interactive digital media

COMPLIANCE WHITEPAPER

GDPR & ePrivacy for Business Messaging

Legally compliant A2P messaging in the EU — the two-law framework, the lawful bases that actually work for SMS, what national regulators enforce in practice, and a practical compliance baseline you can ship.

First edition published 2024

Current revision — February 2026

ABOUT THIS GUIDE

Compliance, without the legalese

First released in 2024 and refreshed for 2026, this guide is written for the people who actually have to implement GDPR- and ePrivacy-compliant business messaging: marketing and CRM leaders, data protection officers, legal counsel, and the engineers who build the opt-in flows. It is not a law review — it is a practical reference that explains what the rules mean when you apply them to an SMS, RCS or WhatsApp Business programme.

The 2026 revision reflects two years of further national enforcement, the continued delay of the ePrivacy Regulation, and the growing importance of sub-processor and data-residency requirements in EU enterprise RFPs.

Contents

01 **Why compliance is mission-critical**
Stakes, recent enforcement, and the business case for getting it right

02 **The two-law framework**
GDPR and ePrivacy — how they interact, and why both apply

03 **Legal bases & consent that works**
Article 6 bases, Article 7 conditions, soft opt-in, documentation

04 **National variations that bite**
Germany, France, Italy, Spain, UK — where enforcement lives

05 **Practical compliance baseline**
A checklist, DPA essentials, and what to automate in your platform

06 **Vendor & processor selection**
Data residency, sub-processors, and EU-first messaging infrastructure

IMPORTANT — NOT LEGAL ADVICE

This guide summarises EU regulation and Member State implementations as a practical reference. It is **not legal advice** and should not be relied upon as a substitute for qualified counsel in your jurisdiction. Regulatory interpretation evolves, Member State rules differ, and case-by-case facts matter. Consult your DPO and external counsel before making material changes to your messaging compliance posture.

CHAPTER 01

Why compliance is mission-critical

The stakes, recent enforcement patterns, and why EU messaging compliance stopped being a "nice-to-have" legal item sometime around 2023.

The cost of getting it wrong

GDPR enforcement matured quickly. In the first years after the regulation came into force in 2018, regulators were publishing guidance, building case law, and issuing mostly modest fines. By 2023–2025 that had reversed: the EDPB reported **cumulative GDPR fines exceeding €5.6 billion** across Member States, with individual decisions regularly entering eight- and nine-figure territory. Messaging programmes are not usually the target of the headline fines — those are reserved for big-tech data-transfer and advertising cases — but SMS, email and WhatsApp marketing programmes sit squarely in the enforcement zone below that headline tier, where regulators act routinely and quickly.

€20M	€300k	€5.6B+	72h
OR 4% OF TURNOVER	**GERMANY (UWG §7)**	**CUMULATIVE FINES**	**BREACH WINDOW**
GDPR maximum fine, whichever higher	per-violation administrative fine	across EU Member States since 2018	to notify the supervisory authority

Where enforcement actually lands for messaging

Four patterns recur across national enforcement actions specifically touching SMS, email and messenger-based marketing programmes:

- **No valid consent.** Pre-ticked boxes, consent bundled with terms and conditions, opt-ins obtained for a different purpose and re-used for marketing. The single most common finding.
- **Inadequate opt-out.** Stop keywords that take days to honour, opt-outs that unsubscribe from one channel but not the programme, no easy way to withdraw consent that is "as easy as it was to give it" (GDPR Art. 7(3)).
- **Missing information to the data subject.** Article 13 and 14 notices that never reach the recipient, or that reach them in language they cannot reasonably be expected to understand.
- **International transfer without safeguards.** Messaging data processed by sub-processors outside the EU/EEA without adequate transfer mechanisms — an issue that grew sharply post-Schrems II and remains actively enforced.

THE BUSINESS CASE BEYOND FINES

Financial penalties get the press attention, but three indirect costs matter more for most enterprises: (1) remediation — rebuilding consent from a cleaned database is painful and expensive; (2) channel suspension — supervisory authorities can and do order temporary suspension of marketing activities; (3) reputational damage — a public decision naming your company on a regulator's website lives online permanently.

CHAPTER 02

The two-law framework

GDPR and ePrivacy both apply to business messaging — how they interact, which takes precedence when they seem to conflict, and what the stalled ePrivacy Regulation changes in practice.

EU business messaging compliance rests on two overlapping instruments, not one. The **General Data Protection Regulation (GDPR, Regulation 2016/679)** governs any processing of personal data — and a mobile phone number tied to an identifiable person is personal data. The **ePrivacy Directive (2002/58/EC, as amended by 2009/136/EC)** governs electronic communications specifically, including the rules for unsolicited direct marketing by SMS, email and messenger channels. Both apply simultaneously; neither displaces the other.

