



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Germany

COUNTRY **Germany**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **29 October 2026**

KEY REGULATORS **Bundesnetzagentur · Federal Commissioner for Data Protection and Freedom of Information (BfDI) · Federal Office for Information Security (BSI)**

Key takeaways

- No telecoms licence is needed to sell mobile services in Germany, but every network operator and every non-messaging telecoms provider must notify the Federal Network Agency (Bundesnetzagentur) before starting.
- Telecom operators are not covered by the anti-money laundering (AML) law. Identity checks come from the Telecommunications Act instead, and they apply hardest to prepaid mobile.
- A prepaid SIM or eSIM may not be switched on until the customer's name, address and date of birth have been checked against an official identity document. Selling it first and checking later is not allowed.
- Online activation is allowed only through set methods: the German online ID function (eID), agent-led or automated video identification meeting Bundesnetzagentur rules, or matching against an earlier verified identification. Video methods also need an accredited conformity certificate, which cannot be obtained yet; the regulator has said it will not open proceedings for that gap alone before 1 May 2027.
- SIM swaps, eSIM re-issues and address changes are the main fraud risk. The data protection regulator fined Vodafone EUR 45 million in 2025, partly because weak authentication let third parties obtain eSIM profiles.

Germany is open to mobile network operators, mobile virtual network operators (MVNOs) and resellers, including fully digital and eSIM-only brands. There is no licensing gate for services: entry is by notification, and the Bundesnetzagentur supervises compliance after launch.

The principal authorities are the Bundesnetzagentur for subscriber identification, number porting and network security, and the Federal Commissioner for Data Protection and Freedom of Information (BfDI) for how operators handle customer data, including authentication in shops, call centres and online accounts.

The biggest obstacle for a digital entrant is the prepaid identification rule. Remote identification methods must meet a detailed Bundesnetzagentur specification, and a certification step written into the law cannot yet be completed because no certification body has been accredited.

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

Authority	Remit for mobile services	Level	Official site
Bundesnetzagentur (Federal Network Agency)	Notification of providers; prepaid identification and the approved methods; subscriber data for authority requests; number porting; network security catalogue; fines under the Telecommunications Act	Federal	bundesnetzagentur.de
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)	Data protection supervisor for all processing done to provide telecoms services; authentication guidance; fines under the General Data Protection Regulation (GDPR)	Federal	bfdi.bund.de
Bundesamt für Sicherheit in der Informationstechnik (BSI)	IT security standards; co-author of the telecoms security catalogue; TR-03147 identity-proofing assurance levels	Federal	bsi.bund.de
Bundesministerium für Digitales und Staatsmodernisierung (BMDS)	National European Digital Identity Wallet	Federal	bmds.bund.de

Conformity assessment bodies for prepaid identification methods are accredited by the national accreditation body, the Deutsche Akkreditierungsstelle (DAkKS), under the Bundesnetzagentur's conformity assessment programme.

2

Licensing and authorisation

The TKG of 23 June 2021, last amended by the Act to modernise the Federal Police Act of 22 October 2026 (BGBl. 2026 I Nr. 318), does not license telecoms services. Under [§ 5 TKG](#), anyone who commercially operates a public telecoms network or provides publicly available telecoms services must notify the Bundesnetzagentur without delay when it intends to start, change or end the activity, using the agency's published form. Number-independent messaging services are excluded from this duty.

The identification duties in § 172 TKG attach to function, not brand. They apply to any provider that assigns phone numbers or other connection identifiers, or that provides connections for numbers assigned by others. An MVNO or reseller that assigns numbers to its own subscribers therefore carries the duty itself.

