interactive digital media

COMPLIANCE-WHITEPAPER

DSGVO & ePrivacy für Business-Messaging

Rechtskonformes A2P-Messaging in der EU — das Zwei-Gesetze-Gerüst, die tatsächlich tragfähigen Rechtsgrundlagen für SMS, was nationale Aufsichtsbehörden wirklich durchsetzen, und eine praktikable Compliance-Basis für den produktiven Einsatz.

Erstausgabe veröffentlicht 2024

Aktuelle Fassung — Februar 2026

ÜBER DIESEN LEITFADEN

Compliance, ohne juristischen Jargon

Erstmals 2024 veröffentlicht und für 2026 aktualisiert, richtet sich dieser Leitfaden an die Menschen, die DSGVO- und ePrivacy-konforme Geschäftskommunikation tatsächlich umsetzen müssen: Marketing- und CRM-Verantwortliche, Datenschutzbeauftragte, Rechtsabteilungen und die Engineering-Teams, die die Opt-in-Flows bauen. Es ist kein juristischer Fachaufsatz, sondern eine praktikable Referenz, die erklärt, was die Regeln bedeuten, wenn man sie auf SMS-, RCS- oder WhatsApp-Business-Programme anwendet.

Die Fassung 2026 berücksichtigt zwei weitere Jahre nationaler Enforcement-Praxis, die anhaltende Verzögerung der ePrivacy-Verordnung und die zunehmende Bedeutung von Unterauftragsverarbeitern und Datenresidenz in Enterprise-Ausschreibungen.

Inhalt

WICHTIG — KEINE RECHTSBERATUNG

Dieser Leitfaden fasst EU-Regulierung und nationale Umsetzungen als praktikable Referenz zusammen. Er ist **keine Rechtsberatung** und ersetzt keine qualifizierte juristische Beratung in der jeweiligen Jurisdiktion. Regulatorische Auslegungen entwickeln sich weiter, Mitgliedstaaten regeln unterschiedlich, und der Einzelfall ist entscheidend. Ziehen Sie Ihren DSB und externe Rechtsberatung hinzu, bevor Sie Ihre Compliance-Aufstellung wesentlich ändern.

KAPITEL 01

Warum Compliance geschäftskritisch ist

Die Risiken, aktuelle Enforcement-Muster und warum EU-Messaging-Compliance spätestens seit 2023 kein „Nice-to-have" mehr ist.

Die Kosten des Scheiterns

Die DSGVO-Durchsetzung hat sich schnell etabliert. In den ersten Jahren nach Inkrafttreten 2018 haben Aufsichtsbehörden vor allem Leitlinien publiziert, Fallrecht aufgebaut und überwiegend moderate Bußgelder verhängt. Bis 2023–2025 drehte sich dieses Bild: Der Europäische Datenschutzausschuss (EDSA) berichtete **kumulierte DSGVO-Bußgelder von über 5,6 Mrd. €** in allen Mitgliedstaaten, mit regelmäßigen Einzelentscheidungen im acht- und neunstelligen Bereich. Messaging-Programme sind selten Gegenstand der Schlagzeilen-Bußgelder — diese bleiben den großen Datentransfer- und Werbefällen vorbehalten — aber SMS-, E-Mail- und WhatsApp-Marketing liegen genau in der Enforcement-Zone darunter, in der Aufsichten routinemäßig und schnell handeln.

20 Mio €
ODER 4 % UMSATZ
DSGVO-Höchstbußgeld, der höhere Betrag gilt

300.000 €
DEUTSCHLAND (§ 7 UWG)
Bußgeld pro Verstoß

5,6 Mrd €
+
SUMME DER BUSSGELDER
EU-weit seit 2018

72 h
MELDEFRIST
für Datenpannen an die Aufsichtsbehörde

Wo Enforcement beim Messaging tatsächlich ansetzt

Vier Muster tauchen in nationalen Entscheidungen zu SMS-, E-Mail- und Messenger-Marketing wiederholt auf:

