PRIVACYBELEID – FREEMINDTRONIC SL

Website & Software – Versie en datum van het document: V2.0 van 28/02/2025

ARTIKEL 1 – INLEIDING

1.1. Identificatie van de verwerkingsverantwoordelijke

Dit privacybeleid is uitgegeven door **Freemindtronic SL,** een naamloze vennootschap die is geregistreerd onder de wetten van het Prinsdom Andorra, met statutaire zetel te:

Av. Co-Prince de Gaulle, 13, Valira Building, begane grond, AD700 Escaldes – Engordany, Andorra.

Freemindtronic is verantwoordelijk voor de verwerking van gegevens die worden verzameld of verwerkt door het gebruik van zijn officiële website https://freemindtronic.com evenals zijn software, applicaties, extensies en embedded systemen.

1.2. Champ d'Application

Dit privacybeleid is van toepassing op alle diensten, software, applicaties, extensies en embedded systemen die door Freemindtronic zijn ontwikkeld en worden geëxploiteerd.

Het is niet van toepassing op websites, diensten of platforms van derden die toegankelijk zijn via de diensten van Freemindtronic. Freemindtronic is niet verantwoordelijk voor het privacybeleid van deze diensten van derden.

1.3. Betrokkenheid: Zero Trust en Zero Knowledge

Freemindtronic houdt zich aan een strikt **Zero Trust & Zero Knowledge-framework**, dat ervoor zorgt dat gebruikersgegevens helemaal niet worden geopend, opgeslagen of gedeeld.

Alle software, applicaties, extensies en embedded systemen die door Freemindtronic zijn ontwikkeld, werken **zonder een externe server, een gecentraliseerde database, het aanmaken van een gebruikersaccount, gebruikersidentificatie en gegevensoverdracht**.

Alle functies van Freemindtronic zorgen ervoor dat gebruikersgegevens niet worden opgeslagen of verzonden naar externe servers. Alle verwerking vindt uitsluitend lokaal plaats op het apparaat van de gebruiker, zonder interactie met een externe infrastructuur.

1.4. Naleving van de regelgeving

- Freemindtronic voldoet aan de strengste internationale regelgeving op het gebied van gegevensbescherming en cyberbeveiliging, waaronder:
- Algemene Verordening Gegevensbescherming (AVG – Verordening (EU) 2016/679)
- Wet digitale operationele veerkracht (DORA – Règlement (UE) 2022/2554)
- NIS2-richtlijn (Richtlijn (EU) 2022/2555) betreffende de cyberbeveiliging van kritieke infrastructuur
- Californische wet op de privacy van consumenten (SCCA – VS, Cal. Civ. Code § 1798.100 e.v.)
- Algemene wet inzake gegevensbescherming (LGPD – Brésil, wet nr. 13.709/2018)
- Wet 15/2003 betreffende de bescherming van persoonsgegevens in Andorra, gewijzigd bij gekwalificeerde wet 29/2021
- Verordening (EU) 2021/821 van 20 mei 2021 betreffende de controle op de uitvoer van producten voor tweeërlei gebruik
- ISO/IEC 27001-normen en NIST (National Institute of Standards and Technology, VS) best practices op het gebied van beveiliging

1.5. DefinitiesIn dit beleid worden de volgende termen als volgt gedefinieerd:

- **Persoonsgegevens** : alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon, direct of indirect, met name door verwijzing naar een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator, of naar een of meer elementen die specifiek zijn voor zijn of haar fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit.
- **Gevoelige gegevens** : alle informatie waarvan de ongeoorloofde openbaarmaking kan leiden tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Dit omvat, maar is niet beperkt tot:
    - Unieke ID's (gebruikersnamen, wachtwoorden, authenticatiecodes).
    - Versleutelings- en authenticatiesleutels.
    - Betalingsgegevens en bankgegevens.
    - Vertrouwelijke gegevens van klanten en partners (commerciële strategieën, octrooien, documenten beschermd door bedrijfsgeheimen).
    - Alle persoonsgegevens die in de speciale categorieën van de AVG vallen (etnische afkomst, politieke opvattingen, religieuze overtuigingen, gezondheid, biometrie, seksleven).
- **Verwerking** betekent elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, aligneren of combineren; beperking, uitwissing of vernietiging.
- **Verwerkingsverantwoordelijke** : de natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of een ander orgaan die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
- **Verwerker** : de natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of ander orgaan die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
- **Toestemming** : elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting van de betrokkene waarmee hij of zij instemt, door middel van een verklaring of een ondubbelzinnige actieve handeling, met de verwerking van hem of haar betreffende persoonsgegevens.
- **Pseudonimisering** : verwerking van persoonsgegevens op zodanige wijze dat deze niet meer kunnen worden herleid tot een specifieke natuurlijke persoon zonder aanvullende informatie, die gescheiden moet worden gehouden en moet worden beschermd door passende technische en organisatorische maatregelen.
- **Anonimisering** : onomkeerbare transformatie van persoonsgegevens op zodanige wijze dat het niet langer mogelijk is om de betrokkene direct of indirect te identificeren.
- **Inbreuk op persoonsgegevens** : Elke inbreuk op de beveiliging die per ongeluk of onrechtmatig leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde openbaarmaking van of de ongeoorloofde toegang tot persoonsgegevens. Dit omvat ongeoorloofde toegang tot logins, wachtwoorden, coderingssleutels of andere beschermde gevoelige gegevens.

ARTIKEL 2 – VERZAMELING EN VERWERKING VAN GEGEVENS

2.1. Gebrek aan systematische gegevensverzameling

Freemindtronic verzamelt, bewaart, deelt of verkoopt geen persoonlijke of technische gegevens van gebruikers, behalve in het geval van directe interactie, inclusief aan:

- Een bestelling via officiële platformen.
- Een contactverzoek met betrekking tot klantenservice of een officieel partnerschap.

De gegevens worden alleen verwerkt in het kader van de strikte uitvoering van het contract of de zakelijke relatie en worden nooit voor andere doeleinden gebruikt.

2.2. Gegevens die kunnen worden verzameld

Als een gebruiker vrijwillig informatie verstrekt, worden alleen de strikt noodzakelijke gegevens verwerkt:

- Identiteit (naam, voornaam)
- Contactgegevens (e-mail, telefoon, factuur- en afleveradres)
- Professionele informatie
- Vrijwillig ingediende inhoud

Transactiegegevens worden uitsluitend gebruikt voor het beheer van bestellingen en de levering ervan, zonder overdracht aan derden, met uitzondering van wettelijke verplichtingen (belasting en boekhouding).