3

Identity framework (AML rules do not apply)

The list of obliged entities in [§ 2\(1\) of the Geldwäschegesetz \(GwG, Money Laundering Act\)](#) does not include telecoms providers. A mobile operator therefore has no customer due diligence, beneficial ownership, transaction monitoring or suspicious activity reporting duty in that capacity. It becomes an obliged entity only if it also carries on a regulated activity in its own right, for example as a licensed payment or e-money institution. Carrier billing is exempt from payment services licensing only within the limits of [§ 2\(1\) No. 11 of the Payment Services Supervision Act \(ZAG\)](#): digital content, voice services, charitable donations or tickets charged to the phone bill, up to EUR 50 per payment and EUR 300 a month per subscriber. The operator must notify the Federal Financial Supervisory Authority (BaFin) and confirm compliance with the limits in an annual audit certificate (§ 2(3) ZAG).

Customer identity in telecoms is governed by three provisions instead:

§ 172(1) TKG: collect before activation

Providers that assign numbers must collect and store, before activation, the number, the holder's name and address, date of birth for individuals, the device number if a handset is supplied with the line, and the assignment and contract start dates. This applies to prepaid and postpaid alike.

§ 172(2) TKG: verify prepaid before activation

Prepaid mobile providers must check name, address and date of birth against a listed official document before activation. This is the only statutory verification duty in the sector.

§ 7 TDDDG: optional ID on contract changes

Under the TDDDG, any telecoms provider may ask for an official ID when a contract is created or changed, where needed to check the customer's details. The eID can replace the physical card.

Postpaid contracts are verified by commercial practice rather than by statute: § 172(1) requires collection, not document verification, and § 7 TDDDG makes an ID check optional. Collected data must be corrected without delay when a change becomes known, and deleted at the end of the calendar year after the contract ends ([§ 172\(4\) and \(6\) TKG](#)).

4

Identity verification and onboarding

Accepted documents for prepaid activation

[§ 172\(2\) sentence 1 TKG](#) lists the documents: a German identity card; a passport; another valid official photo ID that satisfies the German passport and ID obligation, including foreign passports and ID cards recognised under immigration law; a residence title; an asylum arrival certificate or temporary residence permit; or a certificate of suspension of deportation. For legal persons and partnerships, a commercial or cooperative register extract, founding documents or equivalent evidence, or a check of the register itself. The provider must record the method used and, for personal documents, the document type, number and issuing authority.

Approved methods

The baseline is presentation of the document in person. A sales partner may send the provider an electronic copy of the ID card or passport. The eID online function of the German ID card, the EU eID card and the electronic residence permit counts as presentation of an official ID. The Bundesnetzagentur reads § 7(2) TDDDG and § 172(2) TKG together this way in its [guidance of 29 December 2021](#). Any other method must follow [Verfügung Nr. 94/2021](#) (Official Gazette 23/2021), which recognises four:

Method (Vfg 94/2021)	Core requirements
On-site identification by a third party	Personal presence; visual and tactile check of the document; documentation of when, where, by whom and with which document. Sales partners and points of sale are not "third parties" for this method.
Agent-led video identification	Trained staff (refreshed at least yearly) in access-controlled rooms; real-time, uninterrupted, end-to-end encrypted session; checks of optical security features and a machine-readable zone; random assignment of agents; root and jailbreak detection in mobile apps.
Automated video identification	Sequential, time-linked steps with direct interaction for liveness, varied in order or type; manipulation and deepfake detection; penetration and robustness testing; explicit consent; human sample checks within seven days.
Matching against a prior identification	Comparison with data held by a third party, or by the customer in an unalterable record, from an earlier identification with a § 172 document; PIN-authenticated consent to transfer; integrity and currency controls; a name change always requires re-identification.

Before using any of these methods the provider must hold a certificate from an accredited conformity assessment body confirming the method meets the Verfügung, no more than 24 months old (§ 172(2) sentences 4 and 5 TKG). In-person presentation and the eID need no certificate. A provider that uses a third party for collection or verification remains responsible for compliance (§ 172(5) TKG).

