**PRIVACY POLICY – FREEMINDTRONIC SL**

**Website & Software** – Version and date of the document: V2.0 of 28/02/2025

## ARTICLE 1 – INTRODUCTION

### 1.1. Identification of the Data Controller

This Privacy Policy is issued by **Freemindtronic SL**, a limited liability company registered under the laws of the Principality of Andorra, with its registered office at:

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

Freemindtronic is responsible for the processing of data collected or processed through the use of its official website https://freemindtronic.com as well as its software, applications, extensions and embedded systems.

### 1.2. Champ d'Application

This Privacy Policy applies to all services, software, applications, extensions and embedded systems developed and operated by Freemindtronic.

It does not apply to third-party websites, services, or platforms accessible through Freemindtronic's services. Freemindtronic is not responsible for the privacy practices of these third-party services.

### 1.3. Engagement Zero Trust & Zero Knowledge

Freemindtronic adheres to a strict **Zero Trust & Zero Knowledge** framework, ensuring that user data is not accessed, stored, or shared at all.

All software, applications, extensions and embedded systems developed by Freemindtronic operate **without a remote server, a centralized database, the creation of a user account, user identification and data transmission**.

### 1.4. Compliance with Regulations

Freemindtronic complies with the strictest international data protection and cybersecurity regulations, including:

- General Data Protection Regulation (GDPR – Regulation (EU) 2016/679)
- Digital Operational Resilience Act (DORA – Règlement (UE) 2022/2554)
- California Consumer Privacy Act (CCPA – US)
- General Data Protection Law (LGPD – Brésil)
- Law 15/2003 on the Protection of Personal Data in Andorra
- Regulations applicable to cybersecurity and digital resilience solutions
- ISO/IEC 27001 Standards and NIST Security Best Practices

### 1.5. DefinitionsIn this policy, the following terms are defined as follows:

- **Personal data** : any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more elements specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity.
- **Sensitive data** : any information the unauthorized disclosure of which could result in a high risk to the rights and freedoms of data subjects. This includes, but is not limited to:
    - Unique identifiers (usernames, passwords, authentication codes).

    - Encryption and authentication keys.
    - Payment information and bank details.
    - Confidential data of customers and partners (commercial strategies, patents, documents protected by trade secrets).
    - Any personal data that falls into the special categories of the GDPR (ethnic origin, political opinions, religious beliefs, health, biometrics, sex life).
- **Processing** means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, limitation, erasure or destruction.
- **Data controller** : the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Processor** : the natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- **Consent** : any free, specific, informed and unequivocal indication of the data subject's wishes by which he or she agrees, by a statement or by a clear affirmative action, to the processing of personal data concerning him or her.
- **Pseudonymisation** : processing of personal data in such a way that it can no longer be attributed to a specific natural person without additional information, which must be kept separate and protected by appropriate technical and organisational measures.
- **Anonymisation** : irreversible transformation of personal data in such a way that it is no longer possible to directly or indirectly identify the data subject.
- **Personal Data Breach** : Any breach of security that accidentally or unlawfully results in the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes unauthorized access to logins, passwords, encryption keys, or other protected sensitive data.

**ARTICLE 2 – DATA COLLECTION AND PROCESSING**

**2.1. Lack of Systematic Data Collection**

Freemindtronic does not collect, store, share, or sell any personal or technical data from users, except in the case of direct interaction, including to:

- An order via official platforms.
- A contact request related to customer service or an official partnership.

The data is only processed within the strict scope of the performance of the contract or business relationship and is never used for any other purpose.

**2.2. Data that may be collected**

If a user voluntarily provides information, only the data that is strictly necessary is processed:

- Identity (surname, first name)
- Contact details (email, phone, billing and delivery address)
- Professional information

- Voluntarily submitted content

Transactional data is used exclusively for the management of orders and their delivery, without transmission to third parties except for legal obligations (tax and accounting).

**2.3. Data Storage and Security**

Freemindtronic applies the highest security standards, compliant with **GDPR, DORA, NIS2, ISO/IEC 27001 and NIST** regulations.

