

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in the United Kingdom

COUNTRY **United Kingdom**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **16 October 2026**

KEY REGULATORS **Ofcom · Information Commissioner's Office · Home Office**

Key takeaways

- No telecoms licence is needed to sell mobile, SIM or eSIM services in the UK. Every provider is automatically bound by Ofcom's General Conditions of Entitlement, the rulebook that Ofcom can enforce with fines of up to 10% of turnover.
 - Telecoms firms are not covered by the UK anti-money laundering (AML) rules, and the UK has no law requiring identity checks before a SIM or eSIM is sold. Prepaid (pay-as-you-go) SIMs can still be activated without an ID document, online or in a shop.
 - Identity rules are arriving through fraud law instead. From 18 January 2027 mobile operators must cap how many texts each pay-as-you-go SIM can send, and from 15 July 2027 anyone carrying business text messages must run "Know Your Customer" checks on the businesses sending them.
 - Online and in-store sales follow the same rules, but switching provider is built for digital channels: customers must be able to request a switching code by text, phone or online account, and receive it within one minute.
 - Possessing or supplying a "SIM farm" (a device using five or more SIM cards to send calls or texts) without a good reason becomes a criminal offence on 29 October 2026, and suppliers must check and record who they sell to.
-

The UK market is open to mobile network operators, mobile virtual network operators (MVNOs), eSIM-only brands and business messaging platforms under a general authorisation regime: a provider starts trading and the General Conditions apply from day one. Ofcom regulates the sector UK-wide, the Information Commissioner's Office (ICO) supervises personal data and the Privacy and Electronic Communications Regulations, and the Home Office leads on telecoms fraud, including the new SIM farm offences.

The biggest change for a new entrant in 2026 and 2027 is the shift of scam prevention from voluntary practice to binding rules. General Condition C9 makes mobile operators and messaging aggregators responsible for limiting pay-as-you-go messaging, blocking scam numbers and verifying every business that sends bulk texts, while Ofcom is already investigating providers whose numbers were used by scammers.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Telecommunications regulation is UK-wide: the same General Conditions apply in England, Wales, Scotland and Northern Ireland. The criminal penalties for SIM farm offences are the main point where the rules differ by nation (see section 9).

Regulator	Remit for telecom and mobile services	Level	Official site
Ofcom	General Conditions of Entitlement, numbering, switching and porting, scam call and text rules, network security enforcement, Online Safety Act for online messaging apps	UK-wide	ofcom.org.uk
Information Commissioner's Office	UK GDPR, Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, including biometric data used in onboarding	UK-wide	ico.org.uk
Department for Science, Innovation and Technology	Telecoms policy, the Telecommunications Security Code of Practice, the digital verification services trust framework	UK-wide	gov.uk/dsit
Home Office	Fraud strategy, Fraud Sector Charter for telecoms, SIM farm offences under the Crime and Policing Act 2026	UK-wide (penalties vary by nation)	gov.uk/home-office

2 Licensing and authorisation

The UK does not license telecoms operators individually. The General Conditions of Entitlement replaced the former licensing regime in 2003 and are the regulatory conditions every provider of electronic communications networks and services must meet to provide services in the UK ([Ofcom, General Conditions of Entitlement](#)). They cannot be imposed on a single named provider; each condition defines which category of provider it binds, for example condition C8 applies only to mobile service providers. The current unofficial consolidated version took effect on 8 April 2026.

Three permissions sit alongside the General Conditions. Telephone numbers are allocated by Ofcom, and a range holder must make sure numbers it passes to customers are used effectively and efficiently under condition B1. Using certain radio equipment requires a separate Ofcom licence. Charges for digital content, voice-based services, tickets or charity donations billed to a phone account fall outside the Payment Services Regulations 2017 only while a single transaction stays at or below £40 and a subscriber's monthly total at or below £240 ([Schedule 1, Part 2, paragraph 2\(I\)](#)); above those limits, payment services authorisation rules apply.