2.2.1 – Gegevens die lokaal zijn opgeslagen op de extensie of applicatieSommige Freemindtronic-applicaties en -extensies kunnen lokaal opslagruimte of de Web Storage API gebruiken om lokale instellingen tijdelijk op het apparaat van de gebruiker op te slaan. Deze gegevens worden nooit doorgegeven aan servers op afstand en zijn alleen toegankelijk binnen de gebruikte software.

2.3. Gegevensopslag en -beveiliging

Freemindtronic hanteert de hoogste beveiligingsstandaarden, in overeenstemming met **de AVG, DORA, NIS2, ISO/IEC 27001 en NIST-regelgeving**.

- **Veilige offline opslag** : Gegevens worden bewaard op versleutelde media die alleen toegankelijk zijn via EviKey NFC beveiligde USB-flashstations en/of versleutelde opslagmedia en/of versleutelde gegevens.
- **Zero Trust & Zero Knowledge** : Gebrek aan externe servers en gecentraliseerde databases om gevoelige gegevens op te slaan en/of te beheren voor alle Freemindtronic-producten.
- **Verbeterde beveiliging van gevoelige communicatie**: De uitwisseling van gevoelige gegevens vindt uitsluitend plaats via **DataShielder-tools** of een beveiligd protocol dat door de klant is gedefinieerd.
- **Opgelegd alternatief indien nodig** : Als de service van de klant geen voldoende beveiligingsniveau garandeert, biedt Freemindtronic **DataShielder** aan als het enige veilige kanaal.

2.4. Bescherming van gerubriceerde gegevens en gevoelige omgevingen

Freemindtronic-oplossingen die zijn geïdentificeerd als een civiel en militair product voor tweeërlei gebruik, zijn ontworpen om kritieke informatie te beschermen en omvatten:

- **Fysieke isolatie en partitionering** : Er worden geen gegevens opgeslagen op een externe server.

- **Sterke authenticatie** : NFC HSM en gepatenteerde versleuteling met gesegmenteerde sleutels. Het gebruik van RSA-4096 asymmetrische encryptie maakt het mogelijk om AES-256 CBC-sleutels veilig te delen tussen HSM NFC-apparaten, ook op afstand, zonder overdracht via gecentraliseerde infrastructuren. Dit mechanisme elimineert het risico van exfiltratie van sleutels en biedt geavanceerde bescherming voor versleutelde uitwisselingen.
- **End-to-end encryptie** : AES-256 CBC, RSA-4096, PGP - Alle veilige symmetrische encryptiesystemen worden gerealiseerd via gesegmenteerde sleutels en gepatenteerde, internationaal geleverde toegangscontrolesystemen. Deze architectuur maakt versleuteling bestand tegen kwantumaanvallen, waardoor gevoelige gegevens op lange termijn worden beschermd.
- **Gedecentraliseerde logboekregistratie** : Lokale black box die alleen in NFC toegankelijk is door een geautoriseerde beheerder.
- **Stresstesten en proactieve cyberbeveiliging** : Regelmatige beoordelingen tegen APT-aanvallen, industriële spionage en geavanceerde cyberdreigingen.

Als een Freemindtronic-extensie of -applicatie toegang heeft tot lokale bestanden op een Windows- of Mac-apparaat (bijvoorbeeld om coderingssleutels of beveiligde bestanden op te slaan), worden deze bestanden uitsluitend lokaal verwerkt en zijn ze nooit toegankelijk voor derden. De gebruiker behoudt de volledige controle over zijn gegevens en deze worden niet gedeeld met andere diensten.

2.5. Opslag, verwijdering en bewaring van klantgegevens

- De gegevens die via een contactformulier worden verstrekt, worden alleen gebruikt om op het verzoek te reageren en onmiddellijk na verwerking verwijderd.
- Klantgegevens die voortvloeien uit transacties worden slechts bewaard gedurende de noodzakelijke wettelijke periode, in overeenstemming met de regelgeving die van toepassing is in de volgende rechtsgebieden:
    - **Andorra: Gekwalificeerde wet 29/2021 – bewaring van belastingdocumenten gedurende 5 jaar**
    - **Europese Unie: Artikel 6 van de Richtlijn Consumentenbescherming 2011/83/EU – bewaring van transactiegegevens tot 10 jaar, afhankelijk van de lokale boekhoudkundige vereisten**
    - **Frankrijk: Artikel L123-22 van het Franse Wetboek van Koophandel – verplichte bewaring van boekhoudkundige documenten gedurende 10 jaar**
    - **VS: IRS-publicatie 583 - 3-7 jaar bewaren van transactiegegevens**
- **Er worden geen bankgegevens opgeslagen** : de verwerking van transacties vindt plaats via **beveiligde externe aanbieders** (bijv. PayPal).

2.6. Internationale gegevensoverdracht

Freemindtronic draagt geen gegevens over buiten de EER, tenzij een adequaat wettelijk kader wordt toegepast (**Standard Contractual Clauses - SCC's**).

2.7. Procedure voor datalekken

In overeenstemming met de artikelen 33 en 34 van de **AVG** en de **gekwalificeerde wet 29/2021** past Freemindtronic een **proactieve reactie toe** in geval van een incident:

- **Onmiddellijke inperkings-** en **impactanalyse**.

- **Kennisgeving binnen 72 uur** aan het Andorrese agentschap voor gegevensbescherming (APDA) indien nodig.
- **Getroffen gebruikers informeren** als er een hoog risico wordt vastgesteld.
- **Audit na het incident** om de beschermingsmaatregelen te versterken.

2.8. Cyberweerbaarheid en bescherming tegen rampen en cyberaanvallen

Freemindtronic garandeert **de integriteit en beschikbaarheid** van gegevens, zelfs in het geval van een storing, diefstal, ramp of massale cyberaanval.

2.8.1. Versleuteling en veilige back-up

- **Geavanceerde versleuteling** : AES-256 CBC, AES-256 CBC PGP, BitLocker met sleutels opgeslagen **op NFC HSM PassCypher**.
- **Scheiding van sleutels en gegevens**: Ontsleutelingssleutels worden nooit opgeslagen op hetzelfde medium als de gegevens. AES-256 CBC-coderingssleutels zijn zeer veilig en kunnen worden gedeeld via NFC HSM DataShielder, en werken contactloos, serverloos en databasevrij. Dit mechanisme zorgt voor een veilige overdracht van sleutels, zelfs op afstand, waardoor elk risico op onderschepping door derden wordt geëlimineerd.
- **Versleutelde en redundante back-ups**: gegevens die offline en veilig **over meerdere media** worden gerepliceerd.