- **Keine wirksame Einwilligung.** Vorangekreuzte Kästchen, Einwilligung gebündelt mit AGB, für einen anderen Zweck eingeholtes Opt-in wurde zweckentfremdet für Marketing wiederverwendet. Die mit Abstand häufigste Feststellung.
- **Unzureichender Widerruf.** STOP-Keywords, deren Umsetzung Tage dauert; Opt-outs, die nur einen Kanal stoppen, nicht das Programm; kein niedrigschwelliger Widerruf, der „so einfach sein muss wie die Erteilung" (Art. 7 Abs. 3 DSGVO).
- **Fehlende Informationen an die betroffene Person.** Informationspflichten nach Art. 13/14 DSGVO, die den Empfänger nie erreichen — oder in einer Sprache, die er vernünftigerweise nicht verstehen muss.
- **Internationale Übermittlung ohne Garantien.** Messaging-Daten werden von Unterauftragsverarbeitern außerhalb der EU/EWR verarbeitet — ein seit Schrems II stark aktives Enforcement-Thema, bis heute.

DER BUSINESS CASE JENSEITS DER BUSSGELDER

Bußgelder bekommen die Presseaufmerksamkeit, aber drei Folgekosten wiegen für die meisten Unternehmen schwerer: (1) Bereinigung — aus einer bereinigten Datenbasis eine neue Einwilligung wieder aufzubauen, ist aufwendig und teuer; (2) Kanalsperrung — Aufsichtsbehörden können und ordnen temporäre Aussetzung von Marketing-Aktivitäten an; (3) Reputationsschaden — eine öffentliche Entscheidung, die Ihr Unternehmen auf der Webseite einer Aufsicht nennt, lebt dauerhaft online weiter.

KAPITEL 02

Das Zwei-Gesetze-Gerüst

DSGVO und ePrivacy gelten beide gleichzeitig für Business-Messaging — wie sie ineinandergreifen, welches Regelwerk in Konfliktfällen vorgeht, und was die stockende ePrivacy-Verordnung praktisch verändert.

EU-Business-Messaging-Compliance steht auf zwei sich überlappenden Säulen, nicht auf einer. Die **Datenschutz-Grundverordnung (DSGVO, Verordnung 2016/679)** regelt jede Verarbeitung personenbezogener Daten — und eine Mobilfunknummer, die einer identifizierbaren Person zuzuordnen ist, ist ein personenbezogenes Datum. Die **ePrivacy-Richtlinie (2002/58/EG in der Fassung von 2009/136/EG)** regelt elektronische Kommunikation speziell, einschließlich der Regeln zu unverlangten Direktmarketing-Kommunikationen per SMS, E-Mail und Messenger. Beide gelten gleichzeitig; keine verdrängt die andere.

Wie beide Regelwerke in der Praxis zusammenspielen

Die ePrivacy-Richtlinie ist *lex specialis* — die spezielle Regel, die dort vorgeht, wo sie einen Sachverhalt ausdrücklich regelt (z. B. das Einwilligungserfordernis für unaufgeforderte SMS-Werbung nach Art. 13). Wo ePrivacy schweigt, füllt die DSGVO die Lücke — etwa bei Betroffenenrechten, Verantwortlichen- und Auftragsverarbeiterpflichten, internationalen Übermittlungen und Dokumentation. Ein konformes Messaging-Programm muss beidem genügen: der ePrivacy-Richtlinie für die Bedingungen, unter denen die Nachricht überhaupt versandt werden darf, und der DSGVO für alles rund um die Nachricht.

Die ausstehende ePrivacy-Verordnung

Die ePrivacy-Verordnung — als Nachfolgerin der Richtlinie von 2002 konzipiert, mit vollständiger Abstimmung auf die DSGVO — befindet sich seit 2017 in politischen Verhandlungen. Anfang 2026 ist sie weiterhin im Trilog, ohne bestätigtes Datum für die Verabschiedung. Für die Praxis bedeutet das: Die aktuelle Richtlinie (in der jeweiligen nationalen Umsetzung) bleibt das verbindliche Instrument, und Unternehmen sollten davon ausgehen, dass dies mindestens für die Laufzeit aktueller mehrjähriger Verträge so bleibt.

