Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Austria

COUNTRY Austria

INDUSTRY Telecom & Mobile Services

LAST UPDATED 11 November 2026

KEY REGULATORS Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR-GmbH) · Telekom-Control-Kommission

Key takeaways

- No telecom licence is needed to sell mobile or fixed services in Austria, but every operator, including a mobile virtual network operator (MVNO, a brand that rents capacity on another network), must notify the regulator electronically before launch.
- Every subscriber must be identified before the contract is performed, and their name, academic degree and date of birth registered. New prepaid SIM cards have needed registration since 1 January 2019, and older anonymous cards must be registered before their first top-up after 1 September 2019.
- SIM and eSIM can be sold fully online. The law accepts an automated photo-identification check (selfie with head or facial movements, ID document capture, document authenticity checks and face matching) or an electronic identity confirmation from a bank.
- Telecom operators are not covered by Austria's anti-money laundering (AML) law. Identity duties come from telecom law, and biometric data from the online check must be deleted as soon as the check ends.
- Fraud controls now sit with the network: calls from abroad showing an Austrian number that cannot be authenticated must have that number hidden, and since 1 October 2026 only SMS sender names listed in the regulator's public register may be delivered. A bill would also let the telecom regulator order internet providers to block illegal gambling sites; it is not yet law.

Austria's mobile market is open to new entrants online, with no licence for service providers, only a prior notification. The Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR-GmbH) receives notifications and writes the detailed rules on numbering, number portability and SMS sender names; the Telekom-Control-Kommission (TKK) takes regulatory decisions; and the Fernmeldebüro, the federal telecommunications authority, imposes administrative fines.

The biggest practical obstacle is identity: no SIM may go live until the subscriber has been identified by one of the methods in the Identification Regulation, and the online method sets out a detailed, step-by-step procedure that onboarding flows must follow exactly.

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 telecom and mobile services	Level	Official site
RTR-GmbH (Telecommunications and Post division)	Receives service notifications; issues the Communications Parameters, Fees and Value-Added Services Regulation 2009 (KEM-V 2009) and the Number Portability Regulation 2022; runs the SMS sender-name register and the number-misuse reporting service	National	rtr.at
Telekom-Control-Kommission (TKK)	Regulatory decisions under the Telecommunications Act 2021 (TKG 2021)	National	rtr.at/TKK
Fernmeldebüro (telecommunications authority)	Enforces TKG 2021, including administrative penalty proceedings under § 188; seven locations in Austria	National	fb.gv.at
Federal Ministry for Housing, Arts, Culture, Media and Sport	Regulation of post and telecommunications (Federal Ministries Act, Annex, part B no. 9); oversees the Fernmeldebüro; the minister issues the Identification Regulation (IVO) with the Interior Minister (TKG 2021 § 166(2))	National	bmwkms.gv.at

Data Protection Authority (Datenschutzbehörde)	Receives personal data breach notifications from operators (TKG 2021 § 164)	National	dsb.gv.at
Federal Office for Cyber Security (Bundesamt für Cybersicherheit)	Cybersecurity authority under the Network and Information Systems Security Act 2026 (NISG 2026); reports directly to the Interior Minister	National	Ministry of the Interior

Sanctions compliance outside the financial sector is monitored by the Federal Minister of the Interior under SanktG 2024 § 12.

2 Licensing and authorisation

Austria uses a general authorisation. Under TKG 2021 § 6(1), anyone intending to provide a public communications network or offer a public communications service must notify the regulator before starting, changing or ending the activity. Number-independent interpersonal communications services (app-based messaging and calling that does not use numbers) are exempt.

The notification is filed electronically through RTR's e-government system with company details, a short description of the networks or services, the EU member states concerned and the expected start date (§ 6(2)). RTR issues a confirmation within one week of a complete notification and publishes the fact that it was confirmed (§ 6(3)).

MVNOs, which operate on the A1, Magenta or Drei networks, gained share in 2025; RTR counts about 13.8 million SIM cards in use at the end of 2025, excluding machine-to-machine cards (Communications Report 2025).