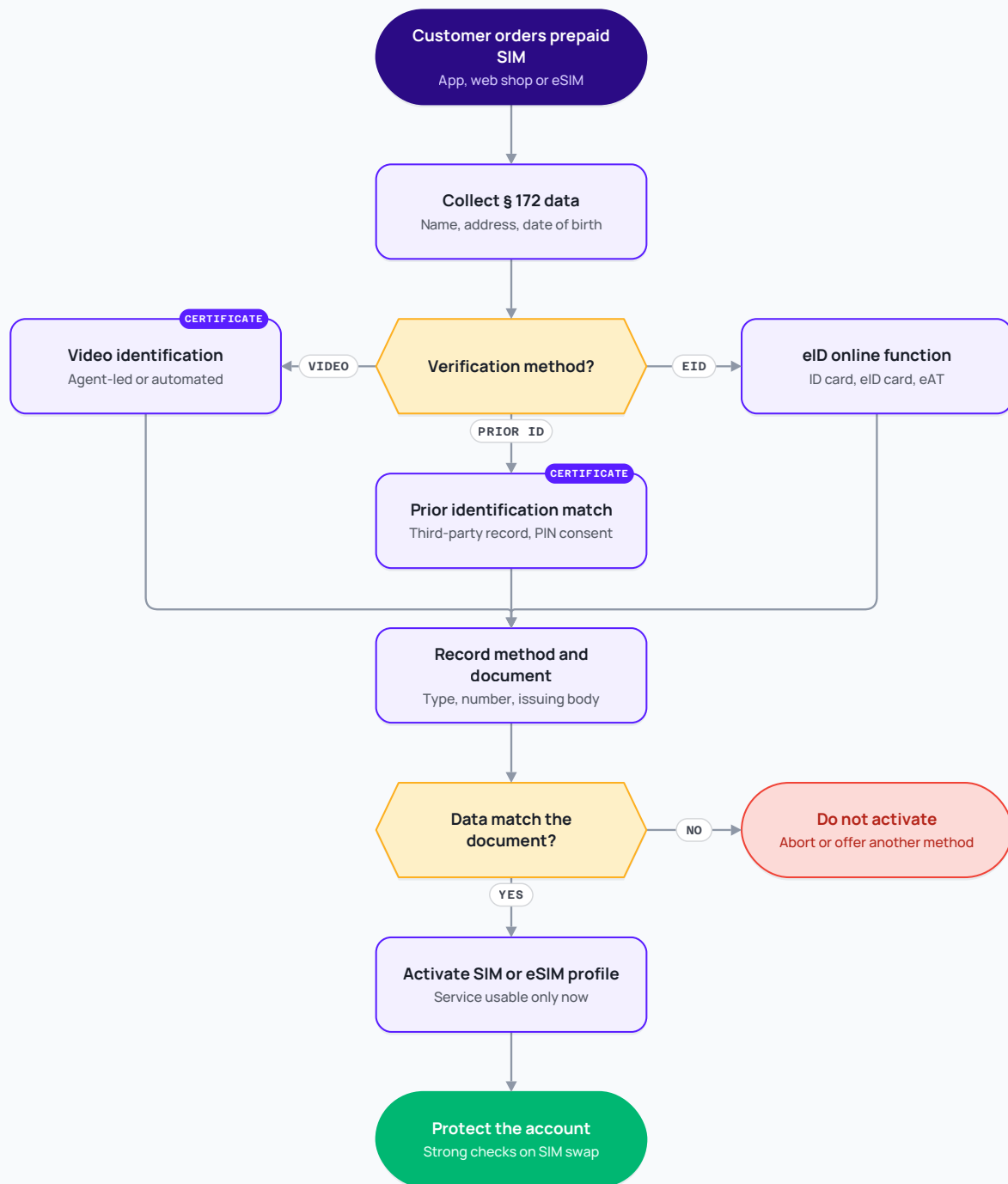


Figure 1. Online prepaid SIM or eSIM activation in Germany under § 172 TKG and Verfügung Nr. 94/2021.