Nationale Umsetzungen zählen mehr als die Richtlinie selbst

Weil ePrivacy eine Richtlinie ist, gelten ihre Regeln nur über die jeweilige nationale Umsetzung. Deshalb kann dasselbe SMS-Marketing-Programm in einem Mitgliedstaat eindeutig konform und im anderen eindeutig nicht-konform sein, obwohl beide Länder „ePrivacy umsetzen". Die nationalen Unterschiede sind kein Detail — dort findet Enforcement statt. Kapitel 4 behandelt die fünf Jurisdiktionen, die den größten Anteil an Messaging-relevanten Enforcement-Entscheidungen stellen.

Warum EU-gehostete Infrastruktur hier zählt. Da DSGVO und ePrivacy beide auf den gesamten Lebenszyklus der Nachricht anwendbar sind — einschließlich der Verarbeitung durch Ihren Messaging-Dienstleister und dessen Unterauftragsverarbeiter — ist der Standort und die rechtliche Jurisdiktion Ihrer Messaging-Infrastruktur selbst eine Compliance-Frage. Die Infrastruktur von IDM ist vollständig in Deutschland gehostet; unser Schwesterunternehmen **AnyMessage** operiert auf derselben EU-ansässigen Grundlage. Für Unternehmen, deren DSB eine klare Linie bei EU-Datenresidenz für Messaging gezogen hat, repräsentieren wir zusammen eine der kürzesten Shortlists am Markt. Es existieren weitere starke EU-basierte Anbieter — dies ist Offenlegung, kein Alleinstellungsanspruch.

KAPITEL 03

Rechtsgrundlagen & belastbare Einwilligung

Welche Rechtsgrundlage nach Art. 6 DSGVO für welchen Nachrichtentyp gilt, was Art. 7 DSGVO für eine wirksame Einwilligung verlangt, und die Soft-Opt-in-Regel, die die meisten Unternehmen falsch auslegen.

Die richtige Rechtsgrundlage wählen

Art. 6 Abs. 1 DSGVO listet sechs mögliche Rechtsgrundlagen für die Verarbeitung personenbezogener Daten auf. Beim Business-Messaging tragen drei davon praktisch den gesamten Verkehr: Einwilligung, Vertragserfüllung und berechtigtes Interesse. Die korrekte Wahl pro Anwendungsfall ist das Fundament, auf dem das restliche Programm steht.

ANWENDUNGSFALL	TYPISCHE RECHTSGRUNDLAGE	WARUM — UND WORAUF ZU ACHTEN IST
OTP / 2FA	Vertrag (Art. 6 Abs. 1 lit. b)	Erfüllung des vom Nutzer angeforderten Dienstes. Kein Marketing. Einwilligung

ANWENDUNGSFALL	TYPISCHE RECHTSGRUNDLAGE	WARUM — UND WORAUF ZU ACHTEN IST
		regelmäßig nicht erforderlich.
Liefer- / Servicebenachrichtigungen	Vertrag oder berechtigtes Interesse	„Ihr Auftrag wurde versandt"-Nachrichten sind transaktional. Grenze zum Cross-Selling beachten.
Terminerinnerungen	Berechtigtes Interesse (Art. 6 Abs. 1 lit. f)	Tragfähig, wenn der Dienst angefordert wurde und die Erinnerung No-Shows reduziert. Abwägung dokumentieren.
Direktmarketing	Einwilligung (Art. 6 Abs. 1 lit. a) + Art. 13 ePrivacy	Vorherige, spezifische, informierte, unmissverständliche Einwilligung erforderlich — oder strenger Soft-Opt-in für Bestandskunden.
Umfragen / Forschung	Berechtigtes Interesse oder Einwilligung	Abhängig davon, ob Teilnahme incentiviert wird und ob die Umfrage wirklich von Marketing trennbar ist.