Operating without notification is an administrative offence punishable by a fine of up to EUR 100,000 (TKG 2021 § 188(6) no. 1).

3 Identity framework (AML rules do not apply)

The Financial Markets Anti-Money Laundering Act (Finanzmarkt-Geldwäschegesetz, FM-GwG) applies only to credit and financial institutions (§ 1(1)). Telecom operators are not obliged entities: they have no AML risk assessment, customer due diligence, beneficial ownership or suspicious transaction reporting duties as telecom providers. A group

company licensed as a payment institution or e-money institution is a financial institution and therefore an obliged entity (FM-GwG § 2 no. 2 letters e and f).

Identity is governed instead by telecom law:

Registration duty

TKG 2021 § 166(2): before the contract is performed, and before the first recharge after 1 September 2019, the provider must establish the user's identity and register the master data needed to identify them, using a suitable identification procedure.

Data to register

The required master data are name, academic degree and date of birth (TKG 2021 § 160(3) no. 5 letters a, b and g). Address is part of master data generally but is not among the identification fields.

Approved methods

The Identification Regulation (Identifikationsverordnung, IVO, BGBl. II No. 7/2019) lists the procedures that are suitable and sufficient. Other procedures may be used if at least equivalent in accuracy, but without reimbursement of costs (IVO § 2).

Purpose limits

Master data may be processed only for the contract, billing, directories and emergency service information (§ 166(1)) and must be deleted once the contract ends, unless still needed for billing, complaints or other legal duties (§ 166(3)).

The duty covers any contract for a communications service, not only prepaid; the explanatory remarks to the 2018 bill that introduced it call for registration before activation. According to the explanatory remarks to TKG 2021 § 166(2), identification is a rule of conduct that does not affect the validity of the contract, and minors can in principle register themselves without a legal representative. There is no ongoing monitoring or re-verification requirement beyond the first recharge rule for older prepaid cards.

4 Identity verification and onboarding

Accepted documents

For a natural person, the default method is personal presentation of an official photo ID (IVO § 3). The IVO borrows the AML law's definition (FM-GwG § 6(2)): a document issued by a state authority with a non-replaceable photograph, name, date of birth, signature and issuing authority. For foreign travel documents, the signature and full date of birth may be missing if the issuing state's law allows.

Remote methods

Where there is no personal contact, the IVO allows two replacements for the in-person check:

- **Bank confirmation** (IVO § 4): electronic confirmation of the subscriber's identity by a credit or financial institution that identified the person under FM-GwG § 6.
- **Photo-ident procedure** (IVO § 5): an automated process on a smartphone, tablet or other internet device with a camera. Every step in § 5(3) to (10) must succeed.

The IVO does not name ID Austria, the national electronic identity. Procedures not listed in the IVO must be at least equivalent in accuracy (IVO § 2). The official ID Austria portal lists several mobile brands among private service providers that use ID Austria, some specifically for SIM card registration.

The photo-ident steps are prescribed in detail. The subscriber enters the SIM card's phone number or IMSI; takes photos or a video of their face while performing requested head or facial movements, to show a live person is present; and captures the relevant pages of the photo ID at the required angle, in quality that allows automated reading. The provider then reads the ID photo's biometric data and the printed data by optical character recognition (OCR), and verifies the document through its optical or holographic security features, the serial number format and the consistency of photo, issue date and date of birth, cross-checking the machine-readable zone where present. Finally it compares the face images with the ID photo biometrically and shows the subscriber a pre-filled master data form to correct and complete.

The process must be aborted if images are unsuitable, the document check or face match fails, or any other inconsistency or uncertainty arises (§ 5(11)).

Business customers and outsourcing

For a legal person, a register extract must show existence, name, legal form and powers of representation, and the person acting for it is identified under §§ 3, 4 or 5 (IVO § 6). A provider may use a processor to run the procedure, but the final responsibility stays with the provider and the allocation of duties must be agreed in writing (IVO § 7).

