankdaten gespeichert**: Die Transaktionen werden über **sichere Drittanbieter** (z.B. PayPal) abgewickelt.

2.6. Internationale Datenübermittlungen

Freemindtronic übermittelt keine Daten außerhalb des EWR, es sei denn, es wird ein angemessener rechtlicher Rahmen angewandt (**Standardvertragsklauseln - SCCs**).

2.7. Verfahren bei Datenschutzverletzungen

In Übereinstimmung mit den Artikeln 33 und 34 der **DSGVO** und dem **qualifizierten Gesetz 29/2021** reagiert Freemindtronic **im Falle eines Vorfalls** proaktiv:

- **Sofortige Eindämmungs-** und **Auswirkungsanalyse**.
- **Benachrichtigung innerhalb von 72 Stunden** an die andorranische Datenschutzbehörde (APDA), falls erforderlich.
- **Betroffene Nutzer informieren** , wenn ein hohes Risiko festgestellt wird.
- **Audit nach einem Vorfall** zur Stärkung der Schutzmaßnahmen.

2.8. Cyberresilienz und Schutz vor Katastrophen und Cyberangriffen

Freemindtronic garantiert **die Integrität und Verfügbarkeit** der Daten auch im Falle eines Ausfalls, Diebstahls, einer Katastrophe oder eines massiven Cyberangriffs.

2.8.1. Verschlüsselung und sichere Sicherung

- **Erweiterte Verschlüsselung**: AES-256 CBC, AES-256 CBC PGP, BitLocker mit Schlüsseln, die **auf NFC HSM PassCypher gespeichert sind**.
- **Trennung von Schlüsseln und Daten**: Entschlüsselungsschlüssel werden niemals auf demselben Medium wie die Daten gespeichert. AES-256 CBC-Verschlüsselungsschlüssel sind hochsicher, können über NFC HSM DataShielder geteilt werden und arbeiten kontaktlos, serverlos und datenbankfrei. Dieser Mechanismus gewährleistet eine sichere Schlüsselübertragung, auch aus der Ferne, und eliminiert jedes Risiko des Abhörens durch Dritte.
- **Verschlüsselte und redundante Backups**: Daten, die offline und sicher **über mehrere Medien** repliziert werden.

2.8.2. Verbesserter Schutz vor Cyberangriffen

- **Ransomware & Überverschlüsselung** : Verschlüsselte Offline-Backups und physisch ausgelagerte Schlüssel offline verhindern Manipulationen oder betrügerische Wiederherstellung.
- **Fortschrittliche Cyberangriffe (APT, Zero-Day, Spionage): Die Zero-Trust- und Zero-Knowledge-Architektur** und **die physische Schlüsseltrennung** verhindern die Exfiltration. Die Sicherheitsarchitektur von Freemindtronic, die patentierte segmentierte Verschlüsselungssysteme und hardwarebasierte Zugriffskontrolle umfasst, stellt sicher, dass keine privaten Schlüssel oder verschlüsselten Daten exfiltriert werden können, selbst wenn physische oder logische Einschränkungen bestehen. Die Kombination aus AES-256 CBC-Verschlüsselung und RSA-4096 erhöht die Widerstandsfähigkeit gegen komplexe Angriffe, einschließlich solcher, die durch künstliche Intelligenz unterstützt werden.
- **Cloud-lose Ausfallsicherheit** : **Keine Abhängigkeit von Remote-Servern**, wodurch das Risiko zentralisierter Angriffe eliminiert wird.

2.8.3. Resilienz gegenüber physischen Katastrophen und unfallbedingten Verlusten

Die Protokolle von Freemindtronic gewährleisten immer den Zugriff auf Daten, die mit ihren Schlüsseln verschlüsselt sind, auch in folgenden Fällen:

- **Diebstahl oder Verlust** von verschlüsselten Medien: Ohne **ausgelagerte Schlüssel** bleiben Daten unbrauchbar.
- **Versehentliche Zerstörung oder Naturkatastrophe** : Doppelte **Backups** sorgen dafür, dass sensible Daten wiederhergestellt werden.
- **Geografische Isolierung von Backups** : Verschlüsselte **Medien** werden an verschiedenen sicheren Orten aufbewahrt, um eine vollständige Kompromittierung zu verhindern.

2.9. Geheimhaltungsvereinbarungen (NDAs) und Vertraulichkeit des Handels

Alle Geschäftsbeziehungen mit Freemindtronic, die den Austausch sensibler oder vertraulicher Informationen beinhalten, sind routinemäßig durch eine **Geheimhaltungsvereinbarung (NDA) abgedeckt.**

- **Strikte Anwendung** : Alle Informationen, die im Rahmen von Partnerschaften, technischen Kooperationen oder Geschäftsgesprächen ausgetauscht werden, sind durch rechtlich verbindliche Vertraulichkeitsklauseln geschützt. Alle sensiblen Dokumente, ob verschlüsselt oder unverschlüsselt, die mit Kunden und Partnern ausgetauscht werden, werden über die in DataShielder HSM PGP eingebettete Funktion systematisch digital signiert. Diese digitale Signatur stellt die Integrität und Authentizität der Dokumente sicher und stellt sicher, dass nach ihrer Ausstellung keine Beschädigungen oder Änderungen vorgenommen wurden. Darüber hinaus wird die E-Mail-Kommunikation mit sensiblen Informationen immer über PGP gesichert, um ein Abfangen oder Manipulieren von Nachrichten zu verhindern.

- **Geltungsbereich der NDA**: Die NDA umfasst **Dokumente, Mitteilungen, technischen Austausch, Innovationen, interne Daten** sowie alle vertraulichen Informationen, die von Freemindtronic übermittelt oder von einem Partner empfangen werden.