- **Secure offline storage** : Data is kept on encrypted media that can only be accessed via EviKey NFC secure USB flash drives and/or encrypted storage media and/or encrypted data.
- **Zero Trust & Zero Knowledge** : Lack of remote servers and centralized databases to store and/or manage sensitive data for all Freemindtronic products.
- **Enhanced security for sensitive communications**: The exchange of sensitive data is carried out exclusively via **DataShielder** tools or a secure protocol defined by the customer.
- **Imposed alternative if necessary** : If the customer's service does not guarantee a sufficient level of security, Freemindtronic offers **DataShielder** as the only secure channel.

**2.4. Protection of Classified Data and Sensitive Environments**

Freemindtronic solutions identified as a dual-use civil and military product are designed to protect critical information and include:

- **Physical isolation and partitioning** : No data is stored on a remote server.
- **Strong authentication** : NFC HSM and patented segmented key encryption. The use of RSA-4096 asymmetric encryption allows AES-256 CBC keys to be securely shared between HSM NFC devices, including remotely, without transmission over centralized infrastructures. This mechanism eliminates the risk of key exfiltration and provides advanced protection for encrypted exchanges.
- **End-to-end encryption** : AES-256 CBC, RSA-4096, PGP - All secure symmetric encryption systems are achieved via segmented keys and patented, internationally delivered access control systems. This architecture makes encryption resistant to quantum attacks, ensuring long-term protection of sensitive data.
- **Decentralized logging** : Local black box accessible only in NFC by an authorized administrator.
- **Stress testing and proactive cybersecurity** : Regular assessments against APT attacks, industrial espionage, and advanced cyber threats.

**2.5. Storage, Deletion and Retention of Customer Data**

- The data provided via a **contact form** is used only to respond to the request and deleted immediately after processing.
- **Customer data from transactions** is kept only for the necessary legal period (tax and accounting).
- **No bank data is stored** : Transactions are processed via **secure third-party providers** (e.g. PayPal).

**2.6. International Data Transfers**

Freemindtronic does not transfer any data outside the EEA unless an adequate legal framework is applied (**Standard Contractual Clauses - SCCs**).

**2.7. Data Breach Procedure**

In accordance with Articles 33 and 34 of the **GDPR** and **Qualified Law 29/2021**, Freemindtronic applies a **proactive response** in the event of an incident:

- **Immediate containment** and **impact analysis**.
- **Notification within 72 hours** to the Andorran Data Protection Agency (APDA) if necessary.
- **Informing affected users** if a high risk is identified.
- **Post-incident audit** to strengthen protection measures.

**2.8. Cyber Resilience and Protection Against Disasters and Cyberattacks**

Freemindtronic guarantees **the integrity and availability** of data even in the event of a breakdown, theft, disaster or massive cyberattack.

**2.8.1. Encryption and Secure Backup**

- **Advanced encryption** : AES-256 CBC, AES-256 CBC PGP, BitLocker with keys stored **on NFC HSM PassCypher**.
- **Separation of keys and data** : Decryption **keys** are never stored on the same media as the data. AES-256 CBC encryption keys are highly secure shareable via NFC HSM DataShielder, operating contactless, serverless, and database-free. This mechanism ensures secure key transmission, even remotely, eliminating any risk of interception by third parties.
- **Encrypted and redundant backups**: Data replicated **across multiple media offline** and secure.

**2.8.2. Enhanced Protection Against Cyberattacks**

- **Ransomware & Over-Encryption** : Encrypted offline backups and physically outsourced keys offline prevent tampering or fraudulent recovery.
- **Advanced Cyberattacks (APT, Zero-Day, Espionage):** Zero Trust & Zero Knowledge **architecture** and **physical key separation** prevent exfiltration. Freemindtronic's security architecture, incorporating patented segmented encryption systems and hardware-based access control, ensures that no private keys or encrypted data can be exfiltrated, even under physical or logical constraint. The combination of AES-256 CBC encryption and RSA-4096 increases resilience to advanced attacks, including those assisted by artificial intelligence.
- **Cloudless resiliency** : **No dependency on remote servers**, eliminating the risk of centralized attacks.

**2.8.3. Resilience to Physical Disasters and Accidental Losses**

Freemindtronic's protocols always ensure access to data encrypted with their keys, even in the event of:

- **Theft or loss** of encrypted media: Without **outsourced keys**, data remains unusable.

- **Accidental destruction or natural disaster** : Duplicate **backups** ensure that sensitive data is recovered.
- **Geographic isolation of backups** : Encrypted **media** is kept in a variety of secure locations, preventing total compromise.