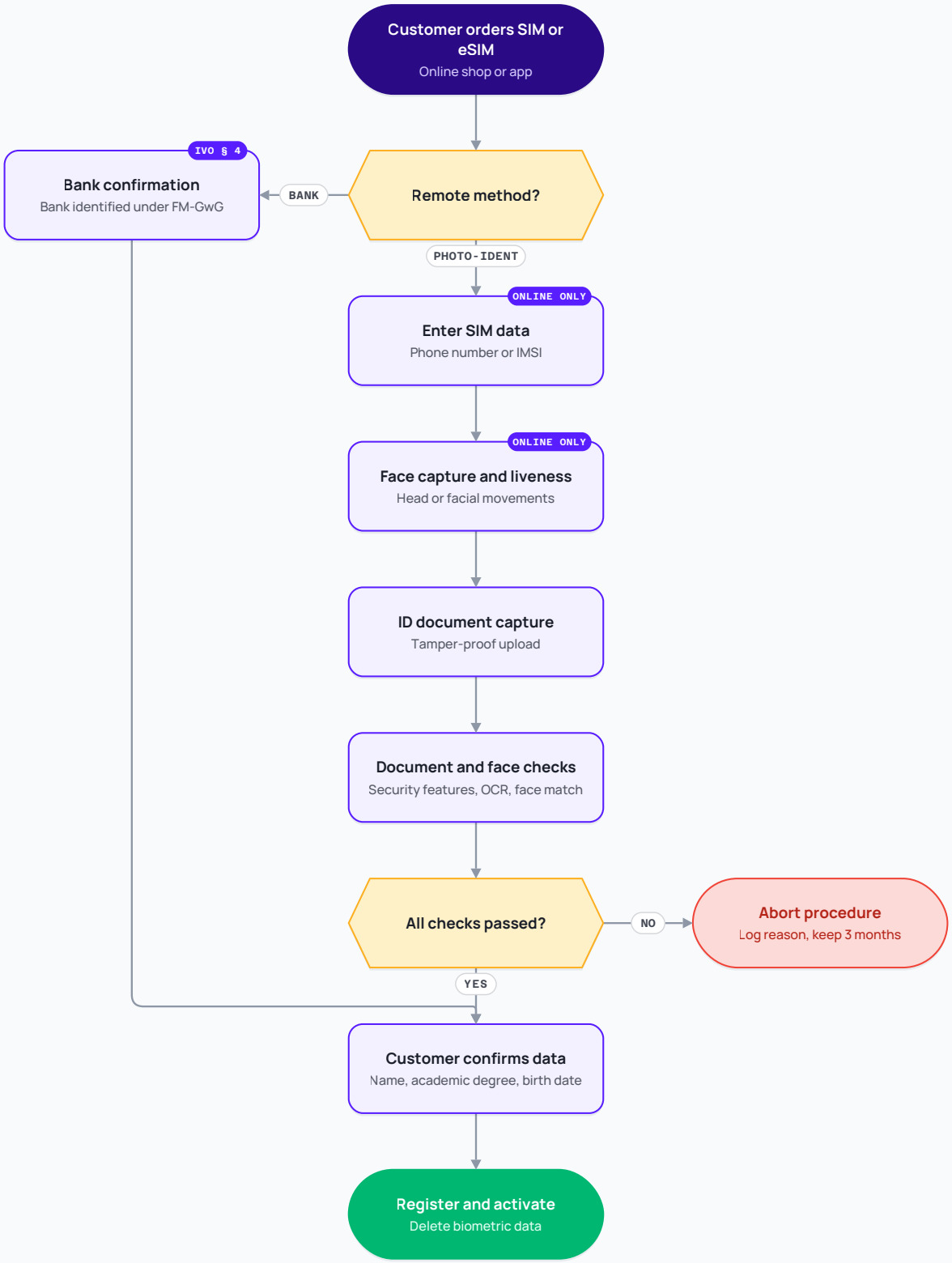


Figure 1. Online SIM or eSIM activation under the Austrian Identification Regulation (IVO).

