

MOBEEP – GLOBAL DATA PRIVACY & SECURITY

COMPLIANCE CHECKLIST

PURPOSE:

This checklist demonstrates how Mobeep meets its obligations as a **data sub-processor** or **service provider**, ensuring alignment with major global data protection frameworks, including the **EU/UK GDPR, CCPA/CPRA, UAE Data Law, Singapore PDPA, PIPEDA (Canada)**, and similar standards.

ORGANIZATIONAL & TECHNICAL SAFEGUARDS

Control Area	Mobeep Practice
Confidentiality of Personnel	All staff with data access are under binding confidentiality and NDAs.
Access Control	Role-based access; limited to authorized personnel on a need-to-know basis.
Encryption	TLS/HTTPS encryption of all data in transit; infrastructure-level safeguards.
Pseudonymisation	Used where feasible to enhance security during processing.
Data Minimisation	Only necessary data (e.g., phone number/email) processed in real time.
Real-Time Processing	No data is stored; data is deleted automatically after delivery.
System Monitoring	Continuous monitoring for unauthorized access or vulnerabilities.
Security Assessments	Periodic penetration tests and internal security audits are conducted.

CONTRACTUAL & LEGAL COMPLIANCE

Requirement	Mobeep Practice
Data Processing Agreements (DPAs)	Executed with all clients and subprocessors.
Clear Role as Sub-Processor	Mobeep does not determine purpose or means of processing.
Use of Subprocessors	Limited, vetted subprocessors; clients notified and contracts enforced.
Lawful Processing Support	Clients define legal basis; Mobeep operates strictly on instructions.
No Sale of Data	Mobeep does not sell, trade, or monetize personal data.
Data Subject Rights	Mobeep assists clients in fulfilling access, deletion, and objection requests.

TRANSPARENCY & ACCOUNTABILITY

Requirement	Mobeep Practice
Privacy Policy	Publicly available and globally aligned with privacy frameworks.
Contact for Privacy Inquiries	Dedicated privacy and DPO email contacts provided.
Audit Rights	Mobeep cooperates with client audits and regulatory inquiries.
Data Breach Notification	Clients notified within 48 hours of a confirmed breach.
Jurisdictional Awareness	Practices aligned with EU, UK, U.S., UAE, Singapore, and Canadian regulations.

CROSS-BORDER DATA TRANSFERS

Requirement	Mobeep Practice
Transfer Mechanisms	Data routed securely via authorized infrastructure providers.

Third-Country Safeguards	Subprocessors subject to contractually binding data protection terms.
Transparency	Subprocessor list and data flow information available upon request.

Privacy Contact: legal@mobeep.io