Bottom line: the duty to verify a prepaid customer before activation is the same in a shop and online, but online the provider may use only the eID or a method that meets Verfügung Nr. 94/2021 and, apart from the eID, carries an accredited conformity certificate.

Requirement	In person / shop	Online / remote	Difference
Prepaid verification before activation	Required (§ 172(2) TKG)	Required (§ 172(2) TKG)	Same
Accepted documents	§ 172(2) list	§ 172(2) list; video methods need a machine-readable zone and verifiable security features	Differs
Method rules	Document presented and checked on site	eID, or a Vfg 94/2021 method (video, automated video, prior-identification match)	Differs
Conformity certificate	Not needed	Needed for Vfg methods; not for the eID	Differs
Liveness and manipulation detection	Staff compare person and photo	Interaction for liveness; deepfake and stream manipulation controls; root detection	Differs
Evidence retained	Method and document details	Same, plus automated-video evidence kept 7 days (up to 8 weeks if fraud is suspected)	Differs
Postpaid identity check	Collection required; ID check optional (§ 7 TDDDG)	Same; the eID may replace the physical card	Same
Authentication for account changes	Risk-based under art. 32 GDPR	Risk-based; BfDI expects a second factor for online accounts and separate secrets per channel	Differs

The conformity certificate gap

The 12-month transition for certificates ended on 1 December 2022 and the TKG does not allow an extension. No conformity assessment body has yet been accredited, so certificates cannot be obtained. In [Mitteilung Nr. 86/2026](#) (Official Gazette 10/2026, 27 May 2026), extending [Mitteilung Nr. 249/2025](#), which had run to 1 May 2026, the Bundesnetzagentur states that it will not open supervisory proceedings under § 183 TKG before 1 May 2027 solely because a certificate is missing

Enforcement relief to 1 May 2027. The relief is conditional: providers must still check for themselves that their methods meet Verfügung Nr. 94/2021 and comply with it, and the agency will open proceedings of its own motion if it learns that a method falls short.

eSIM and in-band identification

Video sessions may run over the purchased mobile service itself, provided the line can be used for nothing except the identification, including any prior data collection, until activation (Vfg 94/2021, A.II.2.6.3 and 3.6.4).

Pending change to video identification

Following security concerns about video identification, the Bundesnetzagentur consulted on a revised Verfügung (draft of November 2022, hearing on 24 November 2022). In May 2026 the agency confirmed that a successor regulation is being drafted and that its new requirements, in particular on the security of identification methods, will apply from its entry into force. Until then Verfügung 94/2021 in its December 2021 form applies, as it has in full since 1 May 2023 **Successor regulation in preparation**.

6 Data protection and biometrics

The GDPR applies to all identity capture, and the BfDI is the competent supervisory authority wherever data are processed to provide telecoms services ([§ 29 TDDDG](#)), not the state data protection authorities.

- **Legal basis.** Collection under § 172 TKG rests on a legal obligation. The Verfügung cites art. 6(1)© GDPR together with § 172.
- **ID copies.** Where a provider asks for an ID under § 7 TDDDG it may copy it, but must destroy the copy as soon as the contract details are established and may not process other data from it.
- **Automated video identification.** The customer must give explicit, documented consent both to processing by automated decision systems and to recording for quality

sampling. Beforehand the customer must be told about the technology and logic involved and what happens to the data. Evidence is deleted after seven days as a rule, kept up to four weeks where sampling reveals fraud or errors and never beyond eight weeks. Reuse for system training falls outside the Verfügung and needs its own legal basis.

- **Biometrics.** The Datenschutzkonferenz (conference of German data protection authorities) treats biometric processing for unique identification as prohibited in principle under art. 9(1) GDPR unless an art. 9(2) exception applies, typically explicit consent that refers to the biometric data ([position paper of 3 April 2019](#), adopted against the votes of Bavaria and Baden-Württemberg).

