ANYMESSAGE

A2P MESSAGING WHITEPAPER

The Complete A2P SMS Guide 2025

Application-to-person messaging in the EU in 2026 — technology fundamentals, the regulatory and sender-ID landscape, what actually moves deliverability, and the vendor-selection criteria that separate the shortlist from the brochure. Written for enterprise buyers, platform owners and compliance leads.

Initial release 2025

Current revision — April 2026

ABOUT THIS GUIDE

A2P SMS in 2026 — still the workhorse, quietly modernising

A2P SMS is the channel everyone assumes is fading and nobody is actually retiring. Global A2P volumes continue to grow year on year; the channel still anchors OTP, two-factor authentication, service alerts and deterministic fallback across essentially every enterprise messaging stack. What has changed is the sophistication required to operate it well in 2026 — tighter regulation, rising sender-ID discipline, AI-enabled fraud, and the gradual convergence with RCS.

This guide is written for enterprise buyers, digital leaders and compliance officers who need a practitioner-grade reference on A2P SMS without wading through vendor collateral. It covers what the channel is, how it actually works, the EU regulatory surface, what drives deliverability, and the vendor-selection criteria that separate a defensible choice from a cheap one. The 2025 edition reflects two years of enterprise deployments, the maturation of EU sender-ID registers, and the industry shift toward AIT detection and GSMA Trust Framework adoption.

Contents

> **A note on vendor mentions.** This guide is produced by AnyMessage. Where AnyMessage is referenced, we identify the claim clearly. The frameworks presented are useful regardless of the vendor you ultimately select.

CHAPTER 01

A2P SMS in 2026 — why it still matters

Four enduring reasons A2P SMS remains the deterministic foundation of enterprise messaging, even as richer channels claim the headlines. The role of SMS is changing — but not retiring.

U

Universal reach, zero prerequisites

SMS reaches every mobile handset in use — no app install, no account, no data connection required. No other channel has this property. For any message where "the recipient must receive this" is the requirement, SMS remains the only deterministic choice.

O

OTP and authentication still anchor here

Despite security-industry pushes toward authenticator apps and passkeys, SMS OTP remains the highest-volume authentication method in enterprise messaging globally. The channel's universality keeps it in the fallback path for essentially every auth flow.

S

Service alerts and critical notifications

Delivery notifications, appointment reminders, outage alerts, fraud warnings — any content where delivery matters more than richness still defaults to SMS. The economics, reach and operational maturity together make it the lowest-risk choice.

F

The fallback beneath richer channels

Mature omnichannel designs use RCS or WhatsApp where supported and SMS where not. SMS is no longer the primary channel for many use cases — but it is the deterministic fallback that guarantees delivery when primary channels fail. The role has shifted; the channel persists.

THE HONEST FRAMING

A2P SMS in 2026 is not growing because it is glamorous — it is growing because no other channel matches its reach-plus-certainty profile. Expect the channel to keep compounding volume in transactional and authentication categories even as rich channels take the consumer-facing headlines. Plan accordingly.

CHAPTER 02

How A2P SMS actually works

The end-to-end flow, the protocol choices that still matter, and the three operational details that catch out every team doing A2P SMS at enterprise volume for the first time.

The end-to-end flow

Application issues a send request to a messaging gateway. The gateway selects a route — direct carrier connection or an aggregator — based on destination, sender ID, priority and policy. The message transits SS7 signalling infrastructure into the destination operator's SMSC, which delivers it to the handset. A delivery receipt (DLR) is returned along the same path, reporting whether the message was received, failed, or remains pending.

SMPP vs REST — the protocol question

SMPP is the traditional binding for messaging platforms and carriers — persistent TCP, binary protocol, high throughput, full control over segmentation and DLR semantics. REST/HTTP APIs have become the default for application integration: easier to implement, better tooling, sufficient for the vast majority of enterprise volume. A serious platform offers both. Internal platform-to-carrier traffic is still overwhelmingly SMPP; application-to-platform traffic is overwhelmingly REST.