Was Art. 7 DSGVO für eine wirksame Einwilligung verlangt

Wo Einwilligung die Rechtsgrundlage ist, müssen die vier kumulativen Bedingungen nach Art. 4 Nr. 11 und Art. 7 DSGVO erfüllt sein: **freiwillig**, **spezifisch**, **informiert** und durch eine **eindeutige bestätigende Handlung**. Schweigen, vorangekreuzte Kästchen und Inaktivität reichen nicht. Einwilligung muss außerdem **nachweisbar** sein (Art. 7 Abs. 1) — das heißt: Sie müssen für jede Mobilfunknummer belegen können, wer eingewilligt hat, wann, über welchen Mechanismus und für welchen Zweck. Und der Widerruf muss „so einfach wie die Erteilung" sein (Art. 7 Abs. 3) — ein „STOP" per SMS ist der De-facto-Standard.

Double-Opt-in — dringend empfohlen

Obwohl die DSGVO kein Double-Opt-in ausdrücklich vorschreibt, behandelt es die deutsche Rechtsprechung als faktischen Beweis-Standard. Das Muster — Mobilfunknummer erfassen, eine SMS mit Bestätigungsbitte versenden, den Teilnehmer erst als eingewilligt behandeln, wenn eine bestätigende Antwort eingeht — erzeugt einen zeitnahen Audit-Trail, der nur schwer anzugreifen ist. Für jedes EU-Programm relevanten Volumens ist es der Weg des geringsten regulatorischen Risikos.

Die Soft-Opt-in-Regel — genau

Art. 13 Abs. 2 ePrivacy erlaubt Direktwerbung per SMS oder E-Mail an Bestandskunden für *eigene ähnliche Produkte oder Dienstleistungen* ohne erneute ausdrückliche Einwilligung, sofern dem Kunden bei Erhebung der Kontaktdaten und in jeder nachfolgenden Nachricht eine klare Widerspruchsmöglichkeit eingeräumt wurde. Diese „Soft-Opt-in"-Ausnahme ist enger, als viele Unternehmen annehmen. Drei häufige Fehlinterpretationen:

- **„Ähnlich" wird eng ausgelegt** — eine Bank kann sich nicht auf Soft-Opt-in stützen, um nicht verwandte Versicherungsprodukte an Hypothekenkunden zu vermarkten.
- **„Bestandskunde" setzt eine tatsächliche Geschäftsbeziehung voraus** — ein Whitepaper-Download allein begründet keinen Kundenstatus.
- **Die Widerspruchsmöglichkeit muss aktiv in jeder Nachricht bestehen** — nicht nur irgendwo in der Datenschutzerklärung verfügbar sein.

KAPITEL 04

Nationale Varianten mit Biss

Die fünf Mitgliedstaaten-Regime, in denen der Großteil des messaging-relevanten Enforcements stattfindet — und die jeweiligen Fallen, die vor der nächsten Kampagne kennen sollte.

DE

Deutschland — UWG, BDSG & TTDSG

Das strengste Verbraucherschutzregime der EU für unaufgeforderte kommerzielle Kommunikation. Bußgelder bis 300.000 € pro Verstoß nach § 7 UWG. Double-Opt-in ist in der Rechtsprechung faktisch Pflicht. BfDI und Landesdatenschutzbehörden setzen beide durch; TTDSG ergänzt die Regeln zur Telekommunikation.

FR

Frankreich — CNIL

Die CNIL verlangt explizites Opt-in und ein klares Opt-out-Keyword (STOP au XXXXX) in jeder kommerziellen SMS. Sanktionen nach der Loi Informatique et Libertés (LIL, DSGVO-Umsetzungsgesetz) können den DSGVO-Höchstrahmen erreichen. Die CNIL ist eine der aktivsten Aufsichten Europas bei SMS-Marketing.

IT

Italien — Garante

Besonders aktiv bei Telemarketing und SMS-Marketing. Mehrfach siebenstellige Bußgelder verhängt. Enforcement konzentriert sich auf die Herkunft der Einwilligung (wer hat tatsächlich eingewilligt) und auf die Nutzung von Drittanbieter-Lead-Datenbanken.

ES

Spanien — AEPD & LSSI

Die spanische AEPD ist in der EU nach Zahl der Entscheidungen die durchsetzungsstärkste Aufsicht. LSSI (Ley de Servicios de la Sociedad de la Información) ergänzt die DSGVO um spezifische Regeln für kommerzielle elektronische Kommunikation. Bußgelder bei unverlangter SMS liegen regelmäßig im sechsstelligen Bereich.