7 Sector-specific obligations

Authentication before SIM swap, eSIM re-issue and contract changes

No German statute sets a specific SIM-swap procedure. The obligation comes from art. 32 GDPR and § 165(1) TKG, which requires measures protecting telecommunications secrecy and personal data. The BfDI's working paper "[Authentifizierung im Bereich Telekommunikation: Risikofelder](#)" sets the supervisor's expectations. Swapping SIM cards and changing the delivery address for a SIM are high-risk processes. eSIMs make swaps easier because nothing is posted. Risks that materialise outside the operator, such as takeover of accounts secured by SMS codes, must still be part of its risk assessment. Online accounts need secure passwords, possibly a second factor and a secure reset process, and passwords used for the call centre or shop must not be reused online. Shop and partner staff should only access the customer data they need. The BfDI's [customer data checklist for telecoms sales and service](#) (January 2025) asks operators to assess SIM swapping both by replacement SIM and by number porting, eSIM issuance, an address change followed by a hardware order and reliance on SMS one-time passwords, and to provide an emergency route for customers whose account has been compromised.

Number porting

Under [§ 59 TKG](#) the receiving provider leads a provider switch and number port. No switch or port may be carried out without the end user's contract with the receiving provider. Service may not be interrupted for more than one working day.

Subscriber data for authority requests

Number-assigning providers keep § 172 data in customer files that the Bundesnetzagentur can retrieve automatically at any time ([§ 173 TKG](#)). For ported numbers they also keep the

current porting identifier. Manual disclosure to authorities under § 174 TKG requires a written or electronic request citing a legal basis. In urgent cases another form is allowed if confirmed in writing without delay.

The general traffic data retention duty in §§ 175 and 176 TKG is still in the statute but is not applied **Inapplicable (BVerwG, 2023)**. In judgments of 14 August 2023 (6 C 6.22 and 6 C 7.22) the Federal Administrative Court held it incompatible with EU law in its entirety, as the [Bundesnetzagentur notes](#).

Network security and multi-factor authentication

Operators and providers that qualify as important or particularly important entities under the BSI Act must base their measures on an all-hazards approach that includes, among other things, multi-factor or continuous authentication (§ 165(2a) TKG, inserted by the [NIS-2 Implementation Act](#), BGBl. 2025 I Nr. 301, in force since 6 December 2025).

Management must implement and oversee these measures and attend regular training. The 29 April 2020 security catalogue remains valid. A revised draft (version 2025-10) was consulted on until 16 January 2026 **Draft catalogue, not adopted**.

Risk indicators and red flags

IDENTITY ABUSE PATTERNS NAMED BY THE BFDI

- **SIM-swap request:** a caller asks for a replacement SIM or eSIM for an existing contract.
- **Address change before dispatch:** the SIM delivery address is changed shortly before a replacement is sent.
- **eSIM profile retrieval:** an eSIM profile is retrieved through a mix of online portal and hotline steps.
- **Partner-agency fraud:** sales staff create fictitious contracts or contract changes in customers' names.
- **Port-out takeover:** the number is ported to another provider so that SMS codes reach the fraudster.
- **Third-party bank account:** a new contract is paid from another person's account.
- **Straw-holder SIMs:** SIMs registered in another person's name and later used for crime.
- **Password reuse across channels:** one secret works for call centre, shop and online account.

Enforcement and penalties

The Bundesnetzagentur prosecutes TKG offences ([§ 228 TKG](#)), which are set per offence:

Breach	Maximum fine
Failing to collect, store or correct § 172 data, to verify prepaid data before activation, or to delete data on time (§ 228(2) Nr. 49, 50 and 53)	EUR 300,000
Failing to ensure the agency can retrieve customer files automatically (§ 228(2) Nr. 54)	EUR 500,000
A third party using inaccurate data, or not passing on changes (§ 228(2) Nr. 51 and 52)	EUR 10,000

Beyond fines, the Verfügung reserves supervisory orders under § 183 TKG and, for serious defects, an order to re-verify the affected subscriber data.