Segmentation, encoding and the 160-character illusion

A single SMS carries 160 GSM-7 characters or 70 UCS-2 (Unicode) characters. Longer messages are segmented into multiple billable SMS with concatenation headers that the handset reassembles. One Unicode character anywhere in a message — an accented letter, a smart quote, an emoji — drops the entire message into UCS-2 mode, cutting capacity by more than half. Enterprises underestimating this end up with surprise bills and truncated content; discipline on content formatting and a clear encoding policy pay immediately.

Delivery receipts (DLRs) — what they actually tell you

A DLR returns one of several states: *DELIVRD* (handset accepted), *UNDELIV* (network couldn't deliver), *EXPIRED* (TTL reached), *REJECTD* (operator or firewall blocked), *UNKNOWN* (no state returned). DLRs are best-effort reporting, not audit-grade truth — some operators are chronically inconsistent about DLR quality, and some routes (particularly grey routes) strip DLRs entirely. A mature platform tracks DLR integrity per route and surfaces this to the enterprise.

> **What this means in practice.** Enterprise teams buying A2P SMS need a platform that handles encoding transparently, reports segmentation and billing clearly, and exposes DLR quality honestly. If your vendor reports 100 % DLR return on every route, they are not distinguishing operator truth from platform-level assumption — and your operational visibility is weaker than the dashboard suggests.

CHAPTER 03

The EU regulatory and sender-ID landscape

A2P SMS in the EU is not a single regulatory regime but a layered one — GDPR first, then ePrivacy, then per-country sender-ID rules that vary substantially. This chapter maps the surface.

GDPR — consent, purpose, retention

Phone numbers are personal data. Processing them for commercial messaging requires lawful basis under GDPR Art. 6 — in practice, consent for marketing and often legitimate interest for transactional messages. Consent must be freely given, specific, informed and unambiguous, and must be recorded so it is demonstrable. Retention limits apply to both the number itself and to the message records; "we kept everything forever" is not a compliant position.

ePrivacy — the messaging-specific layer

The ePrivacy Directive (and its in-progress Regulation successor) layers messaging-specific rules on top of GDPR. Unsolicited commercial SMS to individuals generally requires prior opt-in; the soft-opt-in carve-out for existing customer relationships is real but narrower than vendors often imply, and varies country-by-country. Opt-out must be offered in every commercial SMS and must be honoured within a short timeframe.

Per-country sender-ID registration

Alphanumeric sender IDs in the EU are increasingly regulated at country level. Germany, France, Italy, Spain, the Nordics and several others now operate or are rolling out sender-ID registers; unregistered senders are blocked, replaced with a numeric shortcode, or silently downgraded. A pan-EU A2P deployment requires per-country sender-ID strategy, not a single "EU" registration. Vendors that claim universal EU sender-ID coverage without a country-by-country position are oversimplifying.

What a compliant EU A2P setup looks like

- Consent capture at source, tied to a documented lawful basis per message category.
- Single consent ledger, honoured by every channel, with opt-in / opt-out / re-subscription handling.
- Per-country sender-ID registration for every market served.
- EU-only data processing with a DPA chain terminating at verifiable EU processors.
- Audit trail capturing send decisions, routing and DLR per message.

> **AnyMessage's position.** Our EU compliance posture is architectural: EU-only processing, German-hosted infrastructure, ISO 9001 / 27001 compliance, per-country sender-ID handling as standard. Equivalent postures exist at other EU-first vendors — our baseline, not a differentiator claim.

CHAPTER 04

Deliverability — what actually moves the number

Five levers that actually change A2P SMS deliverability — and three things that sound like levers but rarely are. Focus enterprise effort where the numbers respond.

1 · Direct carrier connectivity vs. aggregation hops

Every hop between sender and destination operator is an opportunity for latency, filtering or DLR loss. Direct carrier connections consistently outperform multi-hop aggregated routes on deliverability, latency and DLR quality. The difference is most pronounced during carrier incidents. For enterprise-grade A2P, direct connectivity on high-volume destinations is not a nice-to-have.

2 · Sender-ID reputation and registration

Operator-side content filtering weighs sender-ID reputation heavily. Unregistered senders, senders that have previously sent flagged content, and senders mis-matched to their content category all see degraded delivery. Proper sender-ID registration in every destination country, combined with content aligned to the registered category, pays back the operational effort in days, not quarters.