- **Strafen für Verstöße** : Jede unbefugte Offenlegung vertraulicher Informationen unterliegt vertraglichen **und gesetzlichen Strafen** , die rechtliche Schritte wegen Verletzung der Vertraulichkeit und von Geschäftsgeheimnissen umfassen können.

- **Schutzdauer**: Geheimhaltungsverpflichtungen bleiben **auch nach Beendigung des Vertragsverhältnisses gemäß** der in der jeweiligen Vereinbarung festgelegten Frist in Kraft.

Diese Klausel bekräftigt das Engagement von Freemindtronic, alle kritischen Informationen, die im Rahmen seiner Geschäftstätigkeit ausgetauscht werden, zu schützen und einen strengen rechtlichen Rahmen gegen Durchsickern oder Kompromittierungen zu gewährleisten.

ARTIKEL 3 – VERWENDUNG VON SENSOREN UND ZUGRIFF AUF STANDORTDATEN

Einige Freemindtronic-Software, -Anwendungen oder -Erweiterungen erfordern möglicherweise Zugriff auf die Sensoren auf den Geräten der Benutzer.

3.1 Zu diesen Sensoren gehören:

- **GPS** (genaue Ortung)
- **Wi-Fi und Mobilfunknetze** (ungefährer Standort)
- **Bluetooth** (lokale Erkennung ohne externe Übertragung)
- **Biometrische Daten** (Fingerabdruck, Gesichtserkennung)
- **Mikrofon und Kamera** (nur mit ausdrücklicher Zustimmung)

- **Umgebungssensoren** (Beschleunigungssensor, Gyroskop, Näherungssensoren, Helligkeit)
- **Sicherheitsmodule** (NFC, HSM, HSM, PGP)

3.2 Alle von diesen Sensoren erzeugten Daten:

- **Sie verbleiben ausschließlich auf dem Gerät des Nutzers** und werden unter keinen Umständen an einen Remote-Server oder einen Dienst eines Drittanbieters übertragen.
- **Sie unterliegen keiner externen oder Remote-Speicherung**.
- **Sind nur mit ausdrücklicher Zustimmung des Nutzers zugänglich**, insbesondere bei empfindlichen Sensoren wie Mikrofon und Kamera.
- **Kann vom Benutzer verwaltet werden**, der die erteilten Berechtigungen jederzeit über seine Geräteeinstellungen ändern oder widerrufen kann.

Die Sensoren der Geräte (Kamera, Mikrofon, NFC, GPS, Wi-Fi, Bluetooth) werden nur lokal verwendet und übertragen niemals Daten an externe Server, Dritte oder andere Dienste von Freemindtronic. Der Benutzer kann diesen Zugriff über seine Geräteeinstellungen steuern und deaktivieren.

3.4 Sicherstellen, dass Sensordaten nicht für Zwecke der Verhaltensverfolgung verwendet werden

Freemindtronic stellt sicher, dass **die über Gerätesensoren gesammelten Daten niemals für Verhaltensverfolgung, gezielte Werbung oder Benutzerprofilerstellung verwendet werden**.

Der Zugriff auf die Sensoren ist streng auf die wesentlichen Softwarefunktionen beschränkt und nur nach ausdrücklicher Zustimmung des Nutzers.

Auf Basis dieser Daten findet keine Analyse des Nutzungsverhaltens statt und sie werden nicht gespeichert oder an Dritte weitergegeben.

ARTIKEL 4 – EINHALTUNG DER VERTRIEBSPLATTFORMEN

Die von Freemindtronic **entwickelte Software, Anwendungen und Erweiterungen** entsprechen den Anforderungen der folgenden Plattformen:

- **Google Play Console** (Anwendungen Android)
- **Chrome Web Store** (Browser-Erweiterungen)
- **Microsoft Store- und Edge-Add-Ons** (Windows-Apps und Browsererweiterungen)
- **Apple macOS und iOS** (Apps, die im App Store vertrieben werden)

Freemindtronic verpflichtet sich, die von **diesen Plattformen auferlegten** Sicherheits- und Datenschutzrichtlinien einzuhalten.

- **Die Zero Trust & Zero Knowledge Architektur ist so gewährleistet** , dass keine Nutzerdaten über das Gerät des Nutzers hinaus gesammelt, übertragen oder gespeichert werden.
- **Es gibt keine Integration mit Diensten von Drittanbietern**, um die mit der Verfolgung oder Erfassung personenbezogener Daten verbundenen Risiken zu mindern.
- **Die Anforderungen jeder Plattform werden regelmäßig überprüft** , um die kontinuierliche Einhaltung der Änderungen der geltenden Vorschriften zu gewährleisten.

ABSCHNITT 5 – NICHTDISKRIMINIERUNGSKLAUSEL (CCPA-KONFORMITÄT)

In Übereinstimmung mit den Bestimmungen des **California Consumer Privacy Act (CCPA) garantiert Freemindtronic, dass die Nutzer** bei der Ausübung ihrer Rechte in Bezug auf den Schutz personenbezogener Daten nicht diskriminiert werden.

Es werden keine Einschränkungen oder Beschränkungen für Benutzer angewendet , die ihre Rechte ausüben möchten, insbesondere in Bezug auf:

- Zugang zu ihren personenbezogenen Daten.
- Berichtigung unrichtiger oder unvollständiger Informationen.
- Löschung der freiwillig zur Verfügung gestellten Daten.
- Widerspruch gegen oder Einschränkung der Verarbeitung ihrer Daten.

Freemindtronic verpflichtet sich, keine zusätzlichen Gebühren oder Änderungen des Zugriffs auf Funktionen zu erheben, wenn ein Benutzer einen Antrag auf Ausübung von Rechten stellt.

Jeder Nutzer, der seine Rechte geltend machen möchte, kann sich über die in dieser Datenschutzerklärung angegebenen Kontaktdaten direkt an Freemindtronic wenden.