5 Digital channels: what's different

Bottom line: the duty to identify every subscriber is the same in a shop and online, but online activation must follow the IVO's fixed photo-ident procedure (liveness, document authenticity checks and face matching) or rely on a bank's prior identification.

Requirement	In person / land-based	Online / remote	Difference
Identify before the contract runs	Required (TKG 2021 § 166 (2))	Required (TKG 2021 § 166 (2))	Same
Data registered	Name, academic degree, date of birth	Name, academic degree, date of birth	Same
Method	Official photo ID presented in person	Photo-ident procedure or bank confirmation	Differs
Liveness	Not specified	Head or facial movements on request	Differs
Document checks	Presentation of the ID	Security features, serial number, data consistency, OCR and machine-readable zone	Differs
Biometric face match	Not specified	Mandatory	Differs
Records	Master data	Master data; abort reasons kept 3 months; biometrics deleted at once	Differs
Use of a processor	Provider stays responsible (IVO § 7)	Provider stays responsible (IVO § 7)	Same

A prescribed procedure, not a risk-based one

The IVO does not let operators calibrate checks to risk: each step of § 5 must be carried out with automated support and must succeed, and any uncertainty is a reason to abort.

eSIM and the SIM data step

In photo-ident, the subscriber enters the phone number or IMSI of the SIM that the contract covers (IVO § 5(3)). For eSIM, the profile's number or IMSI must therefore be known before the check starts.

6 Data protection and biometrics

The General Data Protection Regulation (GDPR) applies; the IVO applies without prejudice to it (IVO § 8). The IVO adds limits on photo-ident:

- **Immediate deletion of biometrics.** The provider must delete the biometric data immediately after the procedure ends (IVO § 5(13)).
- **Purpose limitation.** Applications used for photo-ident may not be used for any other purpose and must be protected against unauthorised access (§ 5(13)).
- **Abort logs.** When a procedure is aborted, the reason must be logged and kept for three months for possible dispute resolution (§ 5(12)).
- **Integrity of capture.** Images must be transmitted automatically and protected against alteration (§ 5(6)).

Under TKG 2021, operators must take data security measures in line with GDPR Articles 24, 25 and 32 for each service (§ 163), notify personal data breaches to the Data Protection Authority without delay and, where privacy is likely to be affected, inform the persons concerned (§ 164).

7 Sector-specific obligations

Port-out authentication

TKG 2021 § 119(2) forbids porting without the end user's express consent, given at least in electronic form. For mobile numbers, the NÜV 2022 turns this into a controlled process: a port request can only be made once the number portability information exists (§ 6(1)), and porting always requires proof that the applicant holds the right to use the number (§ 3(8)). Since 3 November 2025, a port may proceed without that information only if the losing provider failed to issue it after two requests and further conditions are met, including written instruction and proof of the right of use, for example by screenshots of SMS or emails or by presenting the SIM card in a shop (§ 6(2)). The gaining provider must refuse such a request where there is doubt about the customer's authority (§ 6(3)).

Caller ID spoofing

Under KEM-V 2009 § 5a, operators that take over calls from foreign networks showing an Austrian caller number must mark them; the destination network must verify that the number is authentic or suppress its display, and may block the call where there are clear signs the call does not come from the signalled subscriber. The rule applied to mobile numbers from 1 September 2024 and to all other numbers from 31 December 2024. Separately, advertising calls may not suppress or falsify the caller number (TKG 2021 § 174(2)).

SMS sender names

The tenth amendment to the KEM-V 2009 (BGBl. II No. 66/2026) created a public RTR register of alphanumeric SMS sender names, open since 1 July 2026 (§ 5b). Mobile providers register names for their customers, stating the owner's name, address and email and, unless obvious, why the name identifies the owner. A name can be used 14 days after entry, and one end user may register no more than 40 names in six months. Since 1 October 2026, only registered names may be used (§ 5(6)). The operator that first injects the message must check the register at least every 24 hours, replace the name with "Unbekannt" (unknown) if it cannot confirm the message is sent for the owner, and discard messages with unregistered names (§ 5c).

