OUR PROMISE OF INTEGRITY

emaldo

Data Security & GDPR Compliance

At Emaldo, we take data security and GDPR compliance very seriously. We understand that the protection of personal data is essential for maintaining the trust of both our partners and employees alike. That's why we have implemented a comprehensive set of policies and procedures to ensure the confidentiality, integrity, and availability of all the data we handle.

- Our data security measures include, but are not limited to:
- Encryption of sensitive data at rest and in transit
- Regular vulnerability scans and penetration testing
- Access controls and authentication mechanisms
- Monitoring and logging of all critical system activity
- Incident response and disaster recovery plans

In addition, we are fully GDPR compliant and adhere to all the principles and obligations set forth by the regulation. This means that we:

- Ask permission before data is collected
- Obtain and process personal data lawfully, fairly, and transparently
- Limit the collection and processing of personal data to what is necessary for the stated purposes
- Ensure the accuracy and completeness of personal data
- Keep personal data confidential and secure
- Provide data subjects with the right to access, rectify, and erase their personal data
- Notify the supervisory authority and data subjects in case of data breaches

We regularly review and update our data security and GDPR compliance practices to ensure they remain effective and up-to-date with the latest standards and regulations. Our commitment to data protection is an ongoing process, and we strive to maintain the highest level of security and compliance in all our operations.

Product Security: Hardware, Software and Server Communication

The Emaldo Power Cores is designed and built with security in mind from the ground up. We use the latest technologies and standards to ensure that both our hardware and software products are secure and reliable, including:

- Advanced 256 bit on-device encryption (same encryption standard as used in online banking)
- Robust access controls and permissions to prevent misuse or abuse of our products and systems
- Regular digital security audits and vulnerability assessments to identify and mitigate potential risks

In addition, our servers are all based within the EU and are highly secure. We use a variety of measures to protect the privacy and integrity of all data transmitted between our products and our servers, including:

- End-to-end encryption to ensure that data is protected in transit
- Secure communication protocols and standards to prevent eavesdropping or interception
- Multi-factor authentication and authorization mechanisms to control access to our servers
- Regular monitoring and logging of all server activity to detect and respond to any suspicious behaviour

We understand that security is not a one-time event but a continuous process, and we are committed to staying up-to-date with the latest security trends and best practices. Our dedicated data team is constantly monitoring the security landscape and updating our products and protocols to ensure that we are always taking action on potential threats.
If you have any questions or concerns about our data security or GDPR compliance practices, please don't hesitate to contact us. We'll be happy to provide you with more information and address any issues you may have.