How the two interact in practice

The ePrivacy Directive is *lex specialis* — the specific rule that prevails where it addresses a topic (such as the consent requirement for unsolicited SMS marketing under Article 13). Where ePrivacy is silent, GDPR fills the gap — for example on the rights of the data subject, the obligations of the controller, the role of the processor, international transfers, and documentation. In practice, a compliant messaging programme has to satisfy *both*: ePrivacy for the conditions under which the message can be sent at all, and GDPR for everything surrounding the message.

The pending ePrivacy Regulation

The ePrivacy Regulation — intended to replace the 2002 Directive and to align fully with GDPR — has been in political negotiation since 2017. As of early 2026 it remains in trilogue and has no confirmed adoption date. For practical purposes, the current Directive (as implemented into national law by each Member State) is still the binding instrument, and enterprises should plan on it remaining so for at least the duration of current multi-year contracts.

National implementations matter more than the directives

Because ePrivacy is a Directive rather than a Regulation, its rules apply only through national implementation. This is why the same SMS marketing programme can be clearly compliant in one Member State and clearly

non-compliant in another, even though both are "following ePrivacy." The national variations are not trivia — they are where enforcement actually happens. Chapter 4 covers the five jurisdictions that generate the most enforcement volume relevant to business messaging.

> **Why EU-hosted infrastructure matters here.** Because GDPR and ePrivacy both apply to the full message lifecycle — including the processing performed by your messaging vendor and their sub-processors — the location and legal jurisdiction of your messaging infrastructure is itself a compliance question. IDM's infrastructure is hosted entirely in Germany; our sister company **AnyMessage** operates on the same EU-resident footing. For enterprises whose DPO has drawn a red line around EU data residency for messaging, the two of us together represent one of the shortest shortlists in the market. Several other strong EU-based providers exist — this is disclosure, not a claim of uniqueness.

CHAPTER 03

Legal bases & consent that works

Which Article 6 lawful basis applies to which type of message, what Article 7 requires from a consent to actually be valid, and the soft opt-in rule that most enterprises misinterpret.

Choosing the right lawful basis

GDPR Article 6(1) lists six possible lawful bases for processing personal data. For business messaging, three of them carry essentially all the traffic: consent, contractual necessity, and legitimate interest. Choosing the right one per use case is the foundation on which the rest of a compliant programme is built.

USE CASE	TYPICAL BASIS	WHY, AND WHAT TO WATCH
OTP / 2FA	Contract (Art. 6(1)(b))	Delivery of the service the user requested. Not marketing. Consent is not normally needed.
Delivery / service notifications	Contract or legitimate interest	"Your order has shipped" messages are transactional. Watch the line where transactional tips into cross-sell.
Appointment reminders	Legitimate interest (Art. 6(1)(f))	Usually sustainable where the service was requested and the reminder reduces no-shows. Document the balancing test.

USE CASE	TYPICAL BASIS	WHY, AND WHAT TO WATCH
Direct marketing	Consent (Art. 6(1)(a)) + ePrivacy Art. 13	Prior, specific, informed, unambiguous consent required — or strict soft opt-in for existing customers.
Surveys / research	Legitimate interest or consent	Depends on whether participation is incentivised and whether the survey is genuinely separable from marketing.

What Article 7 requires from a valid consent

Where consent is the chosen basis, it must meet the four cumulative conditions of Article 4(11) and Article 7: **freely given**, **specific**, **informed**, and expressed by a **clear affirmative action**. Silence, pre-ticked boxes and inactivity do not count. Consent must also be **demonstrable** (Art. 7(1)) — meaning you must be able to show, for any given phone number, who gave consent, when, through what mechanism, and for what purpose. And withdrawal must be "as easy as giving consent" (Art. 7(3)) — a one-word STOP reply is the de-facto standard for SMS.

Double opt-in — strongly recommended

Although GDPR does not explicitly mandate double opt-in, German case law treats it as the de-facto standard of evidence. The pattern — collect phone number, send an SMS asking for confirmation, treat the subscriber as opted in only once they respond affirmatively — produces a contemporaneous audit trail that is very hard to challenge. For any EU programme at meaningful volume, it is the path of least regulatory risk.

The soft opt-in rule — precisely

ePrivacy Article 13(2) allows direct marketing by SMS or email to existing customers, for the marketer's *own similar products or services*, without fresh explicit consent, provided the customer was given a clear opportunity to object both at the time their contact details were collected and in every subsequent message. This "soft opt-in" exception is narrower than most enterprises assume. Three common failures:

- **"Similar" is interpreted narrowly** — a bank cannot rely on soft opt-in to market unrelated insurance products to mortgage customers.
- **"Existing customer" requires a real prior relationship** — someone who downloaded a whitepaper is not a customer.
- **The opt-out must be active in every message** — not just available somewhere in the privacy policy.