**2.9. Non-Disclosure Agreements (NDAs) and Confidentiality of Trade**

All business relationships with Freemindtronic involving the exchange of sensitive or confidential information are routinely covered by a **Non-Disclosure Agreement (NDA).**

- **Strict application** : Any information exchanged in the context of partnerships, technical collaborations or business discussions is protected by **legally binding confidentiality clauses**.
- **Scope of the NDA** : The NDA covers **documents, communications, technical exchanges, innovations, internal data**, as well as any confidential information transmitted by Freemindtronic or received from a partner.
- **Penalties for violations** : Any unauthorized disclosure of confidential information is subject to **contractual and legal penalties** that may include legal actions for breach of confidentiality and trade secrets.
- **Term of Protection** : Non-disclosure obligations remain in effect **even after the end of the contractual relationship**, according to the term defined in each agreement.

This clause reinforces Freemindtronic's commitment to protect all critical information exchanged in the course of its business, ensuring a strict legal framework against any leakage or compromise.

**ARTICLE 3 – USE OF SENSORS AND ACCESS TO LOCATION DATA**

Some Freemindtronic software, applications, or extensions  may require access to the sensors on users' devices.

**3.1 These sensors include:**

- **GPS** (precise location)
- **Wi-Fi and mobile networks** (approximate location)
- **Bluetooth** (local detection without external transmission)
- **Biometric data** (fingerprint, facial recognition)
- **Microphone and camera** (only with explicit consent)
- **Environmental sensors** (accelerometer, gyroscope, proximity sensors, brightness)
- **Security Modules** (NFC, HSM, HSM, PGP)

**3.2 All data generated by these sensors:**

- **Remain exclusively on the user's device** and are not transmitted to a remote server or third-party service under any circumstances.
- **Are not subject to external or remote storage**.
- **Are only accessible with the explicit consent of the user**, especially for sensitive sensors such as microphone and camera.

- **Can be managed by the user**, who can change or revoke the permissions granted at any time through their device settings.

**3.2 Ensuring that Sensor Data is not used for behavioural tracking purposes**

Freemindtronic ensures that **the data collected via device sensors is never used for behavioral tracking, targeted advertising, or user profiling**.

Access to the sensors is strictly limited to essential software features and only after obtaining the user's explicit consent.

No analysis of usage patterns is carried out on the basis of this data, and it is not stored or passed on to third parties.

**ARTICLE 4 – COMPLIANCE WITH DISTRIBUTION PLATFORMS**

The software, applications and extensions developed by **Freemindtronic** comply with the requirements of the following platforms:

- **Google Play Console** (applications Android)
- **Chrome Web Store** (browser extensions)
- **Microsoft Store and Edge Add-ons** (Windows apps and browser extensions)
- **Apple macOS and iOS** (apps distributed on the App Store)

Freemindtronic is committed to adhering to the **security and privacy guidelines** imposed by these platforms.

- **The Zero Trust & Zero Knowledge architecture is guaranteed** so that no user data is collected, transmitted, or stored beyond the user's device.
- **There is no integration with third-party services** to mitigate the risks associated with tracking or collecting personal data.
- **The requirements of each platform are regularly reviewed** to ensure continuous compliance with changes in the applicable regulations.

**SECTION 5 – NON-DISCRIMINATION CLAUSE (CCPA COMPLIANCE)**

In accordance with the provisions of the **California Consumer Privacy Act (CCPA), Freemindtronic guarantees that users will not be discriminated against** in exercising their rights regarding the protection of personal data.

**No restrictions or limitations will be applied to users wishing to** exercise their rights, in particular with regard to:

- Access to their personal data.
- Rectification of inaccurate or incomplete information.
- Deletion of data provided voluntarily.
- Objecting to or restricting the processing of their data.

**Freemindtronic undertakes not to apply additional fees, or changes in access to features**, in response to a request to exercise rights by a user.

**Any user wishing to assert their rights may contact Freemindtronic directly** using the contact details provided in this Privacy Policy.

In accordance with the CCPA, the exercise of personal data protection rights (access, deletion, opposition) will not result in any modification, restriction or degradation of the services offered by Freemindtronic.

**ARTICLE 6 – NO PROFILING AND FINGERPRINTING**

**6.1. Absence of Profiling and Automated Decisions**

Freemindtronic does not carry out any profiling, behavioral tracking, or automated decision-making affecting users.