2.8.2. Betere bescherming tegen cyberaanvallen

- **Ransomware en over-encryptie** : Versleutelde offline back-ups en fysiek uitbestede sleutels offline voorkomen manipulatie of frauduleus herstel.
- **Geavanceerde cyberaanvallen (APT, Zero-Day, Spionage):** Zero Trust & Zero Knowledge-architectuur en **fysieke sleutelscheiding** voorkomen exfiltratie. De beveiligingsarchitectuur van Freemindtronic, met gepatenteerde gesegmenteerde coderingssystemen en op hardware gebaseerde toegangscontrole, zorgt ervoor dat er geen privésleutels of versleutelde gegevens kunnen worden geëxfiltreerd, zelfs niet onder fysieke of logische beperkingen. De combinatie van AES-256 CBC-codering en RSA-4096 verhoogt de weerbaarheid tegen geavanceerde aanvallen, inclusief aanvallen met behulp van kunstmatige intelligentie.
- **Weerbaarheid zonder cloud: Geen afhankelijkheid van externe servers**, waardoor het risico op gecentraliseerde aanvallen wordt geëlimineerd.

2.8.3. Weerbaarheid tegen fysieke rampen en onopzettelijke verliezen

De protocollen van Freemindtronic zorgen altijd voor toegang tot gegevens die zijn versleuteld met hun sleutels, zelfs in het geval van:

- **Diefstal of verlies** van versleutelde media: Zonder **uitbestede sleutels** blijven gegevens onbruikbaar.
- **Onopzettelijke vernietiging of natuurramp** : Dubbele **back-ups** zorgen ervoor dat gevoelige gegevens worden hersteld.
- **Geografische isolatie van back-ups** : Versleutelde **media** worden op verschillende veilige locaties bewaard, waardoor totale compromittering wordt voorkomen.

2.9. Geheimhoudingsovereenkomsten (NDA's) en vertrouwelijkheid van de handel

Alle zakelijke relaties met Freemindtronic waarbij gevoelige of vertrouwelijke informatie wordt uitgewisseld, worden routinematig gedekt door een **geheimhoudingsovereenkomst (NDA).**

- **Strikte toepassing** : Alle informatie die wordt uitgewisseld in het kader van partnerschappen, technische samenwerkingen of zakelijke besprekingen wordt beschermd door wettelijk bindende vertrouwelijkheidsclausules. Alle gevoelige documenten, al dan niet versleuteld, die met klanten en partners worden uitgewisseld, worden systematisch digitaal ondertekend via de functie die is ingebed in DataShielder HSM PGP. Deze digitale handtekening garandeert de integriteit en authenticiteit van de documenten en zorgt ervoor dat er geen beschadiging of wijzigingen zijn aangebracht nadat ze zijn uitgegeven. Daarnaast is e-mailcommunicatie met gevoelige informatie altijd beveiligd via PGP, waardoor onderschepping of manipulatie van berichten wordt voorkomen.
- **Reikwijdte van de NDA** : De NDA omvat **documenten, communicatie, technische uitwisselingen, innovaties, interne gegevens**, evenals alle vertrouwelijke informatie die door Freemindtronic wordt verzonden of van een partner wordt ontvangen.
- **Sancties voor overtredingen** : Elke ongeoorloofde openbaarmaking van vertrouwelijke informatie is onderhevig aan **contractuele en juridische sancties** , waaronder juridische stappen voor schending van vertrouwelijkheid en handelsgeheimen.
- **Beschermingstermijn**: Geheimhoudingsverplichtingen blijven van kracht, **zelfs na het einde van de contractuele relatie**, volgens de termijn die in elke overeenkomst is gedefinieerd.

Deze clausule versterkt de toewijding van Freemindtronic om alle kritieke informatie die in het kader van zijn activiteiten wordt uitgewisseld te beschermen en zorgt voor een strikt wettelijk kader tegen lekken of compromittering.

ARTIKEL 3 – GEBRUIK VAN SENSOREN EN TOEGANG TOT LOCATIEGEGEVENS

Sommige Freemindtronic-software, -applicaties of -extensies vereisen mogelijk toegang tot de sensoren op de apparaten van gebruikers.

3.1 Deze sensoren omvatten:

- **GPS** (exacte locatie)
- **Wi-Fi en mobiele netwerken** (locatie bij benadering)
- **Bluetooth** (lokale detectie zonder externe transmissie)
- **Biometrische gegevens** (vingerafdruk, gezichtsherkenning)
- **Microfoon en camera** (alleen met expliciete toestemming)
- **Omgevingssensoren** (versnellingsmeter, gyroscoop, nabijheidssensoren, helderheid)
- **Beveiligingsmodules** (NFC, HSM, HSM, PGP)

3.2 Alle gegevens die door deze sensoren worden gegenereerd:

- **Ze blijven uitsluitend op het apparaat van de gebruiker** staan en worden in geen geval doorgegeven aan een externe server of een dienst van derden.
- **Zijn niet onderhevig aan externe of externe opslag**.

- **Zijn alleen toegankelijk met expliciete toestemming van de gebruiker**, met name voor gevoelige sensoren zoals microfoon en camera.
- **Kan worden beheerd door de gebruiker**, die de verleende machtigingen op elk moment kan wijzigen of intrekken via de instellingen van zijn apparaat.

De sensoren van de apparaten (camera, microfoon, NFC, GPS, Wi-Fi, Bluetooth) worden alleen lokaal gebruikt en verzenden nooit gegevens naar externe servers, derden of andere Freemindtronic-diensten. De gebruiker kan deze toegang beheren en uitschakelen via de instellingen van zijn apparaat.

3.4 Ervoor zorgen dat sensorgegevens niet worden gebruikt voor het volgen van gedrag

Freemindtronic zorgt ervoor dat **de gegevens die via apparaatsensoren worden verzameld, nooit worden gebruikt voor het volgen van gedrag, gerichte advertenties of gebruikersprofilering**.

De toegang tot de sensoren is strikt beperkt tot essentiële softwarefuncties en alleen na het verkrijgen van de uitdrukkelijke toestemming van de gebruiker.

Op basis van deze gegevens wordt geen analyse van gebruikspatronen uitgevoerd en deze worden niet opgeslagen of doorgegeven aan derden.

ARTIKEL 4 – NALEVING VAN DISTRIBUTIEPLATFORMS

De door Freemindtronic **ontwikkelde software, applicaties en extensies** voldoen aan de eisen van de volgende platformen:

- **Google Play Console** (applicaties Android)
- **Chrome Web Store** (browserextensies)
- **Microsoft Store- en Edge-add-ons** (Windows-apps en browserextensies)
- **Apple, macOS en iOS** (apps die worden gedistribueerd in de App Store)

Freemindtronic zet zich in om zich te houden aan de **beveiligings- en privacyrichtlijnen** die door deze platforms worden opgelegd.

