interactive digital media

ENTERPRISE-WHITEPAPER

Der A2P-SMS-Leitfaden

Was Unternehmen über Application-to-Person-Messaging wissen müssen: Technologie, Regulierung, Best Practices und Anbieterauswahl — auf zwölf Seiten.

Erstausgabe veröffentlicht 2024

Aktuelle Fassung — Februar 2026

ÜBER DIESEN LEITFADEN

Ein praktischer Leitfaden für Enterprise-Messaging

Erstmals 2024 veröffentlicht und für 2026 aktualisiert, fasst dieser Leitfaden zwei Jahrzehnte operativer Erfahrung im Application-to-Person (A2P) SMS-Bereich zu einer praktikablen Referenz zusammen — für die Menschen, die tatsächlich Messaging-Programme verantworten oder auswählen.

Die Fassung 2026 aktualisiert die regulatorischen Bezüge, die Marktdaten, das Kapitel zur Sicherheit (insbesondere zu Artificially Inflated Traffic, AIT) sowie die Kriterien der Anbieterauswahl. Inhalt und Struktur spiegeln wider, was Einkäufer in aktuellen Ausschreibungen tatsächlich fragen.

Inhalt

Ein Hinweis zur Nennung von Anbietern. Dies ist ein vom Anbieter selbst veröffentlichter Leitfaden. Wo konkrete Anbieter genannt werden — einschließlich IDM und unser Schwesterunternehmen AnyMessage — kennzeichnen wir dies klar. Die beschriebenen Kriterien und Rahmenwerke sind unabhängig davon nützlich, für welchen Anbieter sich Leser letztlich entscheiden.

KAPITEL 01

A2P-SMS und wie es funktioniert

Eine pragmatische Arbeitsdefinition, warum SMS auch 2026 dominiert, und der Ende-zu-Ende-Zustellpfad, den jede Nachricht von der Anwendung bis zum Endgerät durchläuft.

Eine Arbeitsdefinition

Application-to-Person (A2P) SMS ist jede Textnachricht, die von einer Software an einen Mobilfunkteilnehmer gesendet wird. Die Anwendung kann ein CRM, ein Banking-Kernsystem, eine E-Commerce-Plattform, ein Authentifizierungsdienst oder ein IoT-Backend sein; der Empfänger ist jeder Mobilfunkteilnehmer mit einem SMS-fähigen Endgerät. Das Pendant ist **Person-to-Person (P2P)** — zwei Menschen, die sich gegenseitig Nachrichten senden. Diese Unterscheidung ist nicht nur Terminologie: Sie bestimmt die Preisgestaltung (A2P-Terminierungsentgelte liegen deutlich über P2P-Raten), das Routing (A2P muss über registrierte kommerzielle Routen laufen, nicht über graue Routen), die Regulierung (Einwilligungs-, Absender- und Opt-out-Pflichten gelten für A2P) und die SLA-Erwartungen (Zustellquittungen, Fallback-Routing, 24/7-Support).

Warum SMS 2026 weiter dominiert

SMS ist der einzige Business-Messaging-Kanal, der auf jedem Mobiltelefon, in jedem Land, ohne App, ohne Datenverbindung, ohne Login und ohne Plattformbetreiber-Freigabe funktioniert. Wenn eine Bank ein Einmal-Passwort in 200 Länder in unter drei Sekunden zustellen muss, gibt es nichts Vergleichbares.

~98 %	< 3 s	100 %	0
ÖFFNUNGSRATE	**TYPISCHE LATENZ**	**GERÄTEABDECKUNG**	**APP-INSTALLATIONEN**
innerhalb von Minuten nach Zustellung	A2P zum Endgerät, weltweit	jedes SIM-fähige Telefon	keine Datenverbindung erforderlich

Der Ende-zu-Ende-Zustellpfad

Eine A2P-SMS durchläuft zwischen Ursprungsanwendung und Empfängergerät vier bis sechs unterschiedliche Systeme. Jeder Hop ist ein Moment für Routing, Filterung oder Ausfall — und jeder ist der Punkt, an dem ein seriöser Messaging-Anbieter sein Honorar verdient.