Large and medium-sized public telecoms providers must also meet the security duties of the Communications Act 2003 as amended by the Telecommunications (Security) Act 2021. Version 1.1 of the [Telecommunications Security Code of Practice](#) **In force** was issued on 14 July 2026; it applies tiered expectations to Tier 1 and Tier 2 providers and does not expect Tier 3 providers to follow its measures.

3 Identity framework (AML rules do not apply)

Telecoms providers are not "relevant persons" under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, which cover credit and financial institutions, auditors, legal and trust service providers, estate and letting agents, high value dealers, casinos, art market participants and cryptoasset businesses. The amendments made by the [Money Laundering and Terrorist Financing \(Amendment\) Regulations 2026](#) did not add telecoms. There is therefore no customer due

diligence, beneficial ownership or suspicious activity reporting regime specific to the sector.

Nor does UK law require subscriber registration. Ofcom records that operators typically apply lighter credit and identity checks to pay-as-you-go SIMs than to pay-monthly contracts, and that scammers acquire SIMs by buying them in-store or using stolen cards ([Ofcom statement, Combatting mobile messaging scams, 15 July 2026, paragraph 2.24](#)).

What governs identity instead is a set of fraud-driven obligations:

Business customers holding numbers

Under conditions B1.6, B1.8 and B1.9 Ofcom expects providers to run know-your-customer checks on business customers before transferring numbers to them, monitor for misuse and act on reports.

Business text senders

Condition C9

Adopted, effective 15 Jul 2027

requires KYC and know-your-traffic checks on every business that sends application-to-person (A2P) messages.

Account changes

Condition C7 requires authentication before switching codes are issued; the Fraud Sector Charter commits major networks to two-factor authentication before account transfers.

Device suppliers

From 29 October 2026, anyone supplying a SIM farm must verify the recipient's good reason and keep a record of the supply.

4

Identity verification and onboarding

No UK rule prescribes accepted identity documents, a verification method or an identity assurance level for consumer mobile customers. Providers set their own checks, usually tighter for pay-monthly contracts than for prepaid SIMs. As a voluntary benchmark, providers can use "How to check someone's identity (1.0)", the version of Good Practice Guide 45 published on 9 June 2026 under the digital verification services trust framework ([Office for Digital Identities and Attributes](#)).

The most detailed verification standard in the sector applies to business customers. For A2P messaging, KYC under condition C9.10 must, at a minimum, collect and assess trading or registered names, registered or trading address, the nature of the service, payment or bank account information, existing telephone numbers and websites, directors and persons with significant control, and contact details of a senior individual who authorises the messages. Information must be corroborated against public sources, risk-assessed,

and enhanced checks (Companies House, Cifas, the FCA register, Ofcom sanctions) carried out where indicators appear ([Ofcom guidance, Scam mobile messages, paragraphs 2.89 to 2.95](#)). Providers that do not onboard the sender themselves may rely on a downstream party, but only through clear contractual terms they monitor and enforce (condition C9.9).

Biometric checks such as selfie matching are permitted but are special category data processing; the ICO’s position is set out in section 6.



Figure 1. Online SIM and eSIM onboarding and high-risk account requests for a UK mobile provider.

Bottom line: the rules are largely channel-neutral, but switching is designed around remote channels, and the new scam-prevention rules treat online signals (IP address, VPN use, sign-up timing) as risk indicators for business customers onboarded online.

Requirement	In person / retail	Online / remote	Difference
Statutory identity check at SIM sale	None	None	Same
Pay-as-you-go messaging volume limits (from 18 Jan 2027)	Physical SIMs	eSIMs and SIMs bought online	Same
Requesting a switching code (PAC or STAC)	Not a required route	Text, phone and online account routes required; code within one minute	Differs
Business sender onboarding (from 15 Jul 2027)	KYC data and risk assessment	Same data, plus IP location, VPN use and sign-up timing as risk indicators	Differs
Biometric processing	Explicit consent likely needed; alternative required	Same	Same
Supplying SIM farm devices (from 29 Oct 2026)	Good-reason check and supply record	Same	Same