- No user activity analysis is performed.
- No artificial intelligence algorithm is used to classify users.
- No mechanism for personalizing services based on user data is put in place.

**6.2. Absence de Fingerprinting**

Fingerprinting  is a technique that involves collecting specific information about a device's hardware or software, such as IP address, operating system, screen resolution, and other parameters, in order to create a unique digital fingerprint of the user. Unlike cookies, this method is difficult to detect and block, which poses major privacy concerns.

In December 2024, **Google announced that starting February 16, 2025, it would allow advertisers to use fingerprinting** for user tracking, reversing its 2019 policy that prohibited the practice. The move drew criticism from regulators such as **the UK's Information Commissioner's Office (ICO),** which called the change "irresponsible" due to the reduction in choice and control individuals have over the collection of their information.

At **Freemindtronic**, we are strongly committed to respecting the privacy of our users. Thus, we **do not use any form of fingerprinting** in our products or services. **Google announced in December 2024 that it would allow fingerprinting for advertisers from February 16, 2025** (official source - https://blog.google/products/ads-commerce/privacy-sandbox-fingerprinting-policy-change).

The move raised concerns from regulators, including **the UK's ICO**. Freemindtronic rejects these practices and guarantees that **no tracking, device identification, or behavioral profiling** is implemented.

All Freemindtronic IT systems are **completely isolated and independent** of each other. **No user data is recorded, stored or traced** through an exclusively local and offline operation. **The use of hardware encryption and NFC HSM authentication solutions** ensures that no digital fingerprint can be associated with users, including through the use of Freemindtronic's EviBITB technology.

Freemindtronic implements an **advanced cybersecurity strategy** to guard against AI-assisted attacks, CEO fraud, and other identity theft.

- The **emails used for external communication** are **sandbox addresses and no-reply emails** to **reduce the risk of spoofing and phishing**.
- Any attachment opening is subject to a **strict control policy** in order to avoid **any risk of malicious files**.

- Each **customer request** is systematically verified by **a second communication channel** to **confirm its authenticity** (proactive doubt removal).

**ARTICLE 7 – COMPLIANCE WITH DUAL-USE REGULATIONS**

**7.1. Export Regulations and Authorization**

Freemindtronic strictly enforces regulations for the management and export of cybersecurity technologies, including for **encryption products classified as dual-use civil and military**.

DataShielder NFC HSM **products** have received an **import authorization into France from the Principality of Andorra**, validated on **December 7, 2024** via the company **AMG Pro**, in accordance with **Decree No. 2001-1192 of December 13, 2001**, amended by **Decree No. 2024-95 of February 8, 2024**.

This authorisation was obtained after submission of the file to the **ANSSI**, which, in accordance with its mission to **verify compliance with regulatory requirements**, did not refuse within the time limits provided for by the legislation in force.

Since **February 7, 2025**, **DataShielder NFC HSM** products are also **authorized for re-export** from France to the Member States of the European Union, in compliance with **Regulation (EU) 2021/821 of May 20, 2021** on dual-use items.

**7.2. Reference Texts**

This authorisation is issued pursuant to the following texts:

- **Decree No. 2001-1192 of 13 December 2001**, amended by **the Decree of 8 February 2024**, on the control of the export and transfer of dual-use goods and technologies.
- **Regulation (EU) 2021/821 of 20 May 2021** establishing an export control regime for dual-use items.

**7.3. Audit Commitment**

Freemindtronic is committed to ensuring **regular compliance audits** to ensure **continued adherence to legal and regulatory requirements**. These internal audits are carried out periodically in accordance with the regulatory requirements in force.

**ARTICLE 8 – CERTIFICATIONS AND AUDITS**

**8.1. No Cloud Certification Requirement**

Freemindtronic does not require **SOC 2** or **ISO 27001** certifications specific to cloud infrastructures, as **no remote servers are used** for data processing or storage.

The products are designed with a **100% air-gapped** approach, ensuring **total isolation of user data** from any external network infrastructure. This architecture justifies **the absence of certain audits** normally applied to connected systems.

**8.2. Safety Audit and Quality Control**

This approach **is applied throughout the value chain**, from **product design** to **manufacturing**. All audits conducted are aimed at ensuring the **resilience, tamper-proof, and data leak-free of** Freemindtronic's systems.