1 · Anwendung CRM / Core / Auth › **2 · API** HTTP/REST oder SMPP › **3 · Hub** Routing, HLR, Firewall › **4 · Carrier** SMSC, SS7/ Sigtran › **5 · Endgerät** Zustellung + DLR

Im Hub durchläuft jede Nachricht Rufnummernvalidierung, HLR/MNP-Abfrage zur Bestimmung des *aktuellen* Heimnetzes (durch die Rufnummernportabilität ist die ursprüngliche Vorwahl häufig irreführend), Routenauswahl, Inhalts- und Compliance-Filterung sowie Firewall-Prüfung auf AIT- und Impersonations-Muster. Nach dem Routing wird die Nachricht an das SMSC eines Terminierungscarriers übergeben (über SMPP oder SS7/Sigtran), und Zustellquittungen (DLRs) kehren als Nachweis der Zustellung zurück.

WAS „CARRIER-GRADE" TATSÄCHLICH BEDEUTET

Wenn ein Anbieter sich als „carrier-grade" bezeichnet, meint er üblicherweise vier Dinge: geografisch redundante Infrastruktur mit Echtzeit-Replikation, direkte SS7/Sigtran-Konnektivität zu Netzbetreibern, 24/7-NOC-Überwachung mit Alarmierung im Sekundenbereich und eine vertraglich zugesicherte Verfügbarkeit von 99,9 % oder besser. Lassen Sie sich alle vier Punkte belegen — keine Broschüre, sondern Live-Dashboards und Referenzgespräche.

KAPITEL 02

Kernanwendungsfälle

Die fünf Workloads, die rund 90 % des weltweiten A2P-Volumens ausmachen — und was jeder davon vom Kanal verlangt.

O

OTP & 2FA-Authentifizierung

Der volumenmäßig größte Einzelanwendungsfall. Zustellung in unter drei Sekunden, nahezu 100 % Zustellquote, keinerlei Toleranz für Nachrichtenverluste. Der am stärksten durch AIT attackierte Datenverkehrstyp — dedizierte Premium-Routen sind erforderlich. Keine URLs in OTP-Nachrichten: viele Netzbetreiber filtern diese als Phishing.

T

Transaktionale Benachrichtigungen

Lieferverfolgung, Zahlungsbestätigungen, Terminerinnerungen, Reise-Updates. Geringere Latenz-Priorität als OTP, höheres Volumen. Unternehmen verlagern diese zunehmend von E-Mail zu SMS, um das Inbound-Call-Volumen zu reduzieren — eine SMS zu Cent-Bruchteilen schlägt einen 8-Euro-Supportanruf.

M

Marketing & CRM

Höchste Compliance-Anforderungen. Erfordert eine explizite, DSGVO-konforme Einwilligung in der EU, „prior express written consent" nach TCPA in den USA, Template-Registrierung nach DLT in Indien. Kombination mit RCS/WhatsApp dort, wo Opt-in vorliegt — SMS bedient, was diese Kanäle nicht erreichen.

C

Kundenservice & Zwei-Wege-Dialog

Inbound-SMS, Keyword-Befehle (STOP, HELP, STATUS), Kurzwahlen, konversationelle Abläufe. Oft der SMS-Teil eines WhatsApp- oder RCS-Dialogs — SMS als universeller Fallback, nicht als primärer Kanal.

I

M2M / IoT

Gerätegenerierte Signalisierung: Fahrzeug-Telematik, Smart Meter, Alarmanlagen, POS-Terminals. Geringe Volumina je Gerät, große Flotten. In der Regel deterministische Zustellung, lange Gültigkeitsdauern und internationaler Roaming-Support erforderlich.

+

Entstehende Muster

Voice-OTP als Fallback in Märkten mit SMS-Restriktionen, Flash-Call-Verifizierung (in der EU seit 2023 eingeschränkt) und zunehmend KI-gesteuerte Service-Bots hinter Kurzwahlen oder Langnummern.

OPERATIVE FAUSTREGEL

Leiten Sie OTP-Traffic niemals über denselben Carrier-Pfad wie Marketing-Traffic. Unterschiedliche Latenz-Toleranzen, unterschiedliche Firewall-Profile, unterschiedliche Betrugsexposition. Trennen Sie beides in Ihrer Plattform und in Ihren SLAs.

KAPITEL 03

Regulierung & Compliance

Die vier sich überlagernden regulatorischen Ebenen, die für jede unternehmerische A2P-Nachricht gelten — und eine praktikable Compliance-Basis für 2026.