- **De Zero Trust & Zero Knowledge-architectuur is gegarandeerd** , zodat er geen gebruikersgegevens worden verzameld, verzonden of opgeslagen buiten het apparaat van de gebruiker.
- **Er is geen integratie met diensten van derden** om de risico's die gepaard gaan met het volgen of verzamelen van persoonsgegevens te beperken.
- **De vereisten van elk platform worden regelmatig herzien** om ervoor te zorgen dat voortdurend wordt voldaan aan wijzigingen in de toepasselijke regelgeving.

SECTIE 5 – NON-DISCRIMINATIECLAUSULE (CCPA-NALEVING)

In overeenstemming met de bepalingen van de **California Consumer Privacy Act (CCPA) garandeert Freemindtronic dat gebruikers niet worden gediscrimineerd** bij de uitoefening van hun rechten met betrekking tot de bescherming van persoonsgegevens.

Er zullen geen beperkingen of beperkingen worden toegepast op gebruikers die hun rechten willen uitoefenen, in het bijzonder met betrekking tot:

- Toegang tot hun persoonsgegevens.
- Rectificatie van onjuiste of onvolledige informatie.
- Verwijdering van vrijwillig verstrekte gegevens.
- Bezwaar maken tegen of beperking van de verwerking van hun gegevens.

Freemindtronic verbindt zich ertoe geen extra kosten of wijzigingen in de toegang tot functies in rekening te brengen als reactie op een verzoek van een gebruiker om rechten uit te oefenen.

Elke gebruiker die zijn rechten wil doen gelden, kan rechtstreeks contact opnemen met Freemindtronic via de contactgegevens in dit privacybeleid.

In overeenstemming met de CCPA zal de uitoefening van de rechten inzake de bescherming van persoonsgegevens (toegang, verwijdering, verzet) niet leiden tot enige wijziging, beperking of verslechtering van de door Freemindtronic aangeboden diensten.

ARTIKEL 6 – GEEN PROFILERING EN VINGERAFDRUKKEN

6.1. Afwezigheid van profilering en geautomatiseerde beslissingen

Freemindtronic voert geen profilering, gedragstracking of geautomatiseerde besluitvorming uit die van invloed is op gebruikers.

- Er wordt geen analyse van gebruikersactiviteit uitgevoerd.
- Er wordt geen algoritme voor kunstmatige intelligentie gebruikt om gebruikers te classificeren.
- Er is geen mechanisme voor het personaliseren van diensten op basis van gebruikersgegevens.

6.2. Absence de Fingerprinting

Vingerafdrukken zijn een techniek waarbij specifieke informatie over de hardware of software van een apparaat wordt verzameld, zoals IP-adres, besturingssysteem, schermresolutie en andere parameters, om een unieke digitale vingerafdruk van de gebruiker te creëren. In tegenstelling tot cookies is deze methode moeilijk te detecteren en te blokkeren, wat grote privacyproblemen met zich meebrengt.

In december 2024 **kondigde Google aan dat het vanaf 16 februari 2025 adverteerders zou toestaan vingerafdrukken te gebruiken** voor het volgen van gebruikers, waarmee het beleid uit 2019 dat de praktijk verbood, werd teruggedraaid. De stap kreeg kritiek van regelgevers zoals **het Britse Information Commissioner's Office (ICO),** dat de verandering "onverantwoordelijk" noemde vanwege de vermindering van de keuze en controle die individuen hebben over het verzamelen van hun informatie.

Bij **Freemindtronic** doen we er alles aan om de privacy van onze gebruikers te respecteren. Daarom gebruiken we **geen enkele vorm van vingerafdrukken** in onze producten of diensten. **Google kondigde in december 2024 aan dat het vanaf 16 februari 2025 vingerafdrukken voor adverteerders zou toestaan** (officiële bron - https://blog.google/products/ads-commerce/privacy-sandbox-fingerprinting-policy-change).

De stap leidde tot bezorgdheid van toezichthouders, waaronder **de Britse ICO**. Freemindtronic verwerpt deze praktijken en garandeert dat **er geen tracking, apparaatidentificatie of gedragsprofilering** wordt geïmplementeerd.

Alle Freemindtronic IT-systemen zijn **volledig geïsoleerd en onafhankelijk** van elkaar. **Er worden geen gebruikersgegevens geregistreerd, opgeslagen of getraceerd** via een uitsluitend lokale en offline operatie. **Het gebruik van hardware-encryptie en NFC HSM-authenticatieoplossingen** zorgt ervoor dat er geen digitale vingerafdruk aan gebruikers kan worden gekoppeld, onder meer door het gebruik van de EviBITB-technologie van Freemindtronic.

Freemindtronic implementeert een **geavanceerde cyberbeveiligingsstrategie** om zich te beschermen tegen AI-ondersteunde aanvallen, CEO-fraude en andere identiteitsdiefstal.

- De **e-mails die worden gebruikt voor externe communicatie** zijn **sandbox-adressen en no-reply e-mails** om **het risico op spoofing en phishing te verkleinen**.
- Het openen van een bijlage is onderworpen aan een **strikt controlebeleid om** elk risico op kwaadaardige bestanden **te vermijden**.
- Elke **vraag van de klant** wordt systematisch geverifieerd door **een tweede communicatiekanaal** om de **authenticiteit ervan te bevestigen** (proactieve verwijdering van twijfel).

Freemindtronic garandeert **dat het nooit vingerafdrukken van apparaten zal verzamelen, analyseren of gebruiken** via indirecte identificatiemethoden (bijv. schermresolutie, apparaatmodel, browsertaal).

ARTIKEL 7 – NALEVING VAN DE VERORDENING INZAKE PRODUCTEN VOOR TWEEËRLEI GEBRUIK

7.1. Exportvoorschriften en -vergunningen

Freemindtronic handhaaft strikt de regelgeving voor het beheer en de export van cyberbeveiligingstechnologieën, ook voor **coderingsproducten die zijn geclassificeerd als civiel en militair voor tweeërlei gebruik**.

DataShielder NFC HSM-producten hebben een **invoervergunning in Frankrijk ontvangen van het Prinsdom Andorra**, gevalideerd **op 7 december 2024** via het bedrijf **AMG Pro**, in overeenstemming met **decreet nr. 2001-1192 van 13 december 2001**, gewijzigd bij **decreet nr. 2024-95 van 8 februari 2024**.

Deze toestemming werd verkregen na indiening van het dossier bij de **ANSSI**, die, in overeenstemming met haar opdracht om de naleving van **de wettelijke vereisten te controleren**, niet heeft geweigerd binnen de termijnen die in de geldende wetgeving zijn bepaald.

Sinds **7 februari 2025** zijn **DataShielder NFC HSM-producten** ook **toegestaan voor wederuitvoer** vanuit Frankrijk naar de lidstaten van de Europese Unie, in overeenstemming met **Verordening (EU) 2021/821 van 20 mei 2021** betreffende producten voor tweeërlei gebruik.

