ANYMESSAGE

COMPLIANCE WHITEPAPER

# GDPR & ePrivacy Compliance Guide

*A practitioner-grade reference on lawful basis, consent, opt-out, data residency and audit for business messaging across A2P SMS, WhatsApp, RCS, email and voice — with the frameworks and checklists EU enterprises actually use in procurement and in annual compliance review.*

**Initial release** 2025

**Current revision** — April 2026

ABOUT THIS GUIDE

# Compliance is an architecture, not a disclaimer

Business messaging in the EU in 2026 sits inside a layered regulatory environment — GDPR as the foundation, ePrivacy as the messaging-specific layer, NIS2 for security obligations on essential and important entities, the AI Act for AI-enabled messaging, and a proliferation of country-level sender-ID and telecoms rules. The enterprises that handle this well treat compliance as an architectural property of their messaging stack, not as a disclaimer added at the end.

Written for compliance officers, DPOs, legal counsel, and the digital-leader role that sits between compliance and delivery. The guide is practitioner-oriented — what the obligations are, how they show up in the messaging stack, and what a defensible setup actually looks like in 2026. Not legal advice; jurisdictional specifics should always be validated with counsel.

## Contents



> **Scope note.** This guide is produced by AnyMessage, a German cloud communications provider. The frameworks are useful regardless of vendor. Specific regulatory conclusions require jurisdictional validation with counsel — we flag this explicitly where relevant rather than in disclaimers.

CHAPTER 01

# The EU regulatory map

*The four regulations that govern business messaging in the EU, plus the country-level layer that sits underneath. Compliance is not GDPR alone — it is the combination, and each one adds real obligations.*

G

### GDPR — the foundation

Phone numbers and message content are personal data. Processing requires lawful basis, purpose limitation, data minimisation, retention limits, and documented data-subject rights handling. Every messaging process operates within GDPR.

P

### ePrivacy — the messaging layer

The ePrivacy Directive (and in-progress Regulation successor) adds messaging-specific rules: prior-consent for unsolicited commercial messages to individuals, opt-out in every commercial message, and tight soft-opt-in exceptions that vary by country.

N

### NIS2 — security obligations

For essential and important entities, NIS2 imposes cybersecurity, incident-response and supply-chain obligations that include messaging infrastructure. If you are in scope, your messaging vendor is too.

A

### EU AI Act — where AI touches messaging

Transparency obligations for AI systems interacting with users (chatbots, assistants), documentation and risk-management obligations for providers and deployers, and stricter rules for high-risk systems.

## The per-country layer

Underneath the EU regulations sit country-level rules — sender-ID registration regimes (DE, FR, IT, ES, Nordics, etc.), national telecoms authorities' guidance on messaging, and — in DACH — sector-specific rules for financial services and public administration. A pan-EU deployment is never a single regulatory conversation; it is a country-by-country one.

> **THE DIRECTION OF TRAVEL**
>
> Every one of these regimes tightened rather than relaxed through 2023–2026. Expect further tightening through 2027+: ePrivacy Regulation adoption, AI Act phased enforcement, NIS2 member-state implementation maturity. Compliance work is not a project; it is a standing operational capability.

CHAPTER 02

# Lawful basis for messaging

*Every messaging process needs a documented lawful basis under GDPR Art. 6. The three that matter for messaging, how to pick correctly, and the soft-opt-in rule that causes more compliance incidents than any other single provision.*

## 1 · Consent — the default for marketing

For marketing messaging, consent is almost always the lawful basis. Consent must be freely given, specific, informed and unambiguous — pre-ticked boxes, bundled consent, or consent as a condition of service do not qualify. Consent must be recorded so it is demonstrable, and must be revocable as easily as it was given.

## 2 · Legitimate interest — for certain transactional contexts

Legitimate interest can lawfully underpin transactional messaging where the processing is necessary for a legitimate purpose, cannot reasonably be achieved less intrusively, and does not override the data subject's rights. Appropriate for delivery notifications, service alerts and outage communications to existing customers; not appropriate for marketing. Requires a documented legitimate-interests assessment (LIA).

## 3 · Contractual necessity — for narrow cases

Where messaging is strictly necessary to perform a contract with the data subject — for example, sending an OTP to authenticate a login the data subject initiated — contractual necessity can apply. Narrower than it looks; "we decided this was necessary" is not the same as "this is strictly necessary to perform the contract".

## The soft-opt-in caveat

The "soft opt-in" allows existing-customer marketing messaging in some EU jurisdictions without fresh consent, subject to strict conditions — contact details obtained in course of a sale, the marketing is for similar products, and opt-out was clearly offered at the point of capture and in every message. The scope varies by country; in some jurisdictions it barely applies, in others it supports substantial marketing programmes. Validate with counsel per market; do not assume universal availability.