In Übereinstimmung mit dem CCPA führt die Ausübung von Rechten zum Schutz personenbezogener Daten (Zugang, Löschung, Widerspruch) nicht zu einer Änderung, Einschränkung oder Verschlechterung der von Freemindtronic angebotenen Dienste.

ARTIKEL 6 – KEIN PROFILING UND KEINE FINGERABDRÜCKE

6.1. Fehlen von Profiling und automatisierten Entscheidungen

Freemindtronic führt kein Profiling, keine Verhaltensverfolgung oder automatisierte Entscheidungsfindung durch, die die Benutzer betreffen.

- Es wird keine Analyse der Benutzeraktivität durchgeführt.
- Für die Klassifizierung der Nutzer wird kein Algorithmus der künstlichen Intelligenz verwendet.
- Es gibt keinen Mechanismus zur Personalisierung von Diensten auf der Grundlage von Benutzerdaten.

6.2. Abwesenheit von Fingerabdrücken

Fingerprinting ist eine Technik, bei der bestimmte Informationen über die Hardware oder Software eines Geräts gesammelt werden, wie z. B. IP-Adresse, Betriebssystem, Bildschirmauflösung und andere Parameter, um einen eindeutigen digitalen Fingerabdruck des Benutzers zu erstellen. Im Gegensatz zu Cookies ist diese Methode schwer zu erkennen und zu blockieren, was große Bedenken hinsichtlich des Datenschutzes aufwirft.

Im Dezember 2024 **kündigte Google an, dass es Werbetreibenden ab dem 16. Februar 2025 erlauben wird, Fingerabdrücke für die Nutzerverfolgung zu verwenden,** und kehrte damit seine Richtlinie von 2019 um, die diese Praxis verboten hatte. Der Schritt wurde von Regulierungsbehörden wie **dem britischen Information Commissioner's Office (ICO) kritisiert,** das die Änderung als "unverantwortlich" bezeichnete, da die Auswahl und Kontrolle des Einzelnen über die Sammlung seiner Informationen eingeschränkt ist.

Bei **Freemindtronic** verpflichten wir uns sehr, die Privatsphäre unserer Benutzer zu respektieren. Daher verwenden wir in **unseren Produkten oder Dienstleistungen** keine Form von

Fingerabdrücken.**Google kündigte im Dezember 2024 an, Fingerprinting für Werbetreibende ab dem 16. Februar 2025 zu erlauben** (offizielle Quelle - https://blog.google/products/ads-commerce/privacy-sandbox-fingerprinting-policy-change).

Der Schritt löste Bedenken bei den Regulierungsbehörden aus, einschließlich **des britischen ICO**. Freemindtronic lehnt diese Praktiken ab und garantiert, dass **kein Tracking, keine Geräteidentifikation oder Verhaltensprofilerstellung** implementiert wird.

Alle IT-Systeme von Freemindtronic sind **vollständig isoliert und unabhängig** voneinander. Es werden keine Nutzerdaten **durch einen ausschließlich lokalen und Offline-Betrieb** erfasst, gespeichert oder nachverfolgt.**Die Verwendung von Hardware-Verschlüsselung und NFC-HSM-Authentifizierungslösungen** stellt sicher, dass kein digitaler Fingerabdruck mit Benutzern in Verbindung gebracht werden kann, auch durch den Einsatz der EviBITB-Technologie von Freemindtronic.

Freemindtronic implementiert eine **fortschrittliche Cybersicherheitsstrategie** zum Schutz vor KI-gestützten Angriffen, CEO-Betrug und anderem Identitätsdiebstahl.

- Bei den **E-Mails, die für die externe Kommunikation verwendet werden**, handelt es **sich um Sandbox-Adressen und No-Reply-E-Mails**, um **das Risiko von Spoofing und Phishing zu verringern**.
- Das Öffnen von Anhängen unterliegt einer **strengen Kontrollrichtlinie**, um **das Risiko bösartiger Dateien zu vermeiden**.
- Jede **Kundenanfrage** wird systematisch durch **einen zweiten Kommunikationskanal** überprüft , um **ihre Echtheit zu bestätigen** (proaktive Beseitigung von Zweifeln).

Freemindtronic garantiert**, dass es niemals Gerätefingerabdrücke** über indirekte Identifikationsmethoden (z. B. Bildschirmauflösung, Gerätemodell, Browsersprache) sammeln, analysieren oder verwenden wird.

ARTIKEL 7 – EINHALTUNG DER VORSCHRIFTEN ÜBER GÜTER MIT DOPPELTEM VERWENDUNGSZWECK

7.1. Ausfuhrbestimmungen und -genehmigungen

Freemindtronic setzt die Vorschriften für das Management und den Export von Cybersicherheitstechnologien strikt durch, auch für **Verschlüsselungsprodukte, die als zivile und militärische Produkte mit doppeltem Verwendungszweck eingestuft** sind.

Die Produkte DataShielder NFC HSM **haben eine** Einfuhrgenehmigung des Fürstentums Andorra nach Frankreich **erhalten, die am 7.** Dezember 2024 **über die Firma** AMG Pro gemäß dem **Dekret Nr. 2001-1192 vom 13. Dezember 2001**, geändert durch **das Dekret Nr. 2024-95 vom 8. Februar 2024**, validiert wurde.

Diese Genehmigung wurde nach Einreichung des Dossiers bei der **ANSSI eingeholt**, die im Einklang mit ihrer Aufgabe, **die Einhaltung der regulatorischen Anforderungen zu überprüfen**, die Genehmigung nicht innerhalb der in den geltenden Rechtsvorschriften vorgesehenen Fristen verweigerte.

Seit dem **7. Februar 2025** sind **DataShielder NFC HSM-Produkte** gemäß der Verordnung (EU) 2021/821 vom 20. Mai 2021 **über Güter mit doppeltem Verwendungszweck** auch **für die Wiederausfuhr** aus Frankreich in die Mitgliedstaaten der Europäischen Union zugelassen.