A2P-Compliance umfasst vier überlappende Regime, die jeweils unterschiedliche Aspekte derselben Nachricht betreffen: **Einwilligung und Datenschutz** (wer hat wie und für welchen Zweck zugestimmt?), **Inhalt** (länderspezifische Verbotskategorien), **Absenderkennung** (was erscheint auf dem Endgerät, und wurde dies

registriert, wo Registrierung erforderlich ist?) und **Sendefenster und Frequenz** (Tageszeitregeln, Do-Not-Disturb-Listen).

Europa — DSGVO, ePrivacy und nationale Varianten

Innerhalb der EU unterliegt kommerzielle A2P-SMS primär der DSGVO (Verordnung 2016/679) und der ePrivacy-Richtlinie (2002/58/EG). Die Kernregel: **Vor dem Versand einer Direktmarketing-SMS ist eine vorherige, spezifische, informierte und freiwillige Einwilligung erforderlich** — mit der engen „Soft-Opt-in"-Ausnahme nach Art. 13 Abs. 2 ePrivacy für Bestandskunden bei ähnlichen Produkten. Transaktionale Nachrichten — Einmal-Passwörter, Zustellbenachrichtigungen, Terminerinnerungen für angeforderte Dienstleistungen — stützen sich in der Regel auf berechtigtes Interesse oder vertragliche Erforderlichkeit statt auf ausdrückliche Marketing-Einwilligung. Die kritische Grenzlinie ist der Zweck: Eine „Ihr Paket ist da"-SMS, die mit „50 % Rabatt auf Ihren nächsten Einkauf" endet, ist eine Marketingnachricht.

Nationale Umsetzungen verschärfen das Bild. § 7 UWG in Deutschland sieht Bußgelder von bis zu 300.000 Euro pro Verstoß vor; das Double-Opt-in ist faktischer Standard und rechtsprechungsfest. Die französische CNIL verlangt explizites Opt-in und ein klares Opt-out-Keyword in jeder Nachricht. Die britische PECR spiegelt ePrivacy weitgehend; die ICO setzt aktiv durch. Die italienische Garante und die spanische AEPD haben mehrfach siebenstellige Bußgelder für A2P-Marketing ohne Einwilligung verhängt.

> **Wo IDM und AnyMessage hier einzuordnen sind.** Für Unternehmen, deren Hauptanforderung EU/EWR-Datenresidenz, vollständige DSGVO-konforme Verarbeitung, in Deutschland gehostete Infrastruktur und eine Rechtseinheit innerhalb der EU für AVV-Zwecke ist, gehören IDM und das Schwesterunternehmen **AnyMessage** zu den Anbietern, die genau für diese Randbedingung aufgestellt sind. Es gibt weitere starke EU-basierte Anbieter — wir erheben keinen Exklusivanspruch — aber für Einkäufer, bei denen EU-Compliance ein nicht verhandelbares Auswahlkriterium ist, verkürzen IDM und AnyMessage gemeinsam die Shortlist spürbar.

Nordamerika, Indien und darüber hinaus

Die USA stützen sich auf drei Regelwerke: Der **TCPA** (47 USC §227) setzt den Einwilligungsstandard mit gesetzlichem Schadensersatz von 500 bis 1.500 US-Dollar je Nachricht; die **CTIA Messaging Principles** sind ein von Carriern durchgesetzter Kodex zu Inhalt und Opt-in/Opt-out; **10DLC** erfordert die Registrierung von Marke und Kampagne bei The Campaign Registry für A2P über Langnummern. Kanada ergänzt um CASL, das dem EU-Standard näher steht als der TCPA. Indien betreibt das technisch fortschrittlichste Regime weltweit — jede kommerzielle SMS muss ein vorregistriertes Template mit registrierter Absenderkennung auf der DLT-Plattform verwenden; nicht konforme Nachrichten werden an der Netzwerk-Firewall blockiert. VAE, Saudi-Arabien, Katar und eine wachsende Zahl von Regulierungsbehörden am Golf und in Afrika betreiben Absenderkennungs-Whitelists mit Registrierungspflicht.

Eine praktikable Compliance-Basis

- ✓ Dokumentiertes Opt-in für jede Rufnummer: Quelle, Zeitstempel, Einwilligungsumfang.
- ✓ Opt-out-Keywords (STOP und lokale Entsprechungen) innerhalb eines Nachrichtenzyklus beachten.