7.2. Referentie teksten

Deze machtiging wordt verleend op grond van de volgende teksten:

- **Decreet nr. 2001-1192 van 13 december 2001**, gewijzigd bij **het decreet van 8 februari 2024**, betreffende de controle op de uitvoer en overdracht van goederen en technologieën voor tweeërlei gebruik.
- **Verordening (EU) 2021/821 van 20 mei 2021** tot vaststelling van een regeling voor controle op de uitvoer van producten voor tweeërlei gebruik.

7.3. Verbintenis tot controle

Freemindtronic zet zich in voor **regelmatige nalevingsaudits** om ervoor te zorgen dat **de wet- en regelgeving blijft naleven**. Deze interne audits worden periodiek uitgevoerd in overeenstemming met de geldende wettelijke vereisten.

ARTIKEL 8 – CERTIFICERINGEN EN AUDITS

8.1. Geen cloudcertificeringsvereiste

Freemindtronic vereist geen **SOC 2-** of **ISO 27001-certificeringen** die specifiek zijn voor cloudinfrastructuren, aangezien **er geen externe servers worden gebruikt** voor gegevensverwerking of opslag.

De producten zijn ontworpen met een **100% air-gapped** aanpak, waardoor **volledige isolatie van gebruikersgegevens van** elke externe netwerkinfrastructuur wordt gegarandeerd. Deze architectuur rechtvaardigt **de afwezigheid van bepaalde audits** die normaal gesproken worden toegepast op aangesloten systemen.

8.2. Veiligheidsaudit en kwaliteitscontrole

Deze aanpak **wordt toegepast in de hele waardeketen**, van **productontwerp** tot **productie**. Alle uitgevoerde audits zijn gericht op het waarborgen van de **veerkracht, fraudebestendigheid en datalekvrij van** de systemen van Freemindtronic.

Naast interne audits om productconformiteit te garanderen, past Freemindtronic **verbeterde controles toe op betalingsbeheer** en **bescherming van financiële transacties**.

- Het boekhoud- en financiële beheersysteem is geïsoleerd en geen enkele transactie kan worden gevalideerd zonder sterke authenticatie via DataShielder NFC HSM Auth en DataShielder MAuth, waardoor sterke authenticatie wordt gegarandeerd en het risico op fraude wordt geëlimineerd.
- De toegang tot bankrekeningen en betalingssystemen is strikt beperkt tot geautoriseerde aandeelhouders, zonder een relatie van ondergeschiktheid, om de interne risico's van fraude te beperken.

ARTIKEL 9 – FUNCTIONARIS VOOR GEGEVENSBESCHERMING (DPO)

9.1. Benoeming van de DPO

In overeenstemming met de vereisten van de **Algemene Verordening Gegevensbescherming (AVG – Verordening (EU) 2016/679)** en andere toepasselijke regelgeving, heeft Freemindtronic een functionaris voor **gegevensbescherming (DPO) aangesteld** die verantwoordelijk is voor het waarborgen van de naleving van de bescherming van persoonsgegevens door het bedrijf.

De **DPO van Freemindtronic** is:

- **Naam:** Jacques Gascuel
- **Functie:** CEO en DPO van Freemindtronic SL
- **Contact :** dpo [at] freemindtronic.com

9.2. Opdrachten van de DPO

De DPO van Freemindtronic voert verschillende essentiële missies uit, waaronder:

- Ervoor zorgen dat **de gegevensverwerking voldoet** aan de toepasselijke regelgeving (**GDPR, CCPA, LGPD, enz.**).
- Freemindtronic informeren en adviseren over **haar verplichtingen op het gebied van gegevensbescherming**.
- Toezicht houden **op de toepassing van het ingevoerde beveiligings- en gegevensbeschermingsbeleid** .
- Reageren op verzoeken van gebruikers met betrekking tot **hun rechten (toegang, rectificatie, verwijdering, verzet, enz.)**.
- Contacten onderhouden met **gegevensbeschermingsautoriteiten**, waaronder het **Andorrese agentschap voor gegevensbescherming** en relevante Europese of internationale autoriteiten.

9.3. Contact en klachten

Elke gebruiker die informatie wenst over **het beheer van zijn persoonsgegevens** of zijn rechten wil uitoefenen, kan contact opnemen met **de DPO van Freemindtronic** op het volgende adres:

- **E-mail :** dpo [at] freemindtronic.com
- **Postadres:**
  Freemindtronic SLAv. Co-Prince de Gaulle, 13, Valira Building, begane grond, AD700 Escaldes – Engordany, Andorra

Als er binnen 30 dagen **geen antwoord wordt gegeven**, kan de gebruiker de zaak rechtstreeks voorleggen **aan het Andorrese agentschap voor gegevensbescherming (APDA)** wegens **niet-naleving van de wettelijke verplichting om binnen 30 dagen te reageren**.

ARTIKEL 10 – SPECIFIEKE EISEN VOOR DISTRIBUTIEPLATFORMS

10.1. Google Play-console (Android)

Freemindtronic-apps verzamelen, bewaren of verzenden geen persoonlijke gegevens. Sommige Android-machtigingen (zoals NFC, opslag, camera) worden alleen gebruikt om productfunctionaliteit mogelijk te maken en worden niet misbruikt voor doeleinden van derden. Er worden geen gegevens gedeeld met derden en alle bewerkingen worden lokaal uitgevoerd op het apparaat van de gebruiker, in overeenstemming met het privacybeleid van Google Play.

10.1.1. Naleving van het Google Play-beleid met betrekking tot gevoelige gegevens en machtigingenFreemindtronic-apps die toegang vereisen tot gevoelige Android-functies (NFC, opslag, camera, microfoon, GPS, SMS, RCS, MMS) voldoen aan de volgende vereisten:

- **Uitdrukkelijke toestemming** : Standaard zijn er geen machtigingen ingeschakeld. De gebruiker moet deze handmatig inschakelen via de instellingen van het apparaat.
- **Naadloos gebruik** : Toegang tot deze functies is **strikt beperkt tot** de essentiële behoeften van de app en de gegenereerde gegevens blijven **uitsluitend op het apparaat**.
- **Geen misbruik van machtigingen** : Freemindtronic vraagt nooit om toegang tot overbodige functies en respecteert het transparantiebeleid van Google Play.

10.1.2. Gegevensbescherming en lokale opslagAlle gegevens blijven strikt opgeslagen op het apparaat van de gebruiker en **zijn alleen toegankelijk voor de app zelf**. Er worden geen gebruikersgegevens opgeslagen op **externe servers** of gedeeld met **derden**.