7.2. Referenztexte

Diese Ermächtigung wird auf der Grundlage der folgenden Texte erteilt:

- **Dekret Nr. 2001-1192 vom 13. Dezember 2001**, geändert durch **das Dekret vom 8. Februar 2024,** über die Kontrolle der Ausfuhr und des Transfers von Gütern und Technologien mit doppeltem Verwendungszweck.
- **Verordnung (EU) 2021/821 vom 20. Mai 2021** zur Einführung einer Ausfuhrkontrollregelung für Güter mit doppeltem Verwendungszweck.

7.3. Prüfungsverpflichtung

Freemindtronic verpflichtet sich, **regelmäßige Compliance-Audits** durchzuführen, um die **kontinuierliche Einhaltung gesetzlicher und behördlicher Anforderungen zu gewährleisten**. Diese internen Audits werden periodisch in Übereinstimmung mit den geltenden regulatorischen Anforderungen durchgeführt.

ARTIKEL 8 – ZERTIFIZIERUNGEN UND AUDITS

8.1. Keine Cloud-Zertifizierung erforderlich

Freemindtronic benötigt keine **SOC 2-** oder **ISO 27001-Zertifizierungen** , die für Cloud-Infrastrukturen spezifisch sind, da **keine Remote-Server** für die Datenverarbeitung oder -speicherung verwendet werden.

Die Produkte sind mit einem **100%igen Air-Gap-Ansatz** ausgestattet, der eine **vollständige Isolierung der Benutzerdaten** von jeder externen Netzwerkinfrastruktur gewährleistet. Diese Architektur rechtfertigt **das Fehlen bestimmter Audits, die** normalerweise auf verbundene Systeme angewendet werden.

8.2. Sicherheitsaudit und Qualitätskontrolle

Dieser Ansatz **wird in der gesamten Wertschöpfungskette angewendet**, vom **Produktdesign** bis zur **Fertigung**. Alle durchgeführten Audits zielen darauf ab, die **Ausfallsicherheit, Manipulationssicherheit und Datenlecksicherheit der** Systeme von Freemindtronic zu gewährleisten.

Zusätzlich zu internen Audits zur Sicherstellung der Produktkonformität wendet Freemindtronic **verbesserte Kontrollen für das Zahlungsmanagement** und **den Schutz von Finanztransaktionen an**.

- Das Buchhaltungs- und Finanzmanagementsystem ist isoliert, und keine Transaktion kann ohne starke Authentifizierung über DataShielder NFC HSM Auth und DataShielder MAuth validiert werden, wodurch eine starke Authentifizierung gewährleistet und das Betrugsrisiko ausgeschlossen wird.
- Der Zugang zu Bankkonten und Zahlungssystemen ist streng auf autorisierte Aktionäre ohne Unterordnungsverhältnis beschränkt, um die internen Betrugsrisiken zu begrenzen.

ARTIKEL 9 – DATENSCHUTZBEAUFTRAGTER (DSB)

9.1. Ernennung des DSB

In Übereinstimmung mit den Anforderungen der **Datenschutz-Grundverordnung (DSGVO – Verordnung (EU) 2016/679)** und anderen anwendbaren Vorschriften hat Freemindtronic einen **Datenschutzbeauftragten (DSB) ernannt, der** dafür verantwortlich ist, die Einhaltung des Schutzes personenbezogener Daten durch das Unternehmen sicherzustellen.

Der **DSB von Freemindtronic** ist:

- **Name:** Jacques Gascuel
- **Position:** CEO und DPO von Freemindtronic SL
- **Kontakt :** dpo [at] freemindtronic.com

9.2. Aufgaben des DSB

Der DSB von Freemindtronic erfüllt mehrere wichtige Aufgaben, darunter:

- Stellen Sie sicher, dass die **Datenverarbeitung** den geltenden Vorschriften (**DSGVO, CCPA, LGPD usw.) entspricht.**).
- Freemindtronic über seine datenschutzrechtlichen Pflichten **zu informieren und zu beraten**.
- Überwachen Sie die Anwendung **der eingerichteten Sicherheits- und Datenschutzrichtlinien** .
- Beantwortung von Anfragen der Nutzer bezüglich **ihrer Rechte (Zugang, Berichtigung, Löschung, Widerspruch usw.)**.
- Zusammenarbeit mit **den Datenschutzbehörden**, einschließlich der **andorranischen Datenschutzbehörde** und der zuständigen europäischen oder internationalen Behörden.

9.3. Kontakt und Beschwerden

Jeder Nutzer, der Informationen über **die Verwaltung seiner personenbezogenen Daten** erhalten oder seine Rechte ausüben möchte, kann sich **unter der folgenden Adresse an** den Datenschutzbeauftragten von Freemindtronic wenden:

- **E-Mail :** dpo [at] freemindtronic.com
- **Postanschrift:**
  Freemindtronic SLAv. Co-Prince de Gaulle, 13, Valira Building, Erdgeschoss, AD700 Escaldes – Engordany, Andorra

Wenn innerhalb von **30 Tagen keine Antwort erfolgt**, kann der Nutzer die Angelegenheit direkt **an die andorranische Datenschutzbehörde (APDA) verweisen,** wenn er **der gesetzlichen Verpflichtung, innerhalb von 30 Tagen zu antworten, nicht nachgekommen** ist.

ARTIKEL 10 – BESONDERE ANFORDERUNGEN AN VERTRIEBSPLATTFORMEN

10.1. Google Play Konsole (Android)

Freemindtronic Apps erheben, speichern oder übermitteln keine personenbezogenen Daten. Einige Android-Berechtigungen (z. B. NFC, Speicher, Kamera) werden nur verwendet, um die Produktfunktionalität zu aktivieren, und werden nicht für Zwecke Dritter ausgenutzt. Es werden keine Daten an Dritte weitergegeben, und alle Vorgänge werden in Übereinstimmung mit den Datenschutzrichtlinien von Google Play lokal auf dem Gerät des Nutzers ausgeführt.