- ✓ Tageszeitregeln pro Zielland automatisch auf Plattformebene durchsetzen.
- ✓ Absenderkennungen und Templates in jeder Jurisdiktion registrieren, die dies verlangt.
- ✓ Auftragsverarbeitungsvertrag (AVV) mit dem Messaging-Anbieter für EU-Traffic; Datenresidenz bestätigt.
- ✓ Revisionssicherer Audit-Trail — Inhalte, Metadaten und DLRs nach Rechtsgrundlage.

KAPITEL 04

Sicherheit & Betrugsabwehr

Graue Routen, SIM-Boxes, Artificially Inflated Traffic und die Firewalls, die dagegen schützen — die Betrugsmuster, die das Enterprise-Messaging-Risiko im Jahr 2026 prägen.

A2P-Betrug ist kein Randphänomen. Branchenübliche Schätzungen beziffern den jährlichen Umsatzverlust der Netzbetreiber durch graue Routen und verwandten Betrug auf ein- bis zweistellige Milliardenbeträge in US-Dollar; allein die Verluste der Unternehmen durch AIT bewegen sich im dreistelligen Millionenbereich. Zu den direkten Kosten (Bezahlung von Nachrichten, die niemand erreicht) kommen Zweitrundeneffekte: einbrechende Konversionsraten, regulatorische Exposition durch nicht konforme Zwischenhändler und Reputationsschäden, wenn Zustellungen über graue Routen öffentlich scheitern.

Die drei relevanten Betrugsmuster

Graue Routen liefern A2P-Traffic aus und klassifizieren ihn fälschlich als P2P, um höhere Terminierungsentgelte und Compliance-Kontrollen des Netzbetreibers zu umgehen. Die Preise liegen dramatisch unter sauberem A2P — oft 70 bis 80 % darunter — die Zustellung wirkt zunächst normal und verschlechtert sich dann, sobald die Firewalls der Netzbetreiber die Muster lernen. **SIM-Box-Betrug** nutzt Hardware, die mit Verbraucher-SIMs bestückt ist, um eingehenden A2P-Traffic als lokales P2P zu re-originieren — das Terminierungsentgelt wird dem Netzbetreiber entzogen und das Markenbranding der Absenderkennung zerstört. **Artificially Inflated Traffic (AIT)** — auch SMS-Pumping — ist das Muster, das seit 2022 am aggressivsten gewachsen ist: Angreifer betreiben Pools von Rufnummern und schleusen diese in Registrierungs- und OTP-Flüsse von Unternehmen ein, kassieren einen Anteil des Terminierungsentgelts, während das Unternehmen für Nachrichten bezahlt, die niemand Legitimer je wollte.

AIT-WARNSIGNALE — KONTINUIERLICH ÜBERWACHEN

Plötzliche Spitzen bei OTP-Anfragen aus Rufnummernbereichen oder Ländern, in denen Sie nicht vermarkten. Ungewöhnlich hohe Zustellraten bei gleichzeitig ungewöhnlich niedrigen Folgekonversionen (Empfänger „bekommen" das OTP, schließen aber nie die Registrierung ab). Clustering auf spezifischen MNC/MCC-Kombinationen. Registrierungs-Geschwindigkeiten jenseits realistischen menschlichen Verhaltens. Eine moderne, versandseitige Firewall erkennt all dies.

Die SMS-Firewall als operative Verteidigung

F

Traffic-Klassifizierung

Identifiziert A2P, P2P, Spam und grauen-Routen-Traffic in Echtzeit auf Basis von Inhalt, Ursprung und Muster. Verwirft oder berechnet Traffic, der seiner deklarierten Klasse nicht entspricht.

C

Inhaltsfilterung

Blacklists, Whitelists, Keyword-Regeln, länderspezifische Inhaltsrichtlinien, URL-Reputationsabfragen. Setzt vorgeschriebene Beschränkungen automatisch durch.

V

Velocity- & Anomalieerkennung

Kennzeichnet Absenderkennungs-Spoofing, unrealistische Anfragefrequenzen, geografisches Clustering und Rufnummern-Konzentrationen, die auf AIT hindeuten.

R

Revenue Assurance

Gleicht Traffic-Klasse mit Terminierungsentgelten ab. Stellt sicher, dass A2P zu A2P-Raten bezahlt wird und Leckagen über graue Routen erfasst werden, bevor sie zu Disputen werden.