UK

Vereinigtes Königreich — PECR & ICO

Seit dem Brexit formal außerhalb der EU, aber substanziell angeglichen. PECR (2003, mit Änderungen) spiegelt die ePrivacy-Richtlinie. UK-GDPR spiegelt die DSGVO. Die ICO setzt aktiv gegen unverlangte SMS-Kampagnen durch, mit Bußgeldern bis 500.000 £ nach PECR (höher, wo PECR und UK-GDPR zugleich greifen).

EU

EDSA & One-Stop-Shop

Für Unternehmen mit Tätigkeit in mehreren Mitgliedstaaten bestimmt der One-Stop-Shop der DSGVO eine federführende Aufsichtsbehörde — in der Regel im Mitgliedstaat der Hauptniederlassung. ePrivacy unterliegt aber nicht dem One-Stop-Shop: Jede nationale Aufsicht kann unabhängig gegen ePrivacy-Verstöße vorgehen.

Speziell für DACH-Unternehmen. Die Kombination aus § 7 UWG, BDSG, TTDSG und den starken Rechtsprechungsanforderungen an das Double-Opt-in erzeugt in Deutschland das in der EU anspruchsvollste praktische Compliance-Umfeld. IDM ist eine deutsche GmbH mit Hauptsitz in Lübeck; AnyMessage operiert in derselben Konzernstruktur. Für in Deutschland ansässige Unternehmen und DACH-Regionaleinheiten entfällt mit einem Vertragspartner unter derselben Jurisdiktion (und einem unkomplizierten AVV nach § 28 BDSG bzw. Art. 28 DSGVO) eine ganze Klasse von Übermittlungs- und Unterauftragsverarbeiter-Fragen aus der DSB-Prüfung. Andere EU-basierte Anbieter bieten vergleichbare Strukturen; wir erheben keinen Alleinstellungsanspruch.

KAPITEL 05

Praktikable Compliance-Basis

Eine Arbeits-Checkliste, eine Zusammenfassung, was ein Auftragsverarbeitungsvertrag (AVV) tatsächlich abdecken muss, und was auf Plattformebene automatisiert statt Menschen überlassen werden sollte.

Die Compliance-Checkliste

Die folgende Basis ist aus aktuellen EDSA-Leitlinien, aktiven Enforcement-Mustern und dem deutschen Case-Law-Standard abgeleitet. Das Einhalten garantiert keine Compliance — Einzelfälle zählen — aber das Verfehlen eines der Punkte ist ein zuverlässiger Weg, ein Prüfungsverfahren zu verlieren.

- ✓ **Dokumentiertes Opt-in je Rufnummer** — Quelle, Zeitstempel, exakter Einwilligungstext, IP-Adresse bei Online-Erhebung und der konkret eingewilligte Zweck.
- ✓ **Double-Opt-in für Marketing in DE/AT/CH** — und im gesamten EU-Raum dringend empfohlen.
- ✓ **Opt-outs innerhalb eines Nachrichtenzyklus beachtet** — STOP, STOPP, ARRÊT, PARE, CANCELAR und weitere lokale Entsprechungen, je nach bedienten Märkten.
- ✓ **Informationspflichten nach Art. 13/14 DSGVO erfüllt** bei der Datenerhebung — Identität des Verantwortlichen, Zwecke, Rechtsgrundlage, Speicherdauer, Betroffenenrechte, Beschwerderecht bei der Aufsicht.
- ✓ **Tageszeitregeln je Zielland auf Plattformebene durchgesetzt**, nicht einzelnen Kampagnenmanagern überlassen.
- ✓ **AVV mit jedem Messaging-Anbieter** entsprechend Art. 28 DSGVO — siehe unten.
- ✓ **Transparenz zu Unterauftragsverarbeitern** — aktuelle, zugängliche Liste mit Änderungsbenachrichtigung.
- ✓ **Übermittlungsmechanismus dokumentiert** für alle Datenflüsse außerhalb EU/EWR — SCCs, Angemessenheitsbeschluss oder BCRs, mit dokumentiertem Transfer Impact Assessment (TIA).
- ✓ **Aufbewahrungsfristen definiert und automatisiert** — Metadaten und DLRs nur für dokumentierte berechtigte Zwecke und definierte Zeiträume.
- ✓ **72-Stunden-Meldeprozess für Datenpannen** erprobt und einer benannten Person zugewiesen.