10.1.1. Einhaltung der Google Play-Richtlinien in Bezug auf sensible Daten und BerechtigungenFreemindtronic-Anwendungen, die Zugriff auf sensible Android-Funktionen (NFC, Speicher, Kamera, Mikrofon, GPS, SMS, RCS, MMS) benötigen, erfüllen die folgenden Anforderungen:

- **Ausdrückliche Zustimmung** : Standardmäßig sind keine Berechtigungen aktiviert. Der Benutzer muss sie manuell über seine Geräteeinstellungen aktivieren.

- **Nahtlose Nutzung** : Der Zugriff auf diese Funktionen ist **streng auf** die wesentlichen Bedürfnisse der App beschränkt, und die generierten Daten verbleiben **ausschließlich auf dem Gerät**.
- **Kein Missbrauch von Berechtigungen** : Freemindtronic fragt niemals nach Zugriff auf überflüssige Funktionen und respektiert die Transparenzrichtlinie von Google Play.

10.1.2. Datenschutz und lokale SpeicherungAlle Daten verbleiben streng auf dem Gerät des Nutzers gespeichert und **können nur von der App selbst abgerufen werden**. Es werden keine Nutzerdaten auf **externen Servern** gespeichert oder an **Dritte weitergegeben**.

10.2 – Chrome Web Store (Chrome-Erweiterungen)

Freemindtronic-Erweiterungen sammeln oder geben keine Benutzerdaten weiter. Sie können localStorage verwenden, um lokale Informationen vorübergehend zu speichern, die für die ordnungsgemäße Funktion der Erweiterung erforderlich sind.

Es findet kein verstecktes Tracking, keine Weitergabe von Daten an Dritte und kein unberechtigter Zugriff auf Cookies oder den Browserverlauf statt.

10.2.1 Verwendung von Local StorageFreemindtronic-Erweiterungen verwenden ausschließlich die localStorage- und Web-Storage-API , um vorübergehend Einstellungen zu speichern, die für ihr ordnungsgemäßes Funktionieren erforderlich sind.
Diese Daten:

- **Werden niemals an Remote-Server übertragen.**
- **Sind nur für den Benutzer und nur im Kontext der Erweiterung zugänglich.**
- **Einstellungen, die lokal über localStorage und Web Storage gespeichert werden, enthalten keine personenbezogenen oder sensiblen Daten.**
- **Benutzer können gespeicherte lokale Daten manuell über die in die Erweiterung integrierte Option "Daten löschen" löschen.**

10.3. Microsoft Store & Edge Add-ons (Windows)

Freemindtronic Apps und Erweiterungen entsprechen den Datenschutzstandards von Microsoft.

Wenn eine Anwendung auf lokale Dateien zugreift (z. B. sichere Speicherung von Verschlüsselungsschlüsseln), bleiben diese Dateien isoliert und werden niemals mit Diensten von Drittanbietern geteilt.

Freemindtronic garantiert, dass es keine versteckten Fingerabdrücke oder Nachverfolgung in Übereinstimmung mit den Microsoft Store-Richtlinien gibt.

10.3.1. Schutz vor lokalem Dateizugriff (Windows)
Einige Freemindtronic-Anwendungen benötigen möglicherweise Zugriff auf lokale Dateien, um **sensible Daten zu verschlüsseln, zu schützen oder zu authentifizieren**.
Diese Dateien:

- **Werden nie an einen Remote-Server weitergeleitet.**
- **Bleiben ausschließlich auf dem Gerät des Nutzers gespeichert und verarbeitet.**
- **Sind nur für lokal installierte Anwendungen mit Zustimmung des Benutzers zugänglich.**

10.4. Apple App Store (macOS & iOS)

Freemindtronic-Apps verfolgen keine Benutzer, sammeln keine Daten für die Erstellung von Werbeprofilen und übertragen keine Informationen außerhalb des Geräts.

Greift eine App auf iOS/macOS-Sensoren (z.B. NFC, Mikrofon, GPS) zu, ist diese Nutzung streng auf wesentliche und vom Nutzer steuerbare Funktionen beschränkt.

Sofern APIs von Drittanbietern verwendet werden (z.B. Zahlung über Apple Pay), entsprechen deren Auswirkungen auf die Nutzerdaten den Anforderungen von Apple und sind für den Nutzer vollständig transparent.

10.4.1. Einhaltung der Richtlinie zur Transparenz des App-Trackings (ATT)Freemindtronic garantiert**, dass es keine Werbe-IDs** oder **User-Tracking-Tools** für Marketing- oder Werbezwecke verwendet.
In Übereinstimmung mit den Apple-Richtlinien:

- **Es werden keine Nutzerdaten für die Profilerstellung oder das Targeting von Werbung gesammelt.**
- **Es gibt keine Integration mit Werbe- oder Analysediensten von Drittanbietern.**
- **Keine Verwendung der Apple ID (IDFA), um Benutzeraktivitäten in anderen Apps zu verfolgen.**
- **Freemindtronic sammelt oder teilt keine Standortdaten im Hintergrund oder ohne die ausdrückliche Zustimmung des Nutzers.**
- **Apps übertragen keine Daten vom Gerät, es sei denn, der Nutzer führt freiwillig eine Handlung aus, die einen Datenaustausch erfordert.**

ARTIKEL 11 – EINHALTUNG DER ANDORRANISCHEN DATENSCHUTZGESETZGEBUNG

11.1. Anwendung der andorranischen Gesetze

Freemindtronic unterliegt als im **Fürstentum Andorra** registriertes Unternehmen den lokalen **Datenschutzbestimmungen**, einschließlich:

- **Qualifiziertes Gesetz 15/2003 vom 18. Dezember 2003** über den Schutz personenbezogener Daten
- **Qualifiziertes Gesetz 29/2021 vom 28. Oktober 2021**, das Andorra an die Grundsätze der **Datenschutz-Grundverordnung (DSGVO – Verordnung (EU) 2016/679) anpasst**

Diese Gesetze garantieren einen **Datenschutzrahmen**, der den europäischen Standards entspricht und **von der Europäischen Union gemäß** Artikel 45 der DSGVO als **angemessen anerkannt wird**.