Die IMT-HUB®-Firewall von IDM — wie auch die Firewalls jedes glaubwürdigen Hub-Betreibers — macht diese Ebene sowohl für Unternehmenskunden als auch für Netzbetreiber zugänglich. Das heißt: Unternehmen können eigene AIT-Toleranzen definieren und werden in Echtzeit alarmiert, wenn Muster auftreten. Jede seriöse Anbieterbewertung sollte Firewall-Fähigkeiten im Detail prüfen.

KAPITEL 05

Anbieterauswahl

Neun Kriterien, die gute A2P-Anbieter tatsächlich von schlechten unterscheiden, und die Fragen, die in jede Ausschreibung gehören.

#	KRITERIUM	WORAUF PRÜFEN
1	**Abdeckung & Routenqualität**	Direkte Carrier-Anbindungen vs. Sub-Aggregatoren. Anteil des Traffics auf direkten, A2P-zugelassenen Routen. Belege, keine Aussagen.
2	**GSMA-OC-Zertifizierung**	Ist der Hub OC-zertifiziert? Wenn nicht: über welchen OC-Hub wird terminiert?
3	**Zustellbarkeit & DLR-Qualität**	Länderspezifische SLAs. Echte netzbetreiber-generierte Quittungen oder synthetisiert? Live-Dashboards verfügbar?
4	**Firewall & AIT-Schutz**	Welche Erkennung läuft auf ausgehendem Traffic? Welche Kontrollen können Sie konfigurieren? Welche kommerzielle Lösung bei AIT-Schäden?
5	**Compliance & Datenresidenz**	Wo werden Daten verarbeitet und gespeichert? AVV, ISO 27001, SOC 2? EU/EWR-Hosting? Absenderkennungs-Registrierung?
6	**Kanäle & RCS-Bereitschaft**	SMS plus Voice, RCS, WhatsApp, E-Mail? Einheitliche Orchestrierung oder getrennte Werkzeuge? Fallback-Logik konfigurierbar?
7	**Plattform & Integration**	SMPP, HTTP/REST, Webhooks, SDKs. Durchsatz pro Konto. Sandbox. Qualität der Dokumentation.
8	**SLA & Konditionen**	Verfügbarkeits-SLA, Gutschriftenmodell, länderspezifische Preistransparenz, Vertragsflexibilität.
9	**Support-Modell**	24/7/365-NOC? Benannte Kundenbetreuung? Incident-Response-SLA? Sprachabdeckung?

Acht Fragen für jede Ausschreibung

1. Listen Sie Ihre direkten Carrier-Anbindungen vs. Sub-Aggregator-Anbindungen je Land auf.
2. Sind Sie GSMA-OC-zertifizierter SMS-Hub? Wenn nicht: über welchen OC-Hub terminieren Sie?
3. Zeigen Sie Live-Dashboards zur Zustellbarkeit in unseren Zielländern der letzten 90 Tage.
4. Beschreiben Sie Ihre AIT-Erkennungsarchitektur und die Regelung bei AIT-Schäden auf Ihrer Plattform.

5. Für EU-Traffic: Vertragspartner, Hosting-Standort und Ihr Standard-AVV.
6. Wie ist Ihre RCS-Roadmap, welche Netzbetreiber können Sie bedienen und wie funktioniert der SMS-Fallback?
7. Länderspezifische SLAs für Verfügbarkeit, Latenz und Zustellbarkeit, einschließlich Gutschriftenmodell.
8. Beschreiben Sie Ihren 24/7-Support: Wer nimmt Sonntags um 3 Uhr morgens ab, und wie ist die Eskalationskette?

> **IDM und AnyMessage — ehrlich verortet.** Unser Schwerpunkt liegt bei Unternehmen und Netzbetreibern, die **Carrier-grade-Routing, GSMA-OC-Compliance, EU/EWR-Datenresidenz und eine benannte Service-Beziehung** benötigen — wenn diese Eigenschaften wichtiger sind als die Breite tangentialer Kanalintegrationen. Für Einkäufer, deren Hauptanforderung EU-Compliance ist, sind wir eine von mehreren starken Optionen. Für Einkäufer mit wirklich globalen Omnichannel-Bedürfnissen und EU-Compliance als Sekundäranforderung sollten IDM und AnyMessage mit den globalen CPaaS-Anbietern anhand der obigen Kriterien direkt verglichen werden.

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 Ihrem aktuellen Messaging-Betrieb, Ihrer Compliance-Aufstellung oder Ihren Anbietern aufwirft — wir sprechen gerne mit Ihnen, ob ein kommerzielles Gespräch folgt oder nicht. 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