7. How We Protect Your Data

We take the security of your personal data seriously and implement measures to protect it against unauthorized access, alteration, disclosure, or destruction.

7.1 Technical Safeguards

- Data Encryption: Personal data is encrypted during transmission using industry-standard encryption protocols (e.g., HTTPS, SSL/TLS).
- Secure Storage: Data is stored on secure servers with restricted access and strong security protocols.
- Firewalls: Systems are protected by advanced firewalls to prevent unauthorized access.

7.2 Administrative Safeguards

- Access Controls: Access to personal data is limited to authorized personnel who require it for specific purposes.
- Training: Employees undergo regular training on data protection and security best practices.
- Monitoring: Systems are monitored for potential breaches, unauthorized access, or unusual activity.

7.3 Third-Party Security

- We ensure that all third-party service providers handling your data adhere to strict security and privacy standards through contracts and regular audits.

7.4 Incident Response

- In the event of a data breach, we will notify affected users and relevant authorities promptly, as required by applicable laws.

7.5 Limitations

- While we take significant steps to secure your data, no system is completely foolproof. You acknowledge and accept that risks associated with data transmission and storage cannot be entirely eliminated.

7.6 User Responsibilities

- Protect your account credentials by using strong passwords and avoiding reuse across multiple platforms.
- Notify us immediately if you suspect unauthorized access to your account.

Revision #1
Created 23 November 2024 13:58:28 by joaomorais
Updated 23 November 2024 13:59:38 by joaomorais