Data protection breaches are fined by the BfDI under the GDPR's turnover-based scale, and TDDDG offences reach EUR 300,000 ([§ 28 TDDDG](#)). On 3 June 2025 the [BfDI fined Vodafone GmbH](#) a total of EUR 45 million. EUR 15 million was for insufficient checking and monitoring of partner agencies (art. 28(1) GDPR). EUR 30 million was for security defects in authentication when the "MeinVodafone" portal and the hotline were used together, which let unauthorised third parties retrieve eSIM profiles. The fines were accepted and paid.

10 Recent changes and what to watch

- **December 2027: wallet acceptance by telecom operators**

[Adopted, applies from 24 December 2027](#). Under art. 5f(2) of the amended eIDAS Regulation, telecom providers other than micro and small enterprises that must use strong user authentication for online identification must accept EU Digital Identity Wallets at the user's request, 36 months after the implementing acts under arts. 5a(23) and 5c(6) entered into force on 24 December 2024.

- **Early 2027: German EUDI wallet "d-you"** [Launch planned early 2027](#). The free, voluntary state wallet becomes available; recognition of non-state wallets is planned about 12 months later.

- **30 September 2026: BSI injection-attack guidance** [Consultation closed](#). Draft evaluation guidance for injection attack detection in video-based remote identity proofing, a planned extension of TR-03147.

- **19 June 2026: IP address retention bill** [Bill, not enacted](#). Government bill [BT-Drucksache 21/6581](#) would require internet access providers to keep assigned IP addresses for three months, in place of the general retention duty that courts have held inapplicable; it has been referred to committee.

- **27 May 2026: Conformity certificate relief extended** [Relief to 1 May 2027](#). Mitteilung Nr. 86/2026: no proceedings solely for a missing certificate before 1 May 2027; a successor to Verfügung 94/2021 is being drafted. Watch for the new Verfügung and the first accredited bodies.

- **16 January 2026: security catalogue revision** [Draft, not adopted](#). Version 2025-10 adds three risk tiers and 5G measures; comments closed.

- **3 June 2025: Vodafone authentication fines** [Final](#). EUR 45 million in total, including EUR 30 million for authentication defects affecting eSIM profiles.

- **Block service until verified.** For prepaid, activation must wait for a successful check; an eSIM may connect only for the identification session.
- **Support the eID first.** The eID online function needs no conformity certificate and avoids document-image capture, but covers only holders of German ID cards, EU eID cards and electronic residence permits.
- **Design video flows to the Verfügung.** Machine-readable zone and security-feature checks, liveness through varied interaction, deepfake and stream-injection controls, root detection and end-to-end encryption are requirements, not options.
- **Plan for certification.** Document each method now; the current relief runs only to 1 May 2027.
- **Separate consent and retention.** Automated video identification needs explicit consent and a 7-day evidence deletion clock; biometric processing needs an art. 9(2) GDPR basis.
- **Re-verify on risk events.** SIM swaps, eSIM re-issues, address changes and contract extensions call for authentication proportionate to the risk, with a second factor online.

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:

- ID document capture and verification, including NFC chip reading, to check name, address and date of birth before a prepaid SIM or eSIM is activated.
- Video KYC with agent-led sessions for operators using video identification under Bundesnetzagentur rules.
- Biometric liveness and face match to support manipulation and deepfake controls in remote identification.
- Phone and email verification and re-verification workflows for high-risk changes such as SIM swaps and eSIM re-issues.
- No-code workflow builder with cloud, on-premises or hybrid deployment and an audit trail for each check.