Was der AVV abdecken muss

Jeder Auftragsverarbeitungsvertrag muss alle Anforderungen aus Art. 28 Abs. 3 DSGVO abdecken — Verarbeitung nur nach dokumentierten Weisungen, Vertraulichkeit des Personals, Sicherheitsmaßnahmen, Unterauftragsverarbeiter, Unterstützung bei Betroffenenrechten, Unterstützung bei Meldung von Datenpannen, DSFA-Unterstützung, Rückgabe oder Löschung bei Vertragsende und Auditrechte. In der Praxis gehen Enterprise-AVVs weiter: Standort der Verarbeitung (Datenresidenz), Verschlüsselungsstandards in Transit und at Rest, Incident-Response-SLA und Haftungsverteilung.

WAS AUTOMATISIERT STATT MENSCHLICH GEHANDHABT GEHÖRT

Eine moderne Messaging-Plattform muss die Herkunft der Einwilligung (Blockierung von Sends an nicht eingewilligte Nummern), das Beachten des Widerrufs (STOP-Verarbeitung im selben Nachrichtenzyklus), Tageszeitregeln je Land und Aufbewahrungsfristen durchsetzen — ohne dass ein Mensch daran denken müsste. Wenn Ihr aktueller Anbieter diese Punkte Ihnen auf Kampagnenkonfigurationsebene überlässt, ist das eine Lücke, die vor der nächsten Prüfung geschlossen werden sollte.

KAPITEL 06

Anbieter- und Auftragsverarbeiter-Auswahl

Die compliance-spezifischen Kriterien für die Wahl eines Messaging-Anbieters, wenn EU-Datenschutz eine erstrangige Anforderung ist und kein Checkbox-Punkt.

Die meisten Messaging-Ausschreibungen werden über Abdeckung, Zustellbarkeit und Preis entschieden. Für Unternehmen, bei denen EU-Compliance eine nicht verhandelbare Anforderung ist — Banken, Gesundheitswesen, öffentlicher Sektor und zunehmend jede Verbrauchermarke mit signifikanten EU-Operationen — verdienen vier zusätzliche Kriterien Gewicht im Verhältnis zur regulatorischen Exposition.

#	KRITERIUM	WORAUF IN DER AUSSCHREIBUNG PRÜFEN
1	**Vertragspartner & Jurisdiktion**	Mit welcher Rechtseinheit schließen Sie den Vertrag, unter welcher Mitgliedstaaten-Jurisdiktion? Eine EU-Einheit vereinfacht AVV-Verhandlung und reduziert Übermittlungsfragen.
2	**Verarbeitungsorte**	Wo werden personenbezogene Daten verarbeitet, gespeichert, gesichert? Nur EU? EU plus benannte Drittländer? Welche Unterauftragsverarbeiter, wo?
3	**AVV & Art.-28-Abdeckung**	

#	KRITERIUM	WORAUF IN DER AUSSCHREIBUNG PRÜFEN
		Standard-AVV einfordern. Bestätigung der Übereinstimmung mit Art. 28 Abs. 3, SCCs wo relevant, Auditrechte, Incident-Response-SLA.
4	**Unterauftragsverarbeiter-Governance**	Aktuelle Liste der Unterauftragsverarbeiter, Änderungsbenachrichtigungsprozess, Widerspruchsrechte. Carrier-Partner und Hubs zählen als Unterauftragsverarbeiter.
5	**Sicherheitszertifizierungen**	ISO 27001 als Minimum; SOC 2 Type II ein Plus; Infrastruktur in akkreditierten Rechenzentren mit dokumentierten physischen und logischen Kontrollen.
6	**Plattform-seitige Controls**	Kann die Plattform Opt-out-Beachtung, Tageszeitregeln und Aufbewahrungsfristen automatisch je Land/Kampagne durchsetzen?