10.2 – Chrome Web Store (Chrome-extensies)

Freemindtronic-extensies verzamelen of delen geen gebruikersgegevens. Ze kunnen localStorage gebruiken om tijdelijk lokale informatie op te slaan die nodig is om de extensie goed te laten functioneren.

Er wordt geen verborgen tracking uitgevoerd, geen overdracht van gegevens aan derden en geen ongerechtvaardigde toegang tot cookies of browsegeschiedenis.

10.2.1 Lokale opslag gebruikenFreemindtronic-extensies gebruiken uitsluitend de localStorage and Web Storage API om instellingen tijdelijk op te slaan die nodig zijn voor de goede werking ervan.
Deze gegevens:

- **Worden nooit verzonden naar externe servers.**
- **Zijn alleen toegankelijk voor de gebruiker en alleen in de context van de extensie.**
- **Instellingen die lokaal zijn opgeslagen via localStorage en Web Storage bevatten geen persoonlijke of gevoelige gegevens.**
- **Gebruikers kunnen opgeslagen lokale gegevens handmatig wissen via een optie "Gegevens verwijderen" die in de extensie is ingebouwd.**

10.3. Microsoft Store- en Edge-add-ons (Windows)

Freemindtronic-apps en -extensies voldoen aan de privacynormen van Microsoft.

Als een applicatie toegang heeft tot lokale bestanden (bijvoorbeeld veilige opslag van coderingssleutels), blijven deze bestanden geïsoleerd en worden ze nooit gedeeld met services van derden.

Freemindtronic garandeert dat er geen verborgen vingerafdrukken of tracking zullen zijn, in overeenstemming met het beleid van de Microsoft Store.

10.3.1. Lokale bescherming tegen bestandstoegang (Windows)
Sommige Freemindtronic-toepassingen hebben mogelijk toegang tot lokale bestanden nodig om **gevoelige gegevens te versleutelen, te beschermen of te verifiëren**.
Deze bestanden:

- **Worden nooit doorgestuurd naar een externe server.**
- **Blijven uitsluitend opgeslagen en verwerkt op het apparaat van de gebruiker.**
- **Zijn alleen toegankelijk voor lokaal geïnstalleerde applicaties met toestemming van de gebruiker.**

10.4. Apple App Store (macOS en iOS)

Freemindtronic-apps volgen geen gebruikers, verzamelen geen gegevens voor advertentieprofilering en verzenden geen informatie buiten het apparaat.

Als een app toegang heeft tot iOS/macOS-sensoren (bijv. NFC, microfoon, GPS), is dit gebruik strikt beperkt tot essentiële en door de gebruiker te beheren functies.

Als API's van derden worden gebruikt (bijv. betaling via Apple Pay), voldoet de impact ervan op gebruikersgegevens aan de vereisten van Apple en is deze volledig transparant voor de gebruiker.

10.4.1. Naleving van het App Tracking Transparency (ATT)-beleidFreemindtronic garandeert **dat het geen advertentie-ID's** of **tools voor het volgen van gebruikers** gebruikt voor marketing- of advertentiedoeleinden.
In overeenstemming met de richtlijnen van Apple:

- **Er worden geen gebruikersgegevens verzameld voor profilering of reclametargeting.**
- **Er is geen integratie met advertentie- of analyseservices van derden.**
- **Er wordt geen Apple ID (IDFA) gebruikt om gebruikersactiviteit in andere apps bij te houden.**
- **Freemindtronic verzamelt of deelt geen locatiegegevens op de achtergrond of zonder uitdrukkelijke toestemming van de gebruiker.**
- **Apps verzenden geen gegevens vanaf het apparaat, tenzij de gebruiker vrijwillig een actie uitvoert waarvoor gegevensuitwisseling vereist is.**

ARTIKEL 11 – NALEVING VAN DE ANDORRESE WETGEVING INZAKE GEGEVENSBESCHERMING

11.1. Toepassing van de Andorrese wetgeving

Freemindtronic is als bedrijf geregistreerd in **het Prinsdom Andorra** onderworpen aan de lokale regelgeving inzake **gegevensbescherming**, waaronder:

- **Gekwalificeerde wet 15/2003 van 18 december 2003** betreffende de bescherming van persoonsgegevens
- **Gekwalificeerde wet 29/2021 van 28 oktober 2021**, die Andorra in overeenstemming brengt met de beginselen van **de Algemene Verordening Gegevensbescherming (AVG – Verordening (EU) 2016/679)**

Deze wetten garanderen een **kader voor gegevensbescherming** dat gelijkwaardig is aan de Europese normen en die **door de Europese Unie** als adequaat worden erkend in overeenstemming met **artikel 45 van de AVG**.

Naast de huidige regelgeving **implementeert Freemindtronic geavanceerde fysieke en softwaremaatregelen om absolute gegevensbescherming te garanderen**. Dit omvat **volledige versleuteling van digitale media, NFC HSM multi-factor authenticatie en fysieke isolatie van IT-infrastructuren**. Deze maatregelen zorgen voor **de volledige naleving van de artikelen 10 en 45 van de AVG** en garanderen een gegevensbescherming die gelijkwaardig is aan de strengste Europese normen.

ARTIKEL 12 – NALEVINGSBEGINSELEN EN GEGEVENSBEVEILIGING

12.1. Privacy door ontwerp

Freemindtronic integreert **gegevensbescherming** in het **ontwerp van zijn software en diensten**, in overeenstemming met de principes van **privacy by design en privacy by default**.

12.2. Geen gegevensopslag

In overeenstemming met **de Zero Trust & Zero Knowledge-aanpak slaat Freemindtronic geen persoonsgegevens op of verwerkt deze niet**, behalve in het geval van vrijwillige verstrekking door de gebruiker (bijv. contactformulier, technische ondersteuning).

12.3. Vaststelling van verbeterde beveiligingsmaatregelen

Freemindtronic implementeert **geavanceerde beveiligingsmaatregelen** om gegevensbescherming **te waarborgen** en inbreuken te voorkomen, waaronder:

- **Versleutel systematisch** gebruikerscommunicatie en transacties via de gepatenteerde versleutelingssystemen met gesegmenteerde sleutels
- **Gebrek aan unieke** identificatiecodes die kunnen worden gebruikt om gebruikersactiviteit te volgen
- **Regelmatige interne auditeerbaarheid** om naleving van de huidige regelgeving te garanderen

Deze maatregelen zijn in overeenstemming met **artikel 10 van de Gekwalificeerde Wet 29/2021** betreffende de bescherming van persoonsgegevens in Andorra.

Freemindtronic past een uitgebreide cyberbeveiligingsstrategie toe die gegevensbescherming garandeert, zelfs in het geval van een fysieke inbraak in het pand:

Alle computersystemen (vaste, mobiele, server- en opslagapparaten) zijn volledig versleuteld met ≥256-bits sleutels.