Switching is a digital-first process

Under condition C7, providers must let customers request a porting authorisation code (PAC), a service termination authorisation code (STAC) or switching information by at least three methods (text message, phone and online account) and provide it within one minute. Providers may add multi-factor authentication and "stop the clock" while the customer supplies the extra credential, but Ofcom says they should ask for information customers can easily recall, such as date of birth or postcode, not an account number, password or

last bill amount ([Ofcom guidance on multi-factor authentication relating to Auto-Switch](#)). Authentication design therefore has to resist fraud without slowing a legitimate switch.

eSIMs fall inside the scam rules

Ofcom's definition of a pay-as-you-go customer covers SIMs made available or obtained electronically, so eSIM-only brands must apply the same volume limits as retailers of physical SIMs. For thin MVNOs, the host network enforces the limit (guidance paragraphs 2.49 to 2.51).

Online sign-up signals for business senders

Ofcom's list of KYC risk indicators includes an IP address that does not match the claimed location, use of a virtual private network, sign-up outside business hours and generic, non-business email addresses. These signals only exist in remote onboarding, so A2P platforms that onboard customers through a web form or an API need to capture them.

Pending: the A2P due diligence rules [Adopted, effective 15 Jul 2027](#) and the updated CLI guidance on spoofed UK mobile numbers [Adopted, effective 15 Jul 2027](#).

6 Data protection and biometrics

The UK GDPR and the Data Protection Act 2018 apply to all identity capture, and the Privacy and Electronic Communications Regulations 2003 add sector-specific duties for communications providers. Most data protection provisions of the Data (Use and Access) Act 2025 came into force on 5 February 2026, including ICO powers to fine up to £17.5 million or 4% of global turnover under the Privacy and Electronic Communications Regulations; the requirement to have a complaints procedure was scheduled to commence on 19 June 2026 ([ICO statement, 5 February 2026](#)).

Biometric data used to uniquely identify a person, for example a face match against an identity document, is special category biometric data. The ICO states that explicit consent is likely to be the most appropriate condition, that it must be given by a clear statement, and that a provider relying on consent must offer a suitable alternative to customers who decline. If no valid condition applies, the biometric system must not be used ([ICO, How do we process biometric data lawfully?](#)).

For fraud prevention data, Ofcom's C9 guidance points to the "recognised legitimate interests" basis added to the UK GDPR by the 2025 Act, which includes fraud prevention, and expects providers sharing scam intelligence to minimise and restrict the data shared. Condition C9.27 makes data protection compliance a condition in its own right, and records

of KYC risk assessments and evidence must be kept for at least three years after the contract ends.

7

Sector-specific obligations

Scam message rules: General Condition C9

Adopted, effective 18 Jan 2027 and 15 Jul 2027

Ofcom's July 2026 statement sets a new condition C9 and a matching condition for non-providers that hold numbers. For person-to-person (P2P) messaging, from 18 January 2027 operators must cap pay-as-you-go SIM volumes and block a SIM automatically at the limit, act on validated scam reports, and block scam numbers and messages containing known scam links or numbers. For A2P messaging, from 15 July 2027 operators and aggregators must ensure KYC, sender ID and know-your-traffic checks take place, maintain policies on protected and generic sender IDs, and, on becoming aware of a scam by a sender they onboarded, confirm the sender's identity and stop further messages within one working day. Affected senders and recipients must be able to challenge a block.

Numbers, caller ID and spoofing

Condition C6.6 requires providers, where technically feasible, to identify and block calls with invalid or non-dialable caller line identification (CLI) data. Updated CLI guidance

Adopted, effective 15 Jul 2027 expects the first UK provider receiving a call from abroad that shows a UK mobile (+447) number to mark the number as withheld unless the call arrives over a route that verifies it by design ([Ofcom statement, Tackling scam calls from abroad, 15 July 2026](#)).