In addition to internal audits to ensure product compliance, Freemindtronic applies **enhanced controls on payment management** and **financial transaction protection**.

- The accounting and financial management system is isolated, and no transaction can be validated without strong authentication via DataShielder NFC HSM Auth and DataShielder MAuth, ensuring strong authentication and eliminating the risk of fraud.
- Access to bank accounts and payment systems is strictly limited to authorized shareholders, without a relationship of subordination, to limit the internal risks of fraud.

**ARTICLE 9 – DATA PROTECTION OFFICER (DPO)**

**9.1. Appointment of the DPO**

In accordance with the requirements of the **General Data Protection Regulation (GDPR – Regulation (EU) 2016/679)** and other applicable regulations, Freemindtronic has appointed a **Data Protection Officer (DPO)** responsible for ensuring the company's compliance with the protection of personal data.

The **DPO of Freemindtronic** is:

- **Name:** Jacques Gascuel
- **Position:** CEO and DPO of Freemindtronic SL
- **Contact :** dpo [ at ] freemindtronic.com

**9.2. Missions of the DPO**

**Freemindtronic's DPO** carries out several essential missions, including:

- Ensure that **data processing complies** with applicable regulations (**GDPR, CCPA, LGPD, etc.**).
- Inform and advise Freemindtronic on **its data protection obligations**.
- Monitor the application **of the security and data protection policies** put in place.
- Respond to users' requests regarding **their rights (access, rectification, deletion, opposition, etc.)**.
- Liaise with **data protection authorities**, including the **Andorran Data Protection Agency** and relevant European or international authorities.

**9.3. Contact and Complaints**

Any user wishing to obtain information on **the management of their personal data** or to exercise their rights may contact **Freemindtronic's DPO** at the following address:

- **Email :** dpo [ at ] freemindtronic.com
- **Mailing address:**
  Freemindtronic SLAv. Co-Prince de Gaulle, 13, Valira Building, Ground floor, AD700 Escaldes – Engordany, Andorra

If no response is provided within **30 days**, the user may refer the matter directly **to the Andorran Data Protection Agency (APDA)** for **non-compliance with the legal obligation to respond within 30 days**.

**ARTICLE 10 – COMPLIANCE WITH ANDORRAN DATA PROTECTION LEGISLATION**

**10.1. Application of Andorran Laws**

Freemindtronic, as a company registered in **the Principality of Andorra**, is subject to local **data protection regulations**, including:

- **Qualified Law 15/2003 of 18 December 2003** on the Protection of Personal Data
- **Qualified Law 29/2021 of 28 October 2021**, which aligns Andorra with the principles of **the General Data Protection Regulation (GDPR – Regulation (EU) 2016/679)**

These laws guarantee a **data protection framework** equivalent to European standards, recognized as **adequate** by the European Union in accordance with **Article 45 of the GDPR**.

In addition to the current regulations, **Freemindtronic implements advanced physical and software measures to ensure absolute data protection**. This includes **full encryption of digital media, NFC HSM multi-factor authentication, and physical isolation of IT infrastructures**. These measures ensure **full compliance with Articles 10 and 45 of the GDPR**, guaranteeing data protection equivalent to the strictest European standards.

**ARTICLE 12 – COMPLIANCE PRINCIPLES AND DATA SECURITY**

**12.1. Privacy by Design**

Freemindtronic integrates **data protection** into **the design of its software and services**, in accordance with the principles of **privacy by design and privacy by default**.

**12.2. No Data Storage**

In accordance with **the Zero Trust & Zero Knowledge approach**, **Freemindtronic does not store or process any personal data**, except in the case of voluntary provision by the user (e.g. contact form, technical support).

**12.3. Adoption of Enhanced Security Measures**

Freemindtronic implements **advanced security** measures to ensure **data protection** and prevent breaches, including:

- **Systematically encrypt** user communications and transactions through its patented segmented key encryption systems
- **Lack of unique** identifiers that can be used to track user activity
- **Regular internal auditability** to ensure compliance with current regulations

These measures are in accordance with **Article 10 of the Qualified Law 29/2021** on the Protection of Personal Data in Andorra.

Freemindtronic applies a comprehensive cybersecurity strategy that ensures data protection even in the event of a physical intrusion into the premises:

All computer systems (fixed, mobile, server, and storage devices) are fully encrypted with ≥256-bit keys.