CHAPTER 04

National variations that bite

The five Member State regimes that produce most of the messaging-related enforcement volume — and the specific traps in each that are worth knowing before your next campaign.

DE

Germany — UWG §7 and BDSG

The strictest consumer-protection regime in the EU for unsolicited commercial communication. Administrative fines up to €300,000 per violation under UWG §7. Double opt-in is effectively mandatory in case law. BfDI and Länder DPAs both enforce.

FR

France — CNIL

CNIL requires explicit opt-in and a clear opt-out keyword (STOP au XXXXX) in every commercial SMS. Sanctions under the Loi Informatique et Libertés (LIL, national GDPR-implementing law) can reach the GDPR maximum. CNIL is one of the most active regulators in Europe on marketing SMS.

IT

Italy — Garante

Particularly active on telemarketing and SMS marketing. Has issued seven-figure fines repeatedly. Enforcement focuses on opt-in provenance (who actually gave consent) and use of third-party lead databases. Italian law also layers on specific rules for political and public-sector messaging.

ES

Spain — AEPD and LSSI

Spain's AEPD is the highest-volume fining authority in the EU by decision count. LSSI (Ley de Servicios de la Sociedad de la Información) layers specific rules on commercial electronic communications on top of GDPR. Fines for unsolicited SMS commonly land in the six-figure range.

UK

United Kingdom — PECR & ICO

Post-Brexit but substantially aligned. PECR (2003, as amended) mirrors ePrivacy. UK GDPR mirrors GDPR. The ICO actively enforces against unsolicited SMS campaigns with fines under PECR up to £500,000 (rising to GDPR-level where PECR and UK GDPR both apply).

EU

EDPB & one-stop-shop

For enterprises operating across multiple Member States, the GDPR one-stop-shop mechanism designates a lead supervisory authority — usually in the Member State of your main establishment. But ePrivacy is not subject to the one-stop-shop: every national regulator can act on ePrivacy breaches independently.

For DACH enterprises specifically. Germany's combination of UWG §7, BDSG, and strong case-law requirements around double opt-in produces the tightest practical compliance environment in the EU. IDM is a German GmbH headquartered in Lübeck; AnyMessage operates within the same corporate group. For German-headquartered enterprises and DACH-regional operations, contracting with a provider under the same jurisdiction (and under a straightforward BDSG §28-style Auftragsverarbeitungsvertrag) removes an entire class of transfer and sub-processor questions from a DPO's review. Other EU-based providers offer comparable arrangements; we are not the only option.

CHAPTER 05

Practical compliance baseline

A working checklist, a summary of what an Auftragsverarbeitungsvertrag (DPA) actually needs to cover, and what to automate in your messaging platform rather than leave to humans.

The compliance checklist

The following baseline is derived from current EDPB guidance, active national enforcement patterns and German case-law standards. Meeting it does not guarantee compliance — facts matter — but failing any of these items is a reliable way to fail a regulator's audit.

- ✓ **Documented opt-in per number** — source, timestamp, exact consent wording shown, IP address where collected online, and the specific purpose consented to.
- ✓ **Double opt-in for marketing in DE/AT/CH** — and strongly recommended everywhere else in the EU.
- ✓ **Honoured opt-outs within one message cycle** — STOP, STOPP, ARRÊT, PARE, CANCELAR and other local equivalents, depending on markets.
- ✓ **Article 13/14 information provided** at the point of data collection — controller identity, purposes, legal basis, retention period, data subject rights, right to complain to a supervisory authority.
- ✓ **Time-of-day restrictions enforced** per destination country at platform level, not left to individual campaign managers.
- ✓ **Processor agreement (DPA) in place** with every messaging vendor, covering GDPR Article 28 requirements — see below.
- ✓ **Sub-processor transparency** — a current, accessible list of sub-processors with notification of changes.

- ✓ **Transfer mechanism in place** for any data flows outside the EU/EEA — SCCs, adequacy decision, or BCRs, with a transfer impact assessment (TIA) on file.
- ✓ **Retention schedule defined** and automated — messaging metadata and DLRs retained only for documented legitimate purposes and defined periods.
- ✓ **72-hour breach notification process** tested and owned by a named individual.

What the DPA must cover

Every processor agreement must address all of GDPR Article 28(3) — the processor's obligations on processing only on documented instructions, staff confidentiality, security measures, sub-processors, data subject rights support, breach notification support, DPIA support, return or deletion of data on termination, and audit rights. In practice, most enterprise DPAs go further: specifying locations of processing (data residency), encryption standards in transit and at rest, incident-response SLAs, and liability allocation.

