MedByte Data Privacy Policy

At MedByte, we are deeply committed to protecting the privacy and security of the personal data entrusted to us by our users. Our data privacy policy outlines our approach to data protection, compliance with regulatory requirements, and commitment to transparency and accountability in all aspects of our data processing activities. This policy applies to all users of our services, including individuals accessing our support chatbot and third-party mental health providers partnering with us.

1. Data Collection and Use:

MedByte collects and processes personal data from users solely for the purpose of providing our support chatbot service and facilitating access to mental health resources. We collect only the minimum amount of personal data necessary to deliver our services effectively, and we ensure that all data processing activities are conducted in accordance with applicable data protection laws, including the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the California Consumer Privacy Act (CCPA), and other relevant regulations.

2. User Consent and Control:

We obtain explicit consent from users before collecting, processing, or sharing their personal data, providing them with clear information about the purposes of data processing, the types of data collected, and their rights regarding the handling of their information. Users have the right to access, rectify, or delete their personal data at any time, and we provide easy-to-use mechanisms for exercising these rights. Additionally, users have the option to opt out of certain data processing activities, such as targeted advertising or data sharing with third-party providers.

3. Data Security and Confidentiality:

MedByte implements rigorous technical and organizational measures to ensure the security and confidentiality of user data. We employ encryption, access controls, and other industry-standard security protocols to protect against unauthorized access, disclosure, alteration, or destruction of personal data. Our data security practices are regularly reviewed and updated to address emerging threats and vulnerabilities, and we conduct periodic audits and assessments to ensure compliance with established security standards.

4. Third-Party Data Sharing and International Transfers:

We may engage third-party service providers or partners to assist us in delivering our services, and in some cases, personal data may be shared with these parties for specific purposes, such as hosting, data analytics, or mental health support. When transferring personal data to third parties, we ensure that appropriate contractual safeguards are in place to protect the privacy and security of user information. Additionally, we adhere to legal requirements regarding cross-border data transfers, including the use of standard contractual clauses or other approved mechanisms to ensure an adequate level of protection for transferred data.

5. Data Retention and Deletion:

MedByte retains personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by law. We have established clear retention periods for different categories of data, taking into account the nature of the data, legal obligations, and user preferences. Once data retention periods expire or if data is no longer necessary for the intended purposes, we securely delete or anonymize the information to prevent unauthorized access or use.

6. User Rights and Data Subject Requests:

We respect the rights of data subjects as outlined in applicable data protection laws, including the right to access, rectify, erase, restrict processing, and object to the processing of personal data. Users can exercise these rights by contacting our data protection officer or submitting requests through our designated channels. We are committed to responding to data subject requests promptly and in accordance with legal requirements, ensuring transparency and accountability in our data processing activities.

7. Compliance and Accountability:

MedByte is committed to maintaining compliance with all applicable data protection laws and regulations, including the GDPR, HIPAA, CCPA, and other relevant frameworks. We regularly review our data privacy practices and policies to ensure alignment with evolving legal requirements and industry standards. Our data protection officer oversees compliance efforts, conducts privacy impact assessments, and provides guidance on data privacy matters to internal stakeholders and external partners.

8. Data Privacy Training and Awareness:

We provide comprehensive training and awareness programs to employees and contractors involved in data processing activities, ensuring that they understand their responsibilities and obligations under our data privacy policy. Training initiatives cover topics such as data protection principles, secure data handling practices, incident response procedures, and regulatory compliance requirements. By fostering a culture of privacy awareness and accountability, we strive to uphold the highest standards of data privacy and security across our organization.

9. Transparency and Communication:

MedByte is committed to maintaining transparency and open communication with our users regarding our data privacy practices and policies. We regularly update our privacy policy to reflect changes in our data processing activities or regulatory requirements, and we provide clear and easily accessible information about how we collect, use, and protect personal data. Users can contact us with any questions, concerns, or requests related to data privacy, and we are dedicated to providing timely and informative responses to ensure transparency and trust.

10. Continuous Improvement and Review:

We recognize that data privacy is an ongoing commitment that requires continuous monitoring, review, and improvement. We conduct regular audits, assessments, and reviews of our data privacy practices, policies, and procedures to identify areas for enhancement and address any deficiencies or gaps. We actively seek feedback from users, regulators, and other stakeholders to inform our privacy initiatives and ensure that our data privacy program remains effective, responsive, and compliant with legal and regulatory requirements.

11. Data Privacy Concerns and Notification Emails:

In the event of any data privacy concerns, breaches, or inquiries, users and stakeholders are encouraged to reach out to our dedicated data privacy team. We have established specific email addresses to streamline communication and ensure prompt resolution of data privacy issues:

English: dataprivacy@medbyte.ai
Spanish: datos@medbyte.co

These email addresses are monitored by our data privacy officers who are responsible for addressing inquiries, managing data subject requests, and coordinating responses to data privacy incidents. Users can use these channels to report any potential violations of our data privacy policy, seek clarification on data handling practices, or exercise their rights under applicable data protection laws. We are committed to maintaining confidentiality and professionalism in our communications while prioritizing the protection of user privacy and data security.