All sites connected online or on a local network use PassCypher NFC HSM and PassCypher HSM PGP with TOTP/HOTP and/or DataShielder NFC HSM and DataShielder HSM PGP Cyber Defense.

No encryption keys are stored or visible on the production tools.

Sensitive media (USB sticks, hard drives) are stored in a fire and intrusion-resistant safe.

Any extraction of sensitive data is impossible, even in the event of physical theft of servers or illicit exfiltration of files.

These measures ensure that even in the event of an intrusion into Freemindtronic's premises, no data can be exploited even in the event of a successful unlawful intrusion.

**12.4. Commitment to Ongoing Security**

Freemindtronic places **data protection** at the heart of its activities and is committed to:

- **Continuously improve its security measures** by keeping up with evolving threats and regulations.
- **Adapt its protection protocols** to guarantee a level of security in line with new technological advances and cybersecurity best practices.
- **Constantly monitor** cyber threats, including those assisted by artificial intelligence (AI), to anticipate potential intrusion attempts and strengthen defenses accordingly.

**12.4.1 Strategic Protection**: Freemindtronic does not publicly disclose all technical details of its security mechanisms so as not to facilitate an analysis by an attacker or artificial intelligence seeking to identify a possible vulnerability. However, all measures put in place comply with the **strictest** standards in terms of cybersecurity and data protection.

**12.5. Operational Security and Protection of Sensitive Data**

Freemindtronic applies a strict security model that guarantees **maximum protection against the risks of internal and external espionage**.

**12.5.1 Isolation of Computer Systems**

- No network connections between internal systems and no file or printer sharing is allowed.
- Each system is completely independent, avoiding vulnerabilities related to external connections.

**12.5.2 Secure Transfers of Sensitive Data**

- All sensitive file transfers are performed **exclusively** via Freemindtronic's **EviKey NFC** secure USB flash drives.
- These keys have **automatic self-locking** when not in use, preventing unauthorized access.
- A **traceability log** is integrated into the black box of the EviKey NFC keys, allowing each unlock and its geolocation to be verified.

**12.5.3 Physical Isolation and Securing Production Tools**

- Sensitive production equipment and tools **are never connected to the Internet** and are strictly isolated after use.
- After use, these tools are **kept in a special safe that** is resistant to fire and physical intrusion.

**12.5.4 Generating and Securing Authentication Keys**

- Anti-counterfeiting authentication keys that also serve as **segmented keys** are randomly generated by the production tools.
- These keys **are neither displayed nor saved** in the production tools, guaranteeing the absence of any usable trace.

**12.5.5 Strict Access Control and Mitigation of Internal Risks**

- Only **two authorised persons**, who are also **shareholders of the company**, are authorised to use the production tools.
- This restriction aims to **minimise the risks associated with subordinate relationships** and to ensure full control over access to sensitive infrastructure.

**12.6. Strict Access Control and Mitigation of Internal Risks**

**12.6.1 Access Security and Systematic Encryption**

Freemindtronic applies advanced authentication and encryption protocols to ensure that all digital access and media are protected against any intrusion or theft attempts.

**12.6.1.1** Protection of Access to Sites and NetworksAll online and local network systems use only the following strong authentication technologies:

- 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 and/or DataShielder HSM PGP in Cyber Defense version, combining strong authentication and advanced access encryption.
- USB Bluetooth keyboard emulators to secure sensitive data input by eliminating any risk of keylogging.

**12.6.1.2** Encryption of Data and Storage MediaAll computer systems (fixed, mobile) and storage devices containing sensitive data are encrypted with encryption keys equal to or greater than 256 bits.

- Fully encrypted internal and external hard drives.
- Mobile storage and backup devices protected by hardware and/or software encryption.

**12.6.1.3** Resilience to Physical and Digital IntrusionsEverything is designed to ensure that, in the event of an intrusion into Freemindtronic's premises, theft of digital media or illicit extraction of sensitive data, no data is usable or physically accessible.

- Secure encryption keys in NFC HSM devices, preventing unauthorized access.
- Automatic key locking or locking in case of attempted compromise with black box traceability.

