

 IKT-Ost AÖR	Öffentliche Ausschreibung	V050/2026
	Leistungsverzeichnis	19. Juni 2026

Browserbasierte WhatsApp-Business-Kommunikationsplattform (WhatsApp Business API)

 IKT-Ost AÖR	Öffentliche Ausschreibung	V050/2026
	Leistungsverzeichnis	19. Juni 2026

Inhaltsverzeichnis

1. Gegenstand der Ausschreibung.....	3
2. Funktionale Anforderungen	3
3. Compliance & Rechtliches (DSGVO)	4
4. Implementierung & Support	5
5. Vertragsrahmen	5


	Öffentliche Ausschreibung	V050/2026
	Leistungsverzeichnis	19. Juni 2026

1. Gegenstand der Ausschreibung

Gegenstand ist die Bereitstellung einer browserbasierten Software-as-a-Service (SaaS)-Lösung zur rechtskonformen Nutzung (DSGVO) von WhatsApp Business über die offizielle WhatsApp Business API (Cloudbasiert).

2. Funktionale Anforderungen

- **Plattform:** Die Anwendung muss vollständig browserbasiert (web-interface) ohne lokale Softwareinstallation nutzbar sein. Die Nutzung muss mit aktuellen Versionen marktüblicher Browser (MS Edge, Firefox, Chrome) möglich sein.
- **Einbindung in das Content-Management-System „miniKISS“:**
Bei miniKISS handelt es sich um ein webbasiertes Content-Management-System für Microsites.
Ausgangssituation:
Die Microsite besitzt keine direkte, native WhatsApp-API-Schnittstelle.
Anforderung:
Einbindung von Chat-Einstiegspunkten in die Microsite durch den Einbau eines WhatsApp-Buttons nur mittels JavaScript-Code, der die Anwender direkt in den Chat führt.
- **KI-Integration:** Optionale Unterstützung durch Künstliche Intelligenz (z. B. Textvorschläge, Chatbots). Die KI-Funktionen müssen standardmäßig deaktivierbar sein.
- **Datenschutz-Konfiguration:**
 - Vollständige Unterbindung der automatischen **Kontaktsynchronisation** mit mobilen Endgeräten.
 - Deaktivierung von automatischen **Cloud-Backups** durch Drittanbieter (z. B. Meta/iCloud/Google Drive).
 - Datenerhebung in Form von Mitarbeiterauswertungen für statistische Zwecke soll vermieden werden. Die Lösung darf keine personenbezogenen Leistungs- oder Verhaltensprofile der Mitarbeitenden standardmäßig erzeugen.
 - Einsatz einer Funktion zur Sperrung von betrügerischen Nutzeraccounts.
 - Einsatz einer konfigurierbaren Funktion zur automatischen Löschung von Nachrichteninhalten und Kontaktdaten. Die Löschfristen müssen durch Administratoren festgelegt werden können. Die Löschung muss revisionssicher in einer Logdatei dokumentiert sein.
- **Lead-Management:** Unterstützung bei der rechtssicheren Einholung von Einwilligungen, insbesondere durch integrierte **Double-Opt-in-Verfahren**.
- **Multi-User-Zugänge mit Rollen- und Rechteverwaltung:** Die Plattform muss von mindestens 30 Anwendern nutzbar sein. Es muss eine rollenbasierte Rechteverwaltung durch mindestens

 IKT-Ost AÖR	Öffentliche Ausschreibung	V050/2026
	Leistungsverzeichnis	19. Juni 2026

zwei technische Administratoren möglich sein. Die Benutzerverwaltung muss mandantenfähig bzw. rollenbasiert administrierbar sein.

Nachrichtенbearbeitung:

Die Plattform muss folgende Funktionen bereitstellen:

- Einen gemeinsamen Team-Posteingang zur Bearbeitung eingehender Nachrichten
- Die Zuweisung von Nachrichten und Aufgaben an einzelne Nutzer oder Teams
- Die Erstellung und Verwaltung von Nachrichtenvorlagen
- Rollenbasierte Bearbeitungs- und Freigaberechte
- Analyse- und Reportingfunktionen zur Auswertung der Kommunikationsvorgänge


Zusätzliche Funktionen wie:

- Regelbasierte Automatisierungen
- Chatbots
- KI-gestützte Antwortvorschläge oder Assistenfunktionen

müssen verfügbar und administrativ deaktivierbar sein.