[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

- Telekommunikationsgesetz (TKG) [Telecommunications Act] of 23 June 2021, last amended by Art. 12(15) of the Act of 22 October 2026 (BGBl. 2026 I Nr. 318), §§ 5, 59, 165, 172, 173, 174, 228, Gesetze im Internet, gesetze-im-internet.de/tkg_2021
- TKG § 172, Daten für Auskunftersuchen der Sicherheitsbehörden, gesetze-im-internet.de
- Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), §§ 7, 28, 29, gesetze-im-internet.de/ttdsg
- Geldwäschegesetz (GwG) [Money Laundering Act], § 2, gesetze-im-internet.de

- Bundesnetzagentur, Identverfahren für Prepaid-Mobilfunkdienste (incl. Mitteilung Nr. 86/2026 and the November 2022 consultation), [bundesnetzagentur.de](https://www.bundesnetzagentur.de)
- Bundesnetzagentur, Verfügung Nr. 94/2021 zur Festlegung von Verfahren zur Überprüfung von Anschlussinhaberdaten, Official Gazette 23/2021, Stand December 2021, [bundesnetzagentur.de](https://www.bundesnetzagentur.de) (PDF)
- Bundesnetzagentur, Amtsblatt 10/2026, Mitteilung Nr. 86/2026 (conformity certificates), 27 May 2026, [bundesnetzagentur.de](https://www.bundesnetzagentur.de) (PDF)
- Bundesnetzagentur, Amtsblatt 16/2025, Mitteilung Nr. 249/2025 (conformity certificates), 20 August 2025, [bundesnetzagentur.de](https://www.bundesnetzagentur.de) (2025 issues, ZIP)
- Bundesnetzagentur, Verkehrsdatenspeicherung (BVerwG judgments of 14 August 2023), [bundesnetzagentur.de](https://www.bundesnetzagentur.de)
- Bundesnetzagentur, Handreichung zur Verfügung (Version 1.1), 29 December 2021, [bundesnetzagentur.de](https://www.bundesnetzagentur.de) (PDF)
- Bundesnetzagentur, Katalog von Sicherheitsanforderungen gemäß § 167 TKG and draft version 2025-10, [bundesnetzagentur.de](https://www.bundesnetzagentur.de)
- BfDI, Authentifizierung im Bereich Telekommunikation: Risikofelder, [bfdi.bund.de](https://www.bfdi.bund.de)
- BfDI, Checkliste Kundenbestandsdaten bei Vertrieb und Service von Telekommunikationsunternehmen, January 2025, [bfdi.bund.de](https://www.bfdi.bund.de)
- BfDI, BfDI verhängt Geldbußen gegen Vodafone, press release, 3 June 2025, [bfdi.bund.de](https://www.bfdi.bund.de)
- Gesetz zur Umsetzung der NIS-2-Richtlinie, BGBl. 2025 I Nr. 301, 5 December 2025 (Art. 25: TKG; Art. 30: entry into force), [recht.bund.de](https://www.recht.bund.de)
- Zahlungsdiensteaufsichtsgesetz (ZAG) [Payment Services Supervision Act], § 2(1) No. 11 and (3), [gesetze-im-internet.de](https://www.gesetze-im-internet.de)
- Datenschutzkonferenz, Positionspapier zur biometrischen Analyse, version 1.0, 3 April 2019, [datenschutzkonferenz-online.de](https://www.datenschutzkonferenz-online.de) (PDF)
- BSI, TR-03147 and consultation on injection attack detection, [bsi.bund.de](https://www.bsi.bund.de)
- BMDS, EUDI-Wallet "d-you", [bmds.bund.de](https://www.bmds.bund.de)
- Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (European Digital Identity Framework), art. 5f, EUR-Lex, eur-lex.europa.eu
- Commission Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980 and 2024/2982 (art. 5a(23)) and 2024/2981 (art. 5c(6)), OJ 4 December 2024, in force on the twentieth day after publication, eur-lex.europa.eu
- Deutscher Bundestag, BT-Drucksache 21/6581, Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren, 19 June 2026, ds.bundestag.de (PDF)
- Deutscher Bundestag, hib: Gesetzentwurf zur Einführung einer IP-Adressspeicherung (BT-Drucksache 21/6581), [bundestag.de](https://www.bundestag.de)
- Deutsche Bundesbank, Finanzsanktionen, [bundesbank.de](https://www.bundesbank.de)