SIM farm offences

Adopted, effective 29 Oct 2026

Sections 151 to 153 of the [Crime and Policing Act 2026](#) make it an offence to possess or supply a SIM farm, defined as a device capable of using five or more physical SIM cards simultaneously or interchangeably to call or text telephone numbers. Operating or maintaining an electronic communications network is listed as a good reason. A supplier must take reasonable steps to satisfy itself that the recipient has a good reason and must record the date, device, recipient name, address and any company number, and the steps taken ([Home Office guidance, July 2026](#)).

Account takeover and the Fraud Sector Charter

No General Condition sets a specific authentication standard for SIM swaps. The second [Fraud Sector Charter for telecommunications](#) (5 November 2025), signed by the main mobile networks, is voluntary: signatories commit to sector-wide best practice against account takeover, including two-factor authentication before account transfers, to resolving most fraud cases within 21 days after one year and 14 days after two, and to a working group on bogus pay-as-you-go identities.

8

Risk indicators and red flags

Ofcom's C9 guidance and its July 2026 statements identify these fraud and identity-abuse indicators for mobile and messaging providers.

TELECOM FRAUD AND IDENTITY-ABUSE INDICATORS

- **High-volume new SIMs:** very large message volumes from newly activated SIMs, typical of SIM farm use.
- **Location mismatch:** a business sender's IP address does not match the country it claims to be based in.
- **Concealment:** sign-up through a virtual private network or outside business hours.
- **Recycled details:** name, address or IP address matching a disabled or dormant account, or one email used for several accounts.
- **Weak identity:** generic non-business email, incomplete address data or a vague stated use of messaging.
- **Sender ID mismatch:** a requested alphanumeric sender name unrelated to the business, or imitating a bank, delivery firm or public body.
- **Traffic spikes:** sudden, unprecedented increases in volume or in requests for new sender IDs or numbers.
- **Spoofed UK mobile numbers:** calls from abroad showing +447 numbers far exceeding known roaming traffic.

Enforcement and penalties

For breaches of the General Conditions, Ofcom can impose financial penalties of up to 10% of annual turnover under sections 96A to 97 of the Communications Act 2003, suspend a provider's entitlement to provide networks or services (section 100), require blocking of numbers or services, and withdraw number allocations (section 61 and condition B1.18). Separate powers under sections 128 to 130 address persistent misuse of a network or service by any person.

On 24 September 2026 Ofcom opened investigations into [Vonage Business Limited and Voxbone SA](#) under condition B1, examining whether they took appropriate steps, including know-your-customer checks on business customers, to stop scammers misusing numbers allocated to them.

The SIM farm offences are summary offences: in England and Wales the fine is unlimited, and in Scotland and Northern Ireland it is capped at level 5 on the standard scale (section 151(5)). The ICO can fine up to £17.5 million or 4% of global turnover, whichever is higher, for breaches of the Privacy and Electronic Communications Regulations since 5 February 2026.

Recent changes and what to watch

- **29 October 2026** Adopted, effective 29 Oct 2026 SIM farm possession and supply offences take effect after a six-month transition; suppliers of multi-SIM devices need recipient checks and supply records in place.
- **24 September 2026** Investigations open Ofcom investigates Vonage Business and Voxbone over number misuse; expect sharper scrutiny of KYC on business number customers.
- **15 July 2026** Adopted, effective 18 Jan 2027 and 15 Jul 2027 General Condition C9 on scam messages: pay-as-you-go volume limits and blocking first, then A2P KYC and know-your-traffic checks.
- **15 July 2026** Adopted, effective 15 Jul 2027 Updated CLI guidance: calls from abroad showing unverified UK mobile numbers will display as withheld.
- **14 July 2026** In force Telecommunications Security Code of Practice version 1.1 issued for Tier 1 and Tier 2 providers.
- **5 February 2026** In force Most Data (Use and Access) Act 2025 data protection provisions commence, raising maximum fines under the Privacy and Electronic Communications Regulations.

- **5 November 2025** **Voluntary commitment** Second Fraud Sector Charter for telecoms, including two-factor authentication before account transfers and faster fraud case resolution.