3 · Content hygiene

Shortened URLs, links to unverified domains, content with phishing-adjacent patterns, prohibited keywords for specific destinations — all trigger operator-side filtering. A modern platform runs pre-send content screening against destination rules and flags risks before the message hits the operator firewall. This is a larger lever than most enterprises realise.

4 · DLR interpretation, not just DLR counting

Teams reporting "97 % delivered" without distinguishing DLR quality per route are reporting operator trust rather than truth. A mature platform surfaces DLR integrity per-route, flags routes with suspicious DLR patterns, and allows the enterprise to weight reporting accordingly.

5 · Route monitoring and active switching

Carrier performance varies minute to minute. Active monitoring of route performance, with policy-driven switching during incidents, delivers meaningful uplift during the exact moments when messaging matters most — outages, high-volume events, fraud spikes. Static rule-based routing cannot match this.

Things that sound like levers but rarely are

- **"AI-driven send-time optimisation"** — rules based on time zone and opt-in time-of-day perform within 1–2 % of any ML approach in measured deployments.
- **Chasing CPM-lowest routes** — low-cost routing often correlates with lower deliverability and DLR integrity; real cost-per-delivered diverges sharply from cost-per-sent.
- **Vendor-reported delivery percentages on homepages** — without route-level transparency these are marketing, not diagnostics.

CHAPTER 05

Buying A2P SMS — vendor criteria and commercials

The criteria that actually separate the shortlist from the brochure, the commercial patterns worth understanding before contract negotiation, and the honest note on international reach.

The six criteria that matter

1 · Compliance posture

EU-only processing, DPA chain terminating at verifiable EU entities, documented sub-processor position. Disqualifier, not a tiebreaker, for regulated-sector buyers.

2 · Direct connectivity

Direct carrier connections on your primary destinations, with transparent disclosure of the route map. Ask for it in writing during procurement.

3 · Compliance & standards

ISO 9001 and 27001 as baseline; BSI C5 (DE), SOC 2 (international) as differentiators. Request current attestations, not marketing claims.

4 · Sender-ID handling

Per-country sender-ID registration, renewal and monitoring as a managed service, not the enterprise's operational burden.

5 · DLR transparency

Route-level DLR integrity surfaced in the dashboard, with honest flags on routes where DLRs are inconsistent. Opacity here is a red flag.

6 · SLA and incident response

Uptime SLA with service-credit remedies; documented incident response with named contacts; public status history — not a 99.9 % banner.

Commercial patterns worth understanding

A2P SMS pricing is destination-specific; the "€X per SMS" headline rate is always a European or regional average hiding substantial country variation. Look for transparent destination-by-destination rate cards, clarity on minimum commitments, and commercial flexibility as volume changes. Multi-year contracts with price locks are common at enterprise scale. Per-message rebates on quality-of-delivery shortfalls are increasingly available at the mature end of the market.

> **On international reach.** AnyMessage is an EU/DE compliance-first A2P SMS platform. Where enterprises additionally require deep direct-carrier coverage across 200+ countries — typical for global brands, international aggregators and public operators — our sister company *IDM — interactive digital media GmbH* extends the group footprint through one of approximately 40 GSMA Open Connectivity certified hubs. Single contract, EU compliance posture retained, international reach added.

CHAPTER 06

Where A2P SMS is going

Four trends shaping A2P SMS over the next three years — and one thing that is not changing. The direction of travel matters for vendor-selection decisions made in 2026.

1 · RCS convergence — but not replacement

RCS Business Messaging is now established as the natural successor channel for branded transactional content in markets with operator and handset support. The operational pattern that has emerged is RCS-first-with-SMS-fallback, authored from a single template and rendered per channel capability. SMS is not being replaced; it is being pushed into the fallback layer of a richer primary channel. Plan A2P investment with this in mind.

2 · AIT response at platform and carrier level

Artificially inflated traffic (AIT) — traffic generated by fraudulent senders to extract revenue share — has become the industry's largest deliverability-adjacent concern. Both platforms and carriers are deploying ML-based detection, with real measurable impact. For enterprises this primarily shows up as more sophisticated firewall behaviour; for platforms it requires genuine investment in fraud analytics.