> **The operational pattern that works.** Document the lawful basis per message category at design time, not per-message at send time. Transactional messages: legitimate interest or contractual necessity with documented rationale. Marketing: consent, with per-channel opt-in where required. Authentication: contractual necessity. Review the catalogue annually.

CHAPTER 03

# Consent & opt-out as platform primitives

*Consent and opt-out are where fragmented messaging estates accumulate compliance debt fastest. This chapter describes what "consent as a platform primitive" actually means — and why it is architectural rather than operational.*

## One consent record per contact, honoured everywhere

A single contact should have a single consent record, with separate flags per channel and per message category as needed. When a customer opts out — via SMS STOP, a reply on WhatsApp, a click on an email unsubscribe link, or a customer-portal setting — that opt-out must propagate to every channel within a defined, short timeframe. Fragmented consent, where a WhatsApp opt-out doesn't affect SMS sends, is a regulatory exposure.

## The consent state machine

Consent has a lifecycle: *captured* (with timestamp, source, lawful basis, scope), *active*, *revoked* (with timestamp), and *expired* (per retention policy). A production-grade platform models this explicitly — consent state is queryable at send time, every state change is logged, and the message-send pipeline consults the state before routing. "The platform must enforce consent" is the statement; a documented state machine is the implementation.

## Opt-out integrity — the only acceptable target is zero

Messages sent to opted-out contacts are the category of compliance incident regulators take most seriously and customers complain about most loudly. The operational target is zero — not "very low", not "single digits", zero. Achieving this requires opt-out propagation in near-real time across every channel, every destination, every sub-processor, with an audit trail. An opt-out that takes 24 hours to propagate is an opt-out that sent unwanted messages for 24 hours.

## Why this can't live in a spreadsheet

Spreadsheet-based or application-code-based consent management fails operationally (race conditions, stale state, manual handoffs) and legally (no defensible audit, unclear retention, no demonstrable enforcement). In 2026, any compliance-serious enterprise expects its messaging platform to own consent as infrastructure — not as a feature the application layer implements.

> **CONSENT ARCHITECTURE CHECKLIST**
>
> Single consent record per contact · channel flags where needed · opt-in / opt-out / revoked / expired state machine · near-real-time opt-out propagation · immutable audit trail · documented retention policy · queryable at send time · demonstrable on supervisory-authority request.

CHAPTER 04

# Data residency & the DPA chain

*Where your data is processed, by whom, and under what contractual framework — the first question compliance officers ask and the most common reason non-EU vendors exit the regulated-sector shortlist.*

## EU-only is the baseline for regulated sectors

For regulated-sector deployments — banking, insurance, healthcare, public sector — the baseline expectation in 2026 is EU-only processing. The Schrems II ruling invalidated Privacy Shield; standard contractual clauses with supplementary measures remain legally complicated; and the practical compliance-officer position is increasingly "keep the data in the EU". "EU region available" is not the same as "EU-only by architecture"; regulated buyers increasingly require the latter.

## The DPA chain and sub-processor transparency

A data-processing agreement (DPA) between the enterprise (controller) and the messaging vendor (processor) sets out the scope, purpose, duration and security of processing. Where the vendor uses sub-processors — carriers, channel providers, infrastructure providers — those sub-processors must be listed, their locations documented, and material changes notified in advance. An opaque sub-processor position is a red flag in procurement review.

## The DACH-specific posture

In Germany and the DACH region, the compliance expectation tightens further. German public-sector and financial-services procurement increasingly requires German hosting, explicit "Made in Germany" operation, and often BSI C5 conformance. The label is not marketing; it is a documentable infrastructure claim that procurement validates. A vendor whose "German operations" reduce to a German sales entity does not meet this bar.

## What a defensible setup looks like

- EU-only processing with DPA terminating at verifiable EU processors.
- Sub-processor list published and kept current; material changes notified in advance.
- German hosting for DACH-focused deployments where sector requires.
- Infrastructure compliance (ISO 27001 baseline; BSI C5 for German public sector / financial services).
- Documented operational procedures for data-subject rights, breach notification, and international-transfer safeguards where needed.

CHAPTER 05

# Per-channel specifics

*The regulatory surface differs materially by channel. The compliance analysis is per-channel, not global. This chapter maps the notable differences.*

## SMS (A2P)

Consent and opt-out under GDPR + ePrivacy. Per-country sender-ID registration increasingly mandatory in the EU — Germany, France, Italy, Spain, Nordics and several others operate sender-ID registers. STOP must be honoured across the contact, not just on the source number. Message content should be retained proportionately; indefinite retention is not compliant.