Zusätzlich zu den aktuellen Vorschriften **implementiert Freemindtronic fortschrittliche physische und softwaretechnische Maßnahmen, um absoluten Datenschutz zu gewährleisten**. Dazu gehören **die vollständige Verschlüsselung digitaler Medien, NFC HSM Multi-Faktor-Authentifizierung und die physische Isolierung von IT-Infrastrukturen**. Diese Maßnahmen gewährleisten die **vollständige Einhaltung der Artikel 10 und 45 der DSGVO** und garantieren einen Datenschutz, der den strengsten europäischen Standards entspricht.

ARTIKEL 12 – COMPLIANCE-GRUNDSÄTZE UND DATENSICHERHEIT

12.1. Eingebauter Datenschutz

Freemindtronic integriert **den Datenschutz** in die **Gestaltung seiner Software und Dienste** in Übereinstimmung mit den Grundsätzen **von Privacy by Design und Privacy by Default**.

12.2. Keine Datenspeicherung

Gemäß **dem Zero Trust & Zero Knowledge-Ansatz speichert und verarbeitet Freemindtronic keine personenbezogenen Daten**, außer im Falle einer freiwilligen Angabe durch den Nutzer (z.B. Kontaktformular, technischer Support).

12.3. Verabschiedung verstärkter Sicherheitsmaßnahmen

Freemindtronic implementiert **fortschrittliche Sicherheitsmaßnahmen** , um **den Datenschutz zu gewährleisten** und Verstöße zu verhindern, darunter:

- **Systematische Verschlüsselung der** Benutzerkommunikation und -transaktionen durch die patentierten segmentierten Schlüsselverschlüsselungssysteme
- **Fehlen eindeutiger** Identifikatoren, die zur Verfolgung von Benutzeraktivitäten verwendet werden können
- **Regelmäßige interne Auditierbarkeit** , um die Einhaltung der geltenden Vorschriften sicherzustellen

Diese Maßnahmen stehen im Einklang mit **Artikel 10 des qualifizierten Gesetzes 29/2021** über den Schutz personenbezogener Daten in Andorra.

Freemindtronic wendet eine umfassende Cybersicherheitsstrategie an, die den Datenschutz auch im Falle eines physischen Eindringens in die Räumlichkeiten gewährleistet:

Alle Computersysteme (stationäre, mobile, Server- und Speichergeräte) werden vollständig mit ≥256-Bit-Schlüsseln verschlüsselt.

Alle Standorte, die online oder in einem lokalen Netzwerk verbunden sind, verwenden PassCypher NFC HSM und PassCypher HSM PGP mit TOTP/HOTP und/oder DataShielder NFC HSM und DataShielder HSM PGP Cyber Defense.

Auf den Produktionswerkzeugen werden keine Verschlüsselungsschlüssel gespeichert oder sichtbar.

Empfindliche Medien (USB-Sticks, Festplatten) werden in einem feuer- und einbruchsicheren Tresor aufbewahrt.

Jede Extraktion sensibler Daten ist unmöglich, selbst im Falle eines physischen Diebstahls von Servern oder einer illegalen Exfiltration von Dateien.

Diese Maßnahmen stellen sicher, dass auch im Falle eines Einbruchs in die Räumlichkeiten von Freemindtronic auch im Falle eines erfolgreichen rechtswidrigen Eingriffs keine Daten verwertet werden können.

12.4. Verpflichtung zur kontinuierlichen Sicherheit

Freemindtronic stellt **den Datenschutz** in den Mittelpunkt seiner Aktivitäten und verpflichtet sich:

- **Verbessern Sie kontinuierlich Ihre Sicherheitsmaßnahmen** , indem Sie mit den sich entwickelnden Bedrohungen und Vorschriften Schritt halten.
- **Anpassung der Schutzprotokolle** , um ein Sicherheitsniveau zu gewährleisten, das den neuen technologischen Fortschritten und Best Practices für die Cybersicherheit entspricht.

- **Überwachen Sie** ständig Cyberbedrohungen, einschließlich solcher, die durch künstliche Intelligenz (KI) unterstützt werden, um potenzielle Eindringversuche zu antizipieren und die Abwehr entsprechend zu stärken.

12.4.1 Strategischer Schutz: Freemindtronic veröffentlicht nicht alle technischen Details seiner Sicherheitsmechanismen, um eine Analyse durch einen Angreifer oder eine künstliche Intelligenz zur Identifizierung einer möglichen Schwachstelle nicht zu erleichtern. Alle ergriffenen Maßnahmen entsprechen jedoch den **strengsten** Standards in Bezug auf Cybersicherheit und Datenschutz.

12.5. Betriebssicherheit und Schutz sensibler Daten

Freemindtronic wendet ein strenges Sicherheitsmodell an, das **maximalen Schutz vor den Risiken von interner und externer Spionage garantiert**.

12.5.1 Isolierung von Computersystemen

- Es sind keine Netzwerkverbindungen zwischen internen Systemen und keine Datei- oder Druckerfreigabe erlaubt.
- Jedes System ist völlig unabhängig, wodurch Schwachstellen im Zusammenhang mit externen Verbindungen vermieden werden.