**12.6.1.4 Integration of Products using EviKey NFC Technology**

Freemindtronic's products incorporating **EviKey NFC** technology exclusively use the **Fullkey Plus** app for their management and security. This technology is also integrated into the following cybersecurity solutions:

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

The integration of EviKey NFC into these solutions provides advanced access control to storage media and includes the following features:

- **Self-locking when inactive**
- **Secure key management**
- **Access traceability via a black box**, accessible only contactless via **an NFC Android** phone, thanks to the **Fullkey Plus**, **PassCypher NFC HSM** or **DataShielder NFC HSM application**.

Freemindtronic does not take any risks when it comes to safety and does not let itself be surprised: here, **the shoemaker is certainly not the worst shod** ! 😉

Freemindtronic implements **watertight security partitions**, preventing any form of espionage, whether **internal or external**, and ensuring **maximum** protection of digital assets and critical data.

**12.6.1.4 – Protection against AI and advanced attacks** :

Freemindtronic implements specific technologies and protocols to guard against AI-assisted attacks, including deepfakes and audio/video manipulations aimed at compromising the digital identity of executives and users. These measures include enhanced verification of communications and multi-factor analysis of sensitive trade.

**Article 12.7 – Data Breach Management** :

In the event of a hardware compromise or attempted security breach affecting Freemindtronic's infrastructure, incident response procedures are carried out proactively, regardless of the absence of an automated detection system.

Freemindtronic recognizes that it is unrealistic to guarantee absolute protection against a determined attacker, even with the best security measures in the world. This is why the approach adopted is based on a **proactive and preventive** strategy, integrating internationally patented innovations developed to anticipate new forms of espionage, particularly those assisted by **artificial intelligence**.

Freemindtronic's cybersecurity solutions are designed to prevent data from being exploited, even in the event of unauthorized physical or digital access. This approach is based on advanced mechanisms including hardware self-locking, segmented key encryption, infrastructure isolation, and the exclusive use of secure media such as EviKey NFC, PassCypher NFC HSM, and DataShielder NFC HSM.

In the event that a security incident concerns a customer or partner, Freemindtronic undertakes to **inform them as soon as possible**, in accordance with the requirements of the applicable data protection regulations.

**ARTICLE 13 – RIGHTS OF USERS UNDER ANDORRAN LEGISLATION**

In accordance with **Articles 16 to 21 of Law 29/2021**, users have the following rights, aligned with the **GDPR and Andorran legislation** :

- **Right of Access** : To verify what information has been provided voluntarily and processed.
- **Right to Rectification** : To correct any inaccurate or incomplete data.
- **Right to object** : Contest the use of their data.
- **Right to Deletion (Right to be Forgotten):** To demand the permanent deletion of their data.
- **Right to Portability** : Receive their data in a readable format (new obligation reinforced by Law 29/2021).
- **Right to Restriction of Processing** : Restrict the processing of certain information.

**13.1. Processing Time for Requests**

Freemindtronic guarantees that any request to exercise rights will be **processed within a maximum period of 30 days**, except in exceptional circumstances requiring a **justified extension of up to 60 days**.

Requests can be sent by e-mail to:
**contact [ at ] freemindtronic.com** or **dpo [ at ] freemindtronic.com**

**ARTICLE 14 – RECOURSE IN THE EVENT OF A DISPUTE**

If a user believes that **their rights have not been respected**, they may file a complaint with the **Andorran Data Protection Agency (APDA),** the **competent supervisory authority in Andorra**.

**14.1. Complaints Procedure**

In accordance with **Article 25 of Law 29/2021**, any person who considers that the processing of their data has been carried out in **violation of the applicable laws** may:

- **Refer the matter to the Andorran Data Protection Agency (APDA)** for an administrative investigation.
  **APDA Contact** : https://www.apda.ad
- **To lodge an appeal with the competent courts in Andorra** in order to obtain compensation for the damage suffered.

Freemindtronic is committed to **cooperating fully** with data protection authorities in the event of an investigation.

**ARTICLE 15 – CHANGES TO THE PRIVACY POLICY**

Freemindtronic undertakes to update this policy in the event of legislative or regulatory changes affecting data protection.

Any changes will be published explicitly on the official Freemindtronic website.

Users who wish to be notified of updates by email must make an express request by providing their email address to Freemindtronic.

In the event of changes to functionalities involving data processing, Freemindtronic undertakes to inform users by notification on the site or in the applications concerned.

**ARTICLE 16 – CONTACT DETAILS**

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

**End of document**