Alle sites die online of op een lokaal netwerk zijn verbonden, maken gebruik van PassCypher NFC HSM en PassCypher HSM PGP met TOTP/HOTP en/of DataShielder NFC HSM en DataShielder HSM PGP Cyber Defense.

Er zijn geen coderingssleutels opgeslagen of zichtbaar op de productietools.

Gevoelige media (USB-sticks, harde schijven) worden opgeslagen in een brand- en inbraakwerende kluis.

Elke extractie van gevoelige gegevens is onmogelijk, zelfs in het geval van fysieke diefstal van servers of illegale exfiltratie van bestanden.

Deze maatregelen zorgen ervoor dat zelfs in het geval van een inbraak in het terrein van Freemindtronic geen gegevens kunnen worden misbruikt, zelfs niet in het geval van een succesvolle onrechtmatige inbraak.

12.4. Inzet voor voortdurende veiligheid

Freemindtronic stelt **gegevensbescherming** centraal in haar activiteiten en zet zich in voor:

- **De beveiligingsmaatregelen voortdurend verbeteren** door gelijke tred te houden met veranderende bedreigingen en regelgeving.
- **De beschermingsprotocollen aanpassen** om een beveiligingsniveau te garanderen dat in overeenstemming is met nieuwe technologische ontwikkelingen en best practices op het gebied van cyberbeveiliging.
- **Houd cyberdreigingen voortdurend in de gaten** , inclusief die met behulp van kunstmatige intelligentie (AI), om te anticiperen op mogelijke inbraakpogingen en de verdediging dienovereenkomstig te versterken.

12.4.1 Strategische bescherming: Freemindtronic maakt niet alle technische details van zijn beveiligingsmechanismen openbaar om geen analyse door een aanvaller of kunstmatige intelligentie te vergemakkelijken die een mogelijke kwetsbaarheid probeert te identificeren. Alle genomen maatregelen voldoen echter aan de **strengste normen** op het gebied van cyberbeveiliging en gegevensbescherming.

12.5. Operationele beveiliging en bescherming van gevoelige gegevens

Freemindtronic hanteert een streng beveiligingsmodel dat **maximale bescherming garandeert tegen de risico's van interne en externe spionage**.

12.5.1 Isolatie van computersystemen

- Er zijn geen netwerkverbindingen tussen interne systemen en het delen van bestanden of printers is niet toegestaan.
- Elk systeem is volledig onafhankelijk, waardoor kwetsbaarheden met betrekking tot externe verbindingen worden vermeden.

12.5.2 Veilige overdracht van gevoelige gegevens

- Alle overdracht van gevoelige bestanden wordt **uitsluitend** uitgevoerd via Freemindtronic**'s EviKey NFC** beveiligde USB-flashdrives.
- Deze sleutels hebben **automatische zelfvergrendeling** wanneer ze niet in gebruik zijn, waardoor onbevoegde toegang wordt voorkomen.
- In **de zwarte doos van de EviKey NFC-sleutels is een traceerbaarheidslogboek geïntegreerd, waarmee elke ontgrendeling en de geolocatie ervan kunnen worden geverifieerd.**

12.5.3 Fysieke isolatie en beveiliging van productiegereedschappen

- Gevoelige productieapparatuur en gereedschappen **zijn nooit verbonden met het internet** en worden na gebruik strikt geïsoleerd.
- Na gebruik worden deze gereedschappen **bewaard in een speciale kluis die** bestand is tegen brand en fysieke indringing.

12.5.4. Authenticatiesleutels genereren en beveiligen

- Anti-vervalsing authenticatiesleutels die ook als **gesegmenteerde sleutels dienen,** worden willekeurig gegenereerd door de productietools.
- Deze sleutels **worden niet weergegeven of opgeslagen** in de productietools, waardoor de afwezigheid van enig bruikbaar spoor wordt gegarandeerd.

12.5.5 Strikte toegangscontrole en beperking van interne risico's

- Slechts **twee gemachtigde personen**, die ook **aandeelhouder zijn van de onderneming**, zijn bevoegd om de productiewerktuigen te gebruiken.
- Deze beperking is bedoeld om **de risico's die gepaard gaan met ondergeschikte relaties tot een minimum te beperken** en volledige controle over de toegang tot gevoelige infrastructuur te waarborgen.

12.6. Strikte toegangscontrole en beperking van interne risico's

12.6.1 Toegangsbeveiliging en systematische versleuteling

Freemindtronic past geavanceerde authenticatie- en coderingsprotocollen toe om ervoor te zorgen dat alle digitale toegang en media worden beschermd tegen inbraak- of diefstalpogingen.

12.6.1.1 Bescherming van toegang tot sites en netwerkenAlle online en lokale netwerksystemen maken alleen gebruik van de volgende sterke authenticatietechnologieën:

- 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 en/of DataShielder HSM PGP in Cyber Defense-versie, waarbij sterke authenticatie en geavanceerde toegangsversleuteling worden gecombineerd.
- USB Bluetooth-toetsenbordemulators om de invoer van gevoelige gegevens te beveiligen door elk risico op keylogging te elimineren.

12.6.1.2 Versleuteling van gegevens en opslagmediaAlle computersystemen (vast, mobiel) en opslagapparaten die gevoelige gegevens bevatten, zijn versleuteld met versleutelingssleutels die gelijk zijn aan of groter zijn dan 256 bits.

- Volledig versleutelde interne en externe harde schijven.
- Mobiele opslag- en back-upapparaten die worden beschermd door hardware- en/of softwareversleuteling.

12.6.1.3 Weerbaarheid tegen fysieke en digitale indringersAlles is ontworpen om ervoor te zorgen dat, in het geval van een inbraak in de gebouwen van Freemindtronic, diefstal van digitale media of illegale extractie van gevoelige gegevens, geen gegevens bruikbaar of fysiek toegankelijk zijn.

- Veilige coderingssleutels in NFC HSM-apparaten, waardoor ongeoorloofde toegang wordt voorkomen.
- Automatische sleutelvergrendeling of vergrendeling in geval van poging tot compromis met traceerbaarheid van de zwarte doos.

12.6.1.4 Integratie van producten met behulp van EviKey NFC-technologie

De producten van Freemindtronic met **EviKey NFC-technologie** maken uitsluitend gebruik van de **Fullkey Plus-app** voor hun beheer en beveiliging. Deze technologie is ook geïntegreerd in de volgende cyberbeveiligingsoplossingen:

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

De integratie van EviKey NFC in deze oplossingen biedt geavanceerde toegangscontrole tot opslagmedia en omvat de volgende functies:

- **Zelfvergrendelend wanneer inactief**
- **Veilig sleutelbeheer**
- **Toegang tot traceerbaarheid via een zwarte doos**, alleen contactloos toegankelijk via **een NFC Android-telefoon**, dankzij de **Fullkey Plus**, **PassCypher NFC HSM** of **DataShielder NFC HSM-applicatie**.