Wo IDM und AnyMessage hier einzuordnen sind. DSGVO- und ePrivacy-Compliance ist das Marktsegment, in dem unsere Positionierung am deutlichsten ist. IDM ist eine deutsche GmbH mit vollständig in Deutschland gehosteter Infrastruktur. AnyMessage operiert auf derselben EU-ansässigen Grundlage unter demselben Konzern. Unsere AVVs sind auf Art. 28 Abs. 3 DSGVO und § 28 BDSG ausgerichtet; Auditrechte, Transparenz zu Unterauftragsverarbeitern und Incident-Response-SLAs in dem Umfang, den Enterprise-DSBs erwarten, sind für uns Standard. Für Unternehmen, deren Hauptanforderung EU-Compliance ist, sind wir ein natürlicher Shortlist-Kandidat. Für Unternehmen, deren Hauptbedarf globale Omnichannel-Breite mit EU-Compliance als Nebenbedingung ist, empfiehlt sich der direkte Vergleich mit den globalen CPaaS-Anbietern nach den obigen Kriterien.

ÜBER DEN HERAUSGEBER

interactive digital media GmbH

IDM ist ein deutscher Cloud-Kommunikationsdienstleister, 2003 gegründet und mit Hauptsitz in Lübeck. Die proprietäre **IMT-HUB®**-Plattform in vierter Generation ist einer von weltweit rund 40 von der GSMA zertifizierten Open-Connectivity (OC) SMS-Hubs. Wir bedienen Unternehmen, Mobilfunkbetreiber und Service-Provider aller großen Industrien — mit einer vollständig in Deutschland gehosteten Infrastruktur. Seit 2024 gehört IDM zur **United Capital / AnyMessage Gruppe**; unser Schwesterunternehmen AnyMessage betreibt komplementäre Messaging-Infrastruktur, und zusammen bilden wir eine europäische Messaging-Gruppe mit besonderer Stärke in regulierten, compliance-sensitiven Einsatzszenarien.

20+	200+	1.000+	~40
JAHRE	**LÄNDER**	**NETZBETREIBER**	**GSMA-OC-HUBS**
operativer Erfahrung	erreichbar über unser Netz	direkt oder über OC	IDM ist einer davon

Für wen wir arbeiten

IDM betreut Unternehmenskunden aus Banking, Automotive, Healthcare, Forschung, Handel, Tourismus und dem öffentlichen Sektor sowie Carrier-Partner in der EU, der GCC-Region und internationalen Hub-Netzen. Da Messaging für viele unserer Kunden geschäftskritisch ist, nennen wir konkrete Referenzen nur nach vorheriger schriftlicher Zustimmung und im Einzelfall — auf Anfrage unter NDA.

SPRECHEN SIE MIT UNS

Falls dieser Leitfaden Fragen zu Ihrer Compliance-Aufstellung, Ihren AVVs oder Ihren Anbietern aufwirft — wir sprechen gerne mit Ihnen. Unternehmensanfragen: **sales@i-digital-m.com**. Netzbetreiber, Aggregatoren und Reseller: **partners@i-digital-m.com**. Oder telefonisch unter **+49 (0)451 31 70 21-0**.

Lassen Sie uns ins Gespräch kommen

Excellence in Cloud Communication Services

Vertrieb & allgemeine Anfragen
INTERACTIVE DIGITAL MEDIA GMBH
✉ sales@i-digital-m.com
☏ +49 (0)451 31 70 21-0

Partnerprogramm
NETZBETREIBER · AGGREGATOREN · RESELLER
✉ partners@i-digital-m.com
☏ +49 (0)451 31 70 21-0

Online
WEBSITE & KUNDENPORTAL
🌐 www.i-digital-m.com
☏ +49 (0)451 31 70 21-0

Hauptsitz
interactive digital media GmbH · Moislinger Allee 9d · 23558 Lübeck · Deutschland
Niederlassungen in London (UK) und Neu-Delhi (IN) · Teil der United Capital / AnyMessage Gruppe