WhatsApp

Personal data collected:

Account data: Phone number, username, profile picture, and status information.

Interaction data: Record of messages sent and received (not the content), information about calls, and connections with other users.

Metadata: Time and date of interactions, frequency of app usage, approximate location based on IP address.

Device data: Model, operating system, IP address, and performance data.

Optionally shared information: Real-time location, synced contacts, and shared media.

Data processing:

Data is processed to provide essential services like message delivery, contact synchronization, and interaction suggestions.

End-to-end encryption ensures WhatsApp cannot access the content of messages.

Communication and storage:

Communication: WhatsApp may share limited data with Meta companies (WhatsApp's parent company), such as phone numbers, basic interactions, and device information for personalized advertising.

Storage: Undelivered messages are temporarily stored, and backups are saved on external services like Google Drive or iCloud, which may not be end-to-end encrypted.

Analysis of personal data use:

Transparency: WhatsApp explicitly states in its terms and policies what data it collects and why, helping users understand how their data is used.

Protection: The implementation of end-to-end encryption for messages and calls is a strong point in terms of privacy.

Concerns:

Sharing with Meta: Although limited, the integration of data with other Meta platforms may be concerning for users prioritizing privacy.

Third-party dependency: Non-encrypted backups on external services represent a potential vulnerability.

Conclusion:

WhatsApp adheres to strong privacy standards in some aspects, but its connection to the Meta ecosystem raises concerns about the long-term use of personal data. This emphasizes the importance of reading the terms and considering alternatives if privacy is a priority.