11 What this means for identity verification

For consumer SIM and eSIM sales, identity verification is a business and fraud decision rather than a legal requirement, so providers can choose document checks, database checks or biometric face matching for contract customers. If face matching is used, design it around explicit consent and offer a non-biometric alternative. Retail and online journeys can use the same checks, since no rule distinguishes them.

Re-verification matters most at high-risk moments: SIM swaps, eSIM transfers, switching code requests and changes to contact details. Authentication must work within the one-minute switching rule and should not rely on account numbers or passwords customers cannot recall.

Business verification is where the regulatory weight now lies. Operators, aggregators and providers that sub-allocate numbers need know-your-business onboarding that cross-checks company, director and ownership data against public registers, scores signals such as IP location and VPN use, and keeps evidence for three years after the relationship ends, with ongoing monitoring from July 2027.

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- KYB and beneficial owner verification for business messaging senders, matching the data Ofcom's General Condition C9 expects providers to collect and assess.
- Remote KYC onboarding for contract and eSIM customers with ID document capture and verification, including NFC chip reading.
- Biometric liveness and face match with a configurable non-biometric alternative path, supporting explicit-consent journeys.
- Ongoing monitoring and phone and email verification to support step-up checks before SIM swaps, switching and account changes.
- No-code workflow builder with an audit trail for each check, supporting record-keeping obligations.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **General Conditions of Entitlement** (consolidated version in force from 8 April 2026), Ofcom, [ofcom.org.uk](https://www.ofcom.org.uk)
- **Amendments to the General Conditions of Entitlement**, Ofcom (last updated 22 April 2025), [ofcom.org.uk](https://www.ofcom.org.uk)
- **Statement: Combatting mobile messaging scams, new rules and guidance**, Ofcom, 15 July 2026, paragraphs 1.9, 2.24, 4.63 and footnote 66, [ofcom.org.uk](https://www.ofcom.org.uk)
- **Scam mobile messages: guidance on protecting people and businesses**, Ofcom, 15 July 2026, sections 1 and 2, [ofcom.org.uk](https://www.ofcom.org.uk)

- **Statement: Tackling scam calls from abroad, updating the CLI Guidance**, Ofcom, 15 July 2026, [ofcom.org.uk](https://www.ofcom.org.uk)
- **Guidance on multi-factor authentication relating to Auto-Switch (General Condition C7)**, Ofcom, [ofcom.org.uk](https://www.ofcom.org.uk)
- **Ofcom launches investigations into whether two telecoms companies failed to prevent misuse of their phone numbers by scammers**, Ofcom, 24 September 2026, [ofcom.org.uk](https://www.ofcom.org.uk)
- **Crime and Policing Act 2026 (c. 20), sections 151 to 153**, [legislation.gov.uk](https://www.legislation.gov.uk)
- **Crime and Policing Act 2026 Guidance: Offences relating to the possession and supply of SIM farms**, Home Office, 27 July 2026, [gov.uk](https://www.gov.uk)
- **Fraud Sector Charter: telecommunications**, Home Office, 5 November 2025, [gov.uk](https://www.gov.uk)
- **Revised Telecommunications Security Code of Practice 2026 (version 1.1)**, DSIT, issued 14 July 2026, [gov.uk](https://www.gov.uk)
- **The Payment Services Regulations 2017 (SI 2017/752), Schedule 1, Part 2, paragraph 2(l)**, [legislation.gov.uk](https://www.legislation.gov.uk)
- **The Money Laundering and Terrorist Financing (Amendment) Regulations 2026 (SI 2026/621)**, made 9 June 2026, [legislation.gov.uk](https://www.legislation.gov.uk)
- **Statement on the commencement of the Data (Use and Access) Act**, ICO, 5 February 2026, [ico.org.uk](https://www.ico.org.uk)
- **Biometric data guidance: How do we process biometric data lawfully?**, ICO, [ico.org.uk](https://www.ico.org.uk)
- **UK digital verification services trust framework: supporting documents**, Office for Digital Identities and Attributes, [gov.uk](https://www.gov.uk)