> **WHAT TO AUTOMATE, NOT LEAVE TO HUMANS**
>
> A modern messaging platform should enforce opt-in provenance (blocking sends to unconsented numbers), opt-out honouring (STOP handling within the same message cycle), time-of-day rules per country, and retention schedules — without a human having to remember. If your current vendor relies on you to enforce these at the campaign-configuration level, that is a gap worth closing before your next audit.

CHAPTER 06

Vendor & processor selection

The compliance-specific criteria for choosing a messaging vendor when EU data protection is a first-order requirement rather than a checkbox.

Most messaging vendor RFPs are won on coverage, deliverability and price. For enterprises where EU compliance is a non-negotiable requirement — banks, healthcare, public sector, and increasingly any consumer brand with significant EU operations — four additional criteria deserve weight proportional to the regulatory exposure.

#	CRITERION	WHAT TO PROBE IN THE RFP
1	**Contracting entity & jurisdiction**	

#	CRITERION	WHAT TO PROBE IN THE RFP
		Which legal entity will you contract with, and under which Member State's jurisdiction? An EU entity materially simplifies DPA negotiation and reduces transfer questions.
2	**Processing locations**	Where is personal data processed, stored, and backed up? EU-only? EU + named third countries? Which sub-processors and where?
3	**DPA & Article 28 coverage**	Provide the standard DPA. Confirm alignment with Art. 28(3), SCCs where relevant, audit rights, and breach-notification SLA.
4	**Sub-processor governance**	Current list of sub-processors, change-notification mechanism, and objection rights. Carrier partners and hubs count as sub-processors.
5	**Security certifications**	ISO 27001 minimum; SOC 2 Type II a plus; infrastructure hosted in accredited data centres with documented physical and logical controls.
6	**Platform-enforced controls**	Can the platform automatically enforce opt-out honouring, time-of-day restrictions, and retention schedules at country/campaign level?

Where IDM and AnyMessage fit. GDPR and ePrivacy compliance is the area of the messaging market where our positioning is most distinctive. IDM is a German GmbH with all infrastructure hosted in Germany. AnyMessage operates on the same EU-resident basis under the same group umbrella. Our DPAs are drafted against Article 28(3) and BDSG §28 and we are comfortable with audit rights, sub-processor transparency and incident-response SLAs that enterprise DPOs expect. For enterprises whose primary requirement is EU compliance, we are one of the natural shortlist candidates. For enterprises whose primary need is global omnichannel breadth with EU compliance as a secondary constraint, we should be compared against the global CPaaS players using the criteria above.

ABOUT THE PUBLISHER

interactive digital media GmbH

IDM is a German cloud communication service provider founded in 2003 and headquartered in Lübeck. Our proprietary **IMT-HUB®** platform, now in its fourth generation, is one of approximately 40 GSMA Open Connectivity (OC) certified SMS hubs worldwide. We serve enterprises, mobile operators and service providers across every major industry, with infrastructure hosted entirely in Germany. Since 2024, IDM has been part of the **United Capital / AnyMessage group**; our sister company AnyMessage operates complementary messaging infrastructure, and together we represent a European messaging group with particular strength in regulated, compliance-sensitive deployments.

20+	200+	1,000+	~40
YEARS	**COUNTRIES**	**OPERATORS**	**GSMA OC HUBS**
of operating experience	reachable on our network	directly or via OC	IDM is one of them

Who we serve

IDM serves enterprise clients across banking, automotive, healthcare, research, retail, tourism and the public sector, together with carrier partners across the EU, GCC and international hub networks. 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 current compliance posture, your DPAs, or your vendor set — we are happy to talk, whether or not a commercial conversation ever follows. Enterprise enquiries: **sales@i-digital-m.com**. Carriers, aggregators and resellers: **partners@i-digital-m.com**. Or call **+49 (0)451 31 70 21-0**.

Let's start the conversation

Excellence in Cloud Communication Services

Sales & general enquiries

INTERACTIVE DIGITAL MEDIA GMBH

✉ sales@i-digital-m.com

☏ +49 (0)451 31 70 21-0

Partner Program

CARRIERS · AGGREGATORS · RESELLERS

✉ partners@i-digital-m.com

☏ +49 (0)451 31 70 21-0

Online

WEBSITE & CUSTOMER PORTAL

🌐 www.i-digital-m.com

☏ +49 (0)451 31 70 21-0

Headquarters

interactive digital media GmbH · Moislinger Allee 9d · 23558 Lübeck · Germany

Presences in London (UK) and New Delhi (IN) · Part of the United Capital / AnyMessage group