Freemindtronic neemt geen enkel risico als het gaat om veiligheid en laat zich niet verrassen: hier **is de schoenmaker zeker niet de slechtst geschoeid** ! 😉

Freemindtronic implementeert **waterdichte beveiligingspartities**, waardoor elke vorm van spionage, zowel **intern als extern, wordt voorkomen en** maximale bescherming **van digitale activa en kritieke gegevens** wordt gegarandeerd.

12.6.1.4 – Bescherming tegen AI en geavanceerde aanvallen :

Freemindtronic implementeert specifieke technologieën en protocollen om zich te beschermen tegen AI-ondersteunde aanvallen, waaronder deepfakes en audio-/videomanipulaties die gericht zijn op het compromitteren van de digitale identiteit van leidinggevenden en gebruikers. Deze maatregelen

omvatten een betere verificatie van de communicatie en een multifactoranalyse van gevoelige handel.

12.7 – Beheer van datalekken :

In het geval van een inbreuk op de hardware of een poging tot inbreuk op de beveiliging van de infrastructuur van Freemindtronic, worden incidentresponsprocedures proactief uitgevoerd, ongeacht het ontbreken van een geautomatiseerd detectiesysteem.

Freemindtronic erkent dat het onrealistisch is om absolute bescherming te garanderen tegen een vastberaden aanvaller, zelfs met de beste beveiligingsmaatregelen ter wereld. Daarom is de gekozen aanpak gebaseerd op een **proactieve en preventieve strategie**, waarbij internationaal gepatenteerde innovaties worden geïntegreerd die zijn ontwikkeld om te anticiperen op nieuwe vormen van spionage, met name die met behulp van **kunstmatige intelligentie**.

De cyberbeveiligingsoplossingen van Freemindtronic zijn ontworpen om te voorkomen dat gegevens worden misbruikt, zelfs in het geval van ongeoorloofde fysieke of digitale toegang. Deze aanpak is gebaseerd op geavanceerde mechanismen, waaronder zelfvergrendeling van hardware, versleuteling met gesegmenteerde sleutels, isolatie van de infrastructuur en het exclusieve gebruik van beveiligde media zoals EviKey NFC, PassCypher NFC HSM en DataShielder NFC HSM.

In het geval dat een beveiligingsincident een klant of partner betreft, verbindt Freemindtronic zich ertoe **deze zo snel mogelijk te informeren**, in overeenstemming met de vereisten van de toepasselijke voorschriften inzake gegevensbescherming.

ARTIKEL 13 – RECHTEN VAN GEBRUIKERS OP GROND VAN DE ANDORRESE WETGEVING

In overeenstemming met de **artikelen 16 tot en met 21 van Wet 29/2021** hebben gebruikers de volgende rechten, in overeenstemming met de **AVG en de Andorrese wetgeving**:

- **Recht op toegang** : Om na te gaan welke informatie vrijwillig is verstrekt en verwerkt.
- **Recht op rectificatie** : Om onjuiste of onvolledige gegevens te corrigeren.
- **Recht van bezwaar** : Bezwaar maken tegen het gebruik van hun gegevens.
- **Recht op verwijdering (recht om vergeten te worden):** Om de permanente verwijdering van hun gegevens te eisen.
- **Recht op overdraagbaarheid** : Hun gegevens in een leesbaar formaat ontvangen (nieuwe verplichting versterkt door Wet 29/2021).
- **Recht op beperking van de verwerking** : Beperk de verwerking van bepaalde informatie.

13.1. Verwerkingstijd voor aanvragen

Freemindtronic garandeert dat elk verzoek om rechten uit te oefenen **binnen een termijn van maximaal 30 dagen** zal worden behandeld, behalve in uitzonderlijke omstandigheden die een **gerechtvaardigde verlenging van maximaal 60 dagen** vereisen.

Aanvragen kunnen per e-mail gestuurd worden naar:
contact [at] freemindtronic.com of **dpo [at] freemindtronic.com**

ARTIKEL 14 – VERHAAL IN GEVAL VAN EEN GESCHIL

Als een gebruiker van mening is dat **zijn rechten niet zijn gerespecteerd**, kan hij een klacht indienen bij het **Andorrese agentschap voor gegevensbescherming (APDA),** de **bevoegde toezichthoudende autoriteit in Andorra**.

14.1. Klachtenregeling

In overeenstemming met **artikel 25 van wet 29/2021 kan** elke persoon die van mening is dat de verwerking van zijn gegevens in strijd is **met de toepasselijke wetgeving**:

- **Verwijs de zaak door naar het Andorrese agentschap voor gegevensbescherming (APDA)** voor een administratief onderzoek.
  Contactpersoon APDA : https://www.apda.ad
- **Beroep instellen bij de bevoegde rechtbanken van Andorra** om vergoeding te krijgen voor de geleden schade.

Freemindtronic zet zich in om **volledig mee te werken** met gegevensbeschermingsautoriteiten in geval van een onderzoek.

ARTIKEL 15 – WIJZIGINGEN AAN HET PRIVACYBELEID

15.1. Verbintenis tot actualisering

Freemindtronic verbindt zich ertoe dit beleid bij te werken in geval van wijzigingen in de wet- of regelgeving die van invloed zijn op de gegevensbescherming. Eventuele wijzigingen zullen expliciet worden gepubliceerd op de officiële website van Freemindtronic.

15.2. Frequentie en transparantie van updates

Freemindtronic brengt regelmatig updates uit voor zijn software, applicaties en extensies. Er wordt een speciale updatepagina bijgehouden, met expliciet details:

- **De aangebrachte wijzigingen,**
- **Verbeteringen op het gebied van beveiliging,**
- **Eventuele kwetsbaarheden geïdentificeerd en gecorrigeerd.**

De volledige versiegeschiedenis van Freemindtronic software, applicaties en extensies is hier te vinden: Freemindtronic Version History

15.3. Kennisgeving van de Gebruikers

Gebruikers die per e-mail op de hoogte willen worden gehouden van updates, moeten een uitdrukkelijk verzoek indienen door hun e-mailadres aan Freemindtronic te verstrekken.

15.4. Informatie in geval van wijzigingen in de functionaliteiten

In geval van wijzigingen in de functionaliteiten met betrekking tot gegevensverwerking, verbindt Freemindtronic zich ertoe de gebruikers te informeren:

- **Door kennisgeving op de officiële website,**
- **Via de betreffende applicaties.**

ARTIKEL 16 – CONTACTGEGEVENS

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

Einde van het document