3 · GSMA Trust Frameworks and verified senders

GSMA's Trust Framework programme and the broader industry push toward verified sender ecosystems are accelerating. Verified senders see measurable deliverability and engagement uplift; unverified senders will increasingly see operator-side penalties. This is the single most important sender-ID trend to track through 2027.

4 · Data sovereignty pressure on vendor selection

EU data-sovereignty expectations tightened materially through 2024–2025 and are still tightening. Enterprise procurement in regulated sectors increasingly requires EU-only processing and DACH-level sovereignty for public-sector and financial-services deployments. Vendor selection decisions made in 2026 should assume this pressure grows rather than plateaus.

> **WHAT IS NOT CHANGING**
>
> The underlying reason A2P SMS exists — universal, deterministic reach to any mobile handset without prerequisite — is not changing. No competing channel has matched this profile and none is on a realistic path to do so. Expect SMS to keep compounding transactional and authentication volume for the foreseeable future, even as rich channels own the consumer experience layer.

> *"The enterprises buying A2P SMS well in 2026 are not the ones chasing the lowest CPM; they are the ones treating deliverability, compliance and sender-ID discipline as architectural concerns, and treating the vendor relationship as operational rather than transactional."*

— ANYMESSAGE CARRIER OPERATIONS TEAM, 2026

Where AnyMessage fits. AnyMessage operates a German-hosted A2P SMS platform with EU-only processing, direct carrier connections across the EU, and full per-country sender-ID management. For global reach beyond the EU, the AnyMessage/IDM group extends coverage through one of the world's approximately 40 GSMA OC certified hubs. Comparable capability exists at other mature EU-first platforms; the frameworks in this guide apply regardless of your vendor choice.

ABOUT THE PUBLISHER

AnyMessage GmbH

AnyMessage is a German cloud communications provider headquartered in Lübeck. Our platform, the AnyMessage Gateway (AMG), delivers A2P SMS alongside RCS, WhatsApp Business, Voice, Email and Video through a single API, hosted entirely in German data centres and operated under ISO 9001 and ISO 27001 compliance. We serve enterprise clients in banking, insurance, healthcare, public sector, regulated retail and tourism, together with aggregator and carrier partners across the EU.

Since 2024 AnyMessage and *interactive digital media GmbH (IDM)* have operated as a group under United Capital ownership — AnyMessage focused on EU and DACH compliance-sensitive enterprise deployments, IDM focused on global carrier connectivity via one of approximately 40 GSMA Open Connectivity certified hubs. Together the group combines a strong European compliance posture with international reach.

100 %
MADE IN GERMANY
Infrastructure hosted in German Tier 3+ data centres

ISO 9001 / 27001
COMPLIANT
Quality and information-security management

99.9 %
UPTIME
Redundant Tier 3+ infrastructure with SLA backing

6+
CHANNELS · ONE API
SMS, RCS, WhatsApp, Voice, Email, Video

Who we serve

Enterprises across banking, insurance, healthcare, public sector, regulated retail and tourism — organisations for whom GDPR compliance, data residency and auditability are not negotiable. Carrier and aggregator partners across the EU complete our customer base. Because messaging is mission-critical for many of our clients, we name specific references only with prior written consent and on a case-by-case basis — available on request under NDA.

TALK TO US

If this guide raised questions about your A2P SMS vendor set, deliverability posture or EU compliance position, we are happy to have the conversation. Enterprise enquiries: contact@anymessage.cloud. Or call +49 (2173) 26505-0.

ANYMESSAGE

Let's start the conversation

ANY Message. ANY Content. ONE API. ONE APP.

Enterprise enquiries
ANYMESSAGE GMBH
✉ contact@anymessage.cloud
☏ +49 (2173) 26505-0

Partner programme
CARRIERS · AGGREGATORS · RESELLERS
✉ contact@anymessage.cloud
☏ +49 (2173) 26505-0

Online
WEBSITE · DOCS · APP
⌘ www.anymessage.cloud
☏ +49 (2173) 26505-0

Headquarters

AnyMessage GmbH · Moislinger Allee 9D · 23558 Lübeck · Germany
GDPR compliant · Made in Germany · Part of the United Capital group