3. Compliance & Rechtliches (DSGVO)

- **Serverstandort:** Das Hosting und die Datenspeicherung müssen innerhalb der EU/des EWR erfolgen. Der Anbieter hat geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten nachzuweisen.
- **Vertragswesen: Der Anbieter muss einen rechtsgültigen Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO bereitstellen.** Für die Übermittlung personenbezogener Daten an Unterauftragsverarbeiter in Drittstaaten außerhalb der EU/des EWR muss eine gültige Rechtsgrundlage gemäß Art. 44 ff. DSGVO nachgewiesen werden (z. B. ein Angemessenheitsbeschluss oder eine aktive Zertifizierung nach dem EU-U.S. Data Privacy Framework). Dies gilt für die gesamte Kette der Unterauftragsverarbeiter. Sofern ein Unterauftragsverarbeiter in einem Drittland ohne Angemessenheitsbeschluss oder DPF-Status ansässig ist, hat der Anbieter den Abschluss der Standardvertragsklauseln nachzuweisen und die notwendigen Informationen für ein Transfer Impact Assessment (TIA) beizubringen. Die entsprechenden Nachweise sind auf Anforderung des Auftraggebers vorzulegen.
- **Rechtssicherheit:** Die Lösung muss eine vollständig DSGVO-konforme Kommunikation zwischen Unternehmen und Endkunden ohne Zugriff auf private Metadaten Dritter ermöglichen. Die datenschutzrechtliche Verantwortlichkeit des Auftraggebers bleibt unberührt. Der Auftragnehmer unterstützt den Auftraggeber bei der datenschutzkonformen Nutzung der Kommunikationsplattform im Rahmen seiner technischen und organisatorischen Möglichkeiten.


 IKT-Ost AÖR	Öffentliche Ausschreibung	V050/2026
	Leistungsverzeichnis	19. Juni 2026

4. Implementierung & Support

- **Schulung:** Durchführung einer digitalen Anwenderschulung für die künftigen 30 Nutzer zur Bedienung der Kommunikationsplattform und zu rechtlichen Besonderheiten sowie einer digitalen Schulung für die zwei technischen Administration und Systembetreuung. Schulungsunterlagen sind in elektronischer Form bereitzustellen.
 - **Anwenderschulung:**
 - Bedienung des Dashboards und der Chat-Funktionen.
 - Handhabung von Vorlagen (Templates) und dem Double-Opt-in-Prozess.
 - Best Practices für die rechtskonforme Kundenkommunikation.
 - **Technische Administration & Systembetreuung:**
 - Konfiguration der Plattform (Nutzerverwaltung, Rollen- und Rechtekonzept).
 - Steuerung der Datenschutzeinstellungen (Deaktivierung von KI, Backups, Sync).
 - Überwachung der Schnittstellen und Fehlerdiagnose bei der Nachrichtenübermittlung.
 - Verwaltung der WhatsApp-Business-API-Anbindung (Meta Business Manager).
- **Onboarding:** Unterstützung bei der technischen Einrichtung und der Verknüpfung mit der Meta Business API.
- **Support:** Deutschsprachiger Kundendienst zu den Servicezeiten gemäß den vereinbarten Service-Level-Agreements im EVB-IT-Vertrag.

5. Vertragsrahmen

- **Mindestlaufzeit:** Der Vertrag wird für eine feste Laufzeit von **12 Monaten** geschlossen.
- **Verlängerung:** Der Vertrag verlängert sich automatisch um jeweils weitere **12 Monate**, sofern er nicht von einer der Parteien gekündigt wird.
- **Kündigungsfrist:** Die Kündigungsfrist beträgt **3 Monate** zum Ende der jeweiligen Vertragslaufzeit.
- **Preisstabilität:** Die angebotenen monatlichen Gebühren sind für die erste Laufzeit von 12 Monaten verbindlich. Weitere Konditionen werden im EVB-IT-Vertrag geregelt. Preisänderungen nach Ablauf der Erstlaufzeit sind transparent darzustellen.
- **Preisangaben:** Sämtliche laufenden Kosten der angebotenen Lösung einschließlich etwaiger Gebühren der WhatsApp Business Plattform (z. B. Meta-Conversation-Fees, Template-Gebühren oder Gebühren eines eingesetzten Business Solution Providers) sind vollständig und transparent im Angebot auszuweisen. Nicht gesondert ausgewiesene Kosten gelten als mit den angebotenen Preisen abgegolten.
- **Umsetzungszeitraum:** Die Implementierung hat **spätestens bis zum 20. Juli 2026 abgeschlossen zu sein**. Anschließend erfolgen die Schulung und das Onboarding.
- **Datenhoheit bei Vertragsende:** Der Anbieter sichert zu, bei Vertragsbeendigung alle Chat-Verläufe und Kontaktdaten in einem gängigen, maschinenlesbaren Format (z. B. CSV, JSON) für den Export bereitzustellen. Die Daten sind nach Vertragsende datenschutzkonform zu löschen. Der Export darf nicht an proprietäre Formate gebunden sein. Nach Vertragsende sind sämtliche Daten spätestens nach 30 Tagen zu löschen, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

 IKT-Ost AÖR	Öffentliche Ausschreibung	V050/2026
	Leistungsverzeichnis	19. Juni 2026

- **IT-Sicherheit:**

- Verschlüsselung bei Übertragung und Speicherung
- Protokollierung administrativer Zugriffe
- Regelmäßige Sicherheitsupdates