EU-DATENGESETZ (DATA ACT) Nutzerinformationen

ALLGEMEINE TRANSPARENZERKLÄRUNG FÜR VERNETZTE PRODUKTE — IMOO KIDS SMARTWATCHES

Dieses Dokument stellt die Produkt- und Datenübersicht gemäß den regulatorischen Transparenzanforderungen nach Artikel 3 des EU-Datengesetzes (Verordnung (EU) 2023/2854) dar. Es deckt das allgemeine Sortiment der imoo Kinder-Smartwatches im europäischen Markt ab. Das EU-Datengesetz gewährt Verbrauchern und Erziehungsberechtigten das Recht auf transparenten Zugriff und Portabilität bezüglich aller von intelligenten Geräten generierten Datenströme.

> **Wichtiger Kinderschutz- und Datenschutzhinweis:** Als vernetzte Wearables für Kinder unterliegen alle imoo Watch-Modelle höchsten Sicherheitsstandards. Dieses Dokument dient der Erfüllung der gesetzlichen Informationspflichten bezüglich der Datenarchitektur. Informationen zur Einhaltung der DSGVO, zu Verschlüsselungsverfahren und Einwilligungen finden Sie in der *imoo App Datenschutzrichtlinie*.

1. Identifikation der Produktkategorie & zugehörigen Dienste

Produktkategorie:	imoo Kinder-Smartwatches / Smart Wearables (LTE/4G)
Abgedeckte Modelle:	imoo Watch Phone Serie (einschließlich Z1, Z6, Z1 Plus sowie zukünftige EU-Modelle)
Verbundener Dienst:	imoo App (Verwaltungs- und Kopplungs-App für Eltern)
Funktionsbeschreibung:	Zentralisierte, elterlich kontrollierte Kommunikations- und Sicherheitsplattform (Standortabfragen, Audio-/Videotelefonie, sichere Kontaktlisten, Sicherheitszonen und schulspezifischer Klassenmodus).

2. Übersicht der generierten Datenströme und Speicherparameter

Die nachfolgende Tabelle beschreibt die typischen Roh- und Leistungsdaten, die während des Betriebs einer imoo Kinder-Smartwatch erzeugt und mit der Cloud synchronisiert werden:

Datenkategorie	Technisches Format	Häufigkeit	Speicherort	Aufbewahrungsfrist	Zugriffsmeth
Stammdaten & Kontodaten	Text / Numerisch (z.B. Telefonnummern, Geburtsmonat, Nickname)	Bei Ersteinrichtung oder Profiländerung	Sichere Cloud-Server (EU-Rechenzentrum)	Bis zur dauerhaften Löschung des Kontos	Direkt einseh über die Profileinstellu der imoo App

Datenkategorie	Technisches Format	Häufigkeit	Speicherort	Aufbewahrungsfrist	Zugriffsmeth
Standort- & Geodaten	GPS-Koordinaten, WLAN-Umgebungsdaten, LBS-Zellendaten	Kontinuierlich oder bei Abfrage (Intervallgesteuert)	Sichere Cloud-Server (EU-Rechenzentrum)	Rollierend für max. 14 Tage (Standorthistorie)	Echtzeit-Ortungskarte Verlaufspanel der App
Kommunikationsdaten (Chats)	Verschlüsselte Textzeichenfolgen, Voice-Memos (Audioformate)	Ereignisbasiert bei Nachrichtenversand	Sichere Cloud-Server (EU-Rechenzentrum)	Temporär zur Zustellung / lokal im Geräte-Cache	Chatverlauf innerhalb der imoo App und der Watch
Aktivitäts- & Sensordaten	Numerische Werte (Schritte, Kalorien, Bewegungsdauer via G-Sensor)	Tägliche Erfassung und Synchronisierung	Lokaler Gerätespeicher & Cloud-Backup	Bis zu 12 Monate für statistische Auswertungen	Fitness- und Schrittzähler-Dashboard in App
Echtzeit-Medienströme	Verschlüsselte Video- und Audiodatenströme (VoIP/VoLTE)	Nur während aktiver Telefonate oder Videocalls	Keine (Reiner Transitstrom über Gateways)	Sofortige Löschung nach Beendigung des Telefonats	Kein persisten Zugriff möglich (flüchtige Date
Sicherheits- & Whitelist-Konfiguration	Strukturierte Telefonbucheinträge, Administrator-Rechte	Bei Änderung durch den Haupt-Administrator	Gerätespeicher & Cloud-Spiegelung	Bis zur manuellen Entfernung durch Administratoren	Kontaktverwal in den App-Einstellungen

3. Datenverarbeitung und Sicherheitsarchitektur

Die Verarbeitung aller generierten Daten dient ausschließlich der Erbringung der Kernfunktionen der Uhr, insbesondere dem Schutz des Kindes und der Vermeidung unbefugter Kontaktaufnahmen durch Dritte.

Verantwortliche Stelle: imoo Network Technology Co., Ltd. (und autorisierte regionale Servicegesellschaften)

Verarbeitungszweck: Sicherstellung von Notruffunktionen, Standortermittlung im Sicherheitsfall, Abweisung unbekannter Anrufer (Spam-Schutz) und Verteilung kritischer Firmware-Sicherheitsupdates.

Verschlüsselungs-standard: Ende-zu-Ende- oder Transportverschlüsselung (TLS/SSL) für alle sensiblen Kommunikationswege zwischen Smartwatch, Cloud und Smartphone.

4. Gesetzliche Rechte von Verbrauchern nach dem Data Act

Als Nutzer oder gesetzlicher Vertreter haben Sie nach dem EU-Datengesetz umfassende Rechte bezüglich der erhobenen Gerätedaten:

- **Recht auf Datenauskunft:** Sie können jederzeit verlangen, dass Ihnen die vom Gerät generierten und in der Cloud gespeicherten Rohdaten in einem strukturierten, gängigen Format bereitgestellt werden.
- **Recht auf Datenübertragbarkeit (Portabilität):** Sie haben das gesetzliche Recht, imoo anzuweisen, diese generierten Rohdaten direkt an einen anderen Dienstleister oder unabhängige Reparatur- und Analysedienste zu übertragen.
- **Schutz von Geschäftsgeheimnissen:** Die Bereitstellung von Daten darf nicht dazu genutzt werden, proprietäre Quellcodes, Algorithmen oder geschützte Hardware-Designs von imoo offenzulegen. Bei berechtigtem Risiko können Sicherheitsvereinbarungen verlangt werden.
- **Regulatorisches Beschwerderecht:** Sollten Sie Einschränkungen bei der Durchsetzung Ihrer Rechte nach dem Data Act feststellen, können Sie Beschwerde bei der zuständigen nationalen Aufsichtsbehörde Ihres EU-Mitgliedstaates einreichen.

Zur Geltendmachung Ihrer Rechte oder zur Einreichung einer Datenübertragungsanfrage nutzen Sie bitte das offizielle **imoo Datenschutz-Portal** / **Antragsformular für Betroffenenrechte** auf der Herstellerwebsite.