12.5.2 Sichere Übertragung sensibler Daten

- Alle sensiblen Dateiübertragungen werden **ausschließlich** über die EviKey NFC **Secure USB-Flash-Laufwerke** von Freemindtronic durchgeführt.
- Diese Schlüssel verfügen über eine **automatische Selbstverriegelung,** wenn sie nicht verwendet werden, um unbefugten Zugriff zu verhindern.
- **In die Blackbox der EviKey NFC-Schlüssel ist ein Rückverfolgbarkeitsprotokoll integriert, mit dem jede Entsperrung und deren Geolokalisierung überprüft** werden kann**.**

12.5.3 Physische Isolierung und Sicherung von Produktionswerkzeugen

- Empfindliche Produktionsanlagen und Werkzeuge **sind niemals mit dem Internet verbunden** und werden nach dem Einsatz streng isoliert.
- Nach dem Gebrauch werden diese Werkzeuge **in einem speziellen Safe aufbewahrt, der** gegen Feuer und physisches Eindringen resistent ist.

12.5.4. Generieren und Sichern von Authentifizierungsschlüsseln

- Fälschungssichere Authentifizierungsschlüssel, die auch als **segmentierte Schlüssel dienen** , werden von den Produktionswerkzeugen **nach dem Zufallsprinzip generiert**.
- Diese Schlüssel **werden in den Produktionswerkzeugen weder angezeigt noch gespeichert**, so dass keine brauchbare Spur vorhanden ist.

12.5.5 Strenge Zugriffskontrolle und Minderung interner Risiken

- Nur **zwei Bevollmächtigte**, die gleichzeitig **Gesellschafter des Unternehmens** sind, sind berechtigt, die Produktionswerkzeuge zu nutzen.

- Diese Einschränkung zielt darauf ab, **die mit untergeordneten Beziehungen verbundenen Risiken zu minimieren** und die volle Kontrolle über den Zugang zu sensibler Infrastruktur zu gewährleisten.

12.6. Strenge Zugangskontrolle und Minderung interner Risiken

12.6.1 Zugriffssicherheit und systematische Verschlüsselung

Freemindtronic wendet fortschrittliche Authentifizierungs- und Verschlüsselungsprotokolle an, um sicherzustellen, dass alle digitalen Zugriffe und Medien vor Eindringlingen oder Diebstahlversuchen geschützt sind.

12.6.1.1 Schutz des Zugriffs auf Websites und NetzwerkeAlle Online- und lokalen Netzwerksysteme verwenden nur die folgenden starken Authentifizierungstechnologien:

- 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 und/oder DataShielder HSM PGP in der Cyber Defense-Version, die starke Authentifizierung und erweiterte Zugriffsverschlüsselung kombiniert.
- USB-Bluetooth-Tastaturemulatoren zur Sicherung der Eingabe sensibler Daten, indem das Risiko von Keylogging eliminiert wird.

12.6.1.2 Verschlüsselung von Daten- und SpeichermedienAlle Computersysteme (stationär, mobil) und Speichergeräte, die sensible Daten enthalten, werden mit Verschlüsselungsschlüsseln von 256 Bit oder mehr verschlüsselt.

- Vollständig verschlüsselte interne und externe Festplatten.
- Mobile Speicher- und Backup-Geräte, die durch Hardware- und/oder Softwareverschlüsselung geschützt sind.

12.6.1.3 Resilienz gegen physische und digitale EingriffeAlles ist darauf ausgelegt, sicherzustellen, dass im Falle eines Eindringens in die Räumlichkeiten von Freemindtronic, des Diebstahls digitaler Medien oder der unrechtmäßigen Extraktion sensibler Daten keine Daten nutzbar oder physisch zugänglich sind.

- Sichere Verschlüsselungsschlüssel in NFC-HSM-Geräten, um unbefugten Zugriff zu verhindern.
- Automatische Schlüsselverriegelung oder Verriegelung im Falle eines Kompromittierungsversuchs mit Black-Box-Rückverfolgbarkeit.

12.6.1.4 Integration von Produkten mit EviKey NFC-Technologie

Die Produkte von Freemindtronic mit **der EviKey NFC-Technologie** verwenden ausschließlich die **Fullkey Plus-App** für ihre Verwaltung und Sicherheit. Diese Technologie ist auch in die folgenden Cybersicherheitslösungen integriert:

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

Die Integration von EviKey NFC in diese Lösungen bietet eine fortschrittliche Zugriffskontrolle auf Speichermedien und umfasst die folgenden Funktionen:

- **Selbsthemmend bei Inaktivität**
- **Sichere Schlüsselverwaltung**

- **Rückverfolgbarkeit des Zugangs über eine Blackbox**, die dank der Anwendungen **Fullkey Plus**, **PassCypher NFC HSM** oder **DataShielder NFC HSM** nur kontaktlos über **ein NFC-Android-Telefon** zugänglich ist.

Freemindtronic geht in Sachen Sicherheit kein Risiko ein und lässt sich nicht überraschen: Hier **ist der Schuhmacher sicher nicht der schlechteste Beute** ! 😉

Freemindtronic implementiert **wasserdichte Sicherheitspartitionen**, die jede Form von Spionage, ob **intern oder extern**, verhindern und **maximalen Schutz** für digitale Assets und kritische Daten gewährleisten.

12.6.1.4 – Schutz vor KI und fortgeschrittenen Angriffen :

Freemindtronic implementiert spezifische Technologien und Protokolle, um sich vor KI-gestützten Angriffen zu schützen, einschließlich Deepfakes und Audio-/Videomanipulationen, die darauf abzielen, die digitale Identität von Führungskräften und Benutzern zu kompromittieren. Zu diesen Maßnahmen gehören eine verbesserte Überprüfung der Kommunikation und eine Multifaktorenanalyse sensibler Handelsgeschäfte.

12.7 – Umgang mit Datenschutzverletzungen :

Im Falle einer Hardware-Kompromittierung oder einer versuchten Sicherheitsverletzung, die die Infrastruktur von Freemindtronic betrifft, werden proaktiv Incident-Response-Verfahren durchgeführt, unabhängig davon, ob kein automatisiertes Erkennungssystem vorhanden ist.