## WhatsApp Business

In addition to GDPR + ePrivacy, WhatsApp introduces Meta as a processor — the DPA analysis must cover Meta's role, data flows to Meta infrastructure, and the template-approval and categorisation scheme. The 24-hour session window has practical consent implications. Template categories (authentication, utility, marketing) carry different consent expectations.

## RCS Business Messaging

Governed by GDPR + ePrivacy; verified-sender registration is an operator-led process. Rich media and suggested-reply payloads enlarge the content surface for compliance screening. Where RCS is integrated through Google's RBM or operator-hosted RCS, data-flow documentation includes the operator / Google as relevant.

## Email

Compliance surface is distinct — double opt-in expectation (country-variable), unsubscribe-header compliance (RFC 8058), sender authentication via SPF, DKIM, DMARC and BIMI. CAN-SPAM is irrelevant in the EU; the ePrivacy regime governs.

## Voice and Video

Voice OTP falls under messaging regulation; recorded calls introduce recording-retention and consent-to-record obligations. Video consultations — increasingly used in banking, insurance and healthcare — almost always require a DPIA, documented recording-retention policy, and explicit consent handling.

> **AnyMessage's posture.** Our platform normalises consent, opt-out and audit across every channel with a single consent ledger and a unified audit trail. Per-channel mechanics differ; the compliance surface the customer interacts with does not.

CHAPTER 06

# Audit, DPIA & the annual review

*What a defensible audit trail looks like, when a DPIA is required, and the annual review cadence that mature enterprises now operate on their messaging stack. The compliance work that separates "we think we're compliant" from "we can demonstrate it".*

## The audit trail — what it must contain

- Every send request with timestamp, lawful basis, consent state at time of send, template identifier.
- Routing decision, channel adapter translation, carrier route chosen, and why.
- Delivery receipt from carrier with timestamp and disposition.
- Every consent state change with source, timestamp, scope.
- Template approvals, content-screening decisions, compliance flags.
- Access log — who viewed what, when.

## When a DPIA is required

A Data Protection Impact Assessment is required under GDPR Art. 35 where processing is likely to result in a high risk to the rights and freedoms of natural persons. For messaging, that typically means: systematic monitoring on a large scale, special-category data (health, political opinion, etc.), AI-driven decision-making affecting users, video consultations, or any processing a national supervisory authority has listed as DPIA-required. When in doubt, do one — the cost is modest; the cost of not doing one when required is not.

## The annual review cadence

Mature enterprises review their messaging compliance posture annually as standard — lawful-basis catalogue, consent-ledger integrity, opt-out incident history, DPA currency, sub-processor list verification, certification refresh, and DPIA update where material changes have occurred. The review produces a documented output, not just an email. Supervisory authorities see this as evidence of genuine accountability; its absence as evidence of the opposite.

## The drills that matter

- **Audit reconstruction.** Pick a random message sent 6 months ago; reconstruct its full journey. If this takes more than a few hours, your audit trail is weaker than you think.
- **Opt-out propagation.** Submit a STOP; measure propagation to every channel. Target: minutes.
- **Data-subject request.** Rehearse the full response to a DSAR or erasure request involving messaging data. Measure time to complete.

> *"Messaging compliance in 2026 is not a disclaimer you add to the footer — it is a property of the architecture you buy, the audit trail you operate, and the annual review you actually do. The enterprises that get this right compound defensibility quietly over years."*

**— ANYMESSAGE COMPLIANCE TEAM, 2026**

**Where AnyMessage fits.** Our EU compliance posture is architectural — EU-only processing, German-hosted infrastructure, consent as a platform primitive, unified audit trail across every channel, ISO 9001 / ISO 27001 compliance. Equivalent capability exists at other mature EU-first platforms; the frameworks in this guide apply regardless of vendor. Where you do need a vendor with a defensibly German posture, we are happy to have the conversation.

ABOUT THE PUBLISHER

# AnyMessage GmbH

AnyMessage is a German cloud communications provider headquartered in Lübeck. The AnyMessage Gateway (AMG) delivers SMS, RCS, WhatsApp Business, Voice, Email and Video through a single API, hosted entirely in German data centres and operating in line with ISO 9001 and ISO 27001. 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**
Tier 3+ German data centres

**ISO 9001 / 27001**
**COMPLIANT**
Quality and info-security management

**99.9 %**
**UPTIME**
SLA with service-credit remedies

**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. Specific references available on request under NDA.

**TALK TO US**

If this guide raised questions about your messaging compliance posture, DPA chain or audit readiness, 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