Freemindtronic hat erkannt, dass es unrealistisch ist, selbst mit den besten Sicherheitsmaßnahmen der Welt einen absoluten Schutz vor einem entschlossenen Angreifer zu gewährleisten. Aus diesem Grund basiert der gewählte Ansatz auf einer **proaktiven und präventiven Strategie**, die international patentierte Innovationen integriert, die entwickelt wurden, um neue Formen der Spionage zu antizipieren, insbesondere solche, die durch **künstliche Intelligenz unterstützt werden**.

Die Cybersicherheitslösungen von Freemindtronic sind so konzipiert, dass sie verhindern, dass Daten ausgenutzt werden, selbst im Falle eines unbefugten physischen oder digitalen Zugriffs. Dieser Ansatz basiert auf fortschrittlichen Mechanismen wie Hardware-Selbstsperre, segmentierter Schlüsselverschlüsselung, Infrastrukturisolierung und der ausschließlichen Verwendung sicherer Medien wie EviKey NFC, PassCypher NFC HSM und DataShielder NFC HSM.

Für den Fall, dass ein Sicherheitsvorfall einen Kunden oder Partner betrifft, verpflichtet sich Freemindtronic**, diesen so schnell wie möglich** gemäß den Anforderungen der geltenden Datenschutzbestimmungen zu informieren.

ARTIKEL 13 – RECHTE DER NUTZER NACH ANDORRANISCHEM RECHT

In Übereinstimmung mit **den Artikeln 16 bis 21 des Gesetzes 29/2021** haben die Nutzer die folgenden Rechte, die mit der **DSGVO und der andorranischen Gesetzgebung** übereinstimmen:

- **Auskunftsrecht** : Um zu überprüfen, welche Informationen freiwillig zur Verfügung gestellt und verarbeitet wurden.
- **Recht auf Berichtigung** : Auf Berichtigung unrichtiger oder unvollständiger Daten.
- **Widerspruchsrecht** : Widersprechen Sie der Verwendung ihrer Daten.
- **Recht auf Löschung (Recht auf Vergessenwerden):** Die dauerhafte Löschung ihrer Daten zu verlangen.

- **Recht auf Übertragbarkeit** : Sie erhalten ihre Daten in einem lesbaren Format (neue Verpflichtung, die durch das Gesetz 29/2021 verschärft wurde).
- **Recht auf Einschränkung der Verarbeitung** : Beschränken Sie die Verarbeitung bestimmter Informationen.

13.1. Bearbeitungszeit für Anfragen

Freemindtronic garantiert, dass jeder Antrag auf Ausübung von Rechten **innerhalb einer Frist von maximal 30 Tagen bearbeitet** wird, außer in Ausnahmefällen, die eine **gerechtfertigte Verlängerung um bis zu 60 Tage** erfordern.

Anfragen können per E-Mail an folgende Adresse gerichtet werden:
contact [at] freemindtronic.com oder **dpo [at] freemindtronic.com**

ARTIKEL 14 – REGRESS IM STREITFALL

Wenn ein Nutzer der Ansicht ist, dass **seine Rechte nicht respektiert wurden**, kann er eine Beschwerde bei der **andorranischen Datenschutzbehörde (APDA), der** zuständigen Aufsichtsbehörde in Andorra**, einreichen**.

14.1. Beschwerdeverfahren

Gemäß **Artikel 25 des Gesetzes 29/2021** kann jede Person, die der Ansicht ist, dass die Verarbeitung ihrer Daten unter **Verstoß gegen die geltenden Gesetze** erfolgt ist :

- **Verweisen Sie die Angelegenheit an die andorranische Datenschutzbehörde (APDA)** zur administrativen Untersuchung.
  APDA-Kontakt : https://www.apda.ad

- **Einlegung eines Rechtsmittels bei den zuständigen Gerichten in Andorra** , um eine Entschädigung für den erlittenen Schaden zu erhalten.

Freemindtronic verpflichtet sich, **im Falle einer Untersuchung uneingeschränkt mit den Datenschutzbehörden** zusammenzuarbeiten.

ARTIKEL 15 – ÄNDERUNGEN DER DATENSCHUTZRICHTLINIE

15.1. Verpflichtung zur Aktualisierung

Freemindtronic verpflichtet sich, diese Richtlinie im Falle von gesetzlichen oder behördlichen Änderungen, die den Datenschutz betreffen, zu aktualisieren. Alle Änderungen werden explizit auf der offiziellen Freemindtronic-Website veröffentlicht.

15.2. Häufigkeit und Transparenz der Aktualisierungen

Freemindtronic veröffentlicht regelmäßig Updates für seine Software, Anwendungen und Erweiterungen. Es wird eine spezielle Aktualisierungsseite gepflegt, auf der Folgendes explizit aufgeführt ist:

- **Die vorgenommenen Änderungen,**
- **Verbesserungen der Sicherheit,**
- **Alle identifizierten und behobenen Schwachstellen.**

Die vollständige Versionshistorie der Freemindtronic Software, Anwendungen und Erweiterungen finden Sie hier: Freemindtronic Versionsgeschichte

15.3. Benachrichtigung der Nutzer

Benutzer, die über Aktualisierungen per E-Mail benachrichtigt werden möchten, müssen eine ausdrückliche Anfrage stellen, indem sie ihre E-Mail-Adresse an Freemindtronic übermitteln.

15.4. Information bei Änderungen der Funktionalitäten

Im Falle von Änderungen der Funktionalitäten, die mit der Datenverarbeitung verbunden sind, verpflichtet sich Freemindtronic, die Nutzer darüber zu informieren:

- **Durch Benachrichtigung auf der offiziellen Website,**
- **Über die betreffenden Anwendungen.**

ARTIKEL 16 – KONTAKTDATEN

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

Ende des Dokuments