Network security

The NISG 2026, in force since 1 October 2026, treats providers of public electronic communications networks or services that are medium-sized enterprises as essential entities, and providers of any size as at least important entities (§ 24). The competent authority is the Federal Office for Cyber Security, which reports directly to the Interior Minister (§ 3a).

8 Risk indicators and red flags

IDENTITY ABUSE AND FRAUD INDICATORS IN AUSTRIAN TELECOM

- **Failed photo-ident signals**: unusable images, failed document authenticity or consistency checks, or a failed face match (IVO § 5(8) and (11)).
- **Port without portability information**: a request relying on screenshots rather than contract documents, especially where the losing provider normally issues the information (NÜV 2022 § 6(3)).
- **Austrian number from abroad**: an incoming foreign call showing an Austrian number that cannot be authenticated (KEM-V 2009 § 5a).
- **Impersonated SMS sender**: messages using a bank or authority name such as "FinanzOnline" that is unregistered or not sent for its owner (KEM-V 2009 § 5c; RTR).
- **SIM farms on stolen identities**: SIM boxes and numbers registered to other people's identities, sold as a crime service (Operation SIMCARTEL, see section 9).
- **"New number" messages**: SMS or WhatsApp messages from someone posing as the recipient's child with a new number, asking for urgent payment (Federal Criminal Police Office).
- **Messaging fraud**: RTR recorded a marked rise in fraud reports in 2025, especially SMS; the Federal Criminal Police Office reports SMS phishing with fake delivery notices and attempts to take over WhatsApp accounts.

9 Enforcement and penalties

Breaches of TKG 2021 are administrative offences, fined per offence by the Fernmeldebüro in six tiers set by § 188: up to EUR 1,000, 5,000, 10,000, 50,000, 75,000 and 100,000. For the higher tiers, an uncollectable fine converts into up to six weeks' detention. The relevant tiers for onboarding and fraud controls are:

Breach	Provision	Maximum fine
Failing to register master data, or doing so without a suitable identification procedure	§ 188(4) no. 25	EUR 50,000

Porting without consent, delaying or misusing a port	§ 188(4) no. 16	EUR 50,000
Suppressing or falsifying caller ID on advertising calls	§ 188(4) no. 27	EUR 50,000
Breaching an RTR regulation (including the KEM-V 2009 and NÜV 2022) or a TKK or RTR decision	§ 188(6) no. 2	EUR 100,000
Operating without notification	§ 188(6) no. 1	EUR 100,000

In setting the fine, the authority considers whether the offence was commercial or repeated, and takes any unlawful gain into account (§ 188(7)). For offences in the two highest tiers, publication of the penalty decision can be ordered where the offender has two earlier convictions for similar offences and is likely to reoffend (§ 189). RTR can also delete SMS sender names that breach the KEM-V 2009, blocking re-entry for one month (KEM-V 2009 § 5b(3)).

Fernmeldebüro penalty decisions are appealed to the Federal Administrative Court (BVwG). In W295 2297643-1 (24 September 2025), it upheld a fine imposed on a company's responsible officer for unsolicited advertising calls (TKG 2021 § 174(1) with § 188(6) no. 9), with the company jointly liable for the costs.

In Operation SIMCARTEL, the Federal Criminal Police Office, investigators from Latvia and Estonia, Europol and Eurojust made seven arrests in Riga on 10 October 2025 and seized more than 1,200 SIM boxes and 40,000 SIM cards. The network sold phone numbers registered to other people's identities in over 80 countries; investigators linked it to more than 3,200 fraud cases, over 1,700 of them in Austria, with losses above EUR 4.5 million (Cybercrime Report 2025).

10 Recent changes and what to watch

- **1 October 2026** `In force` SMS sender-name rules (KEM-V 2009 §§ 5(6) and 5c) apply: unregistered alphanumeric senders must be discarded. Businesses sending SMS under a brand name need a registered entry.
- **1 October 2026** `In force` NISG 2026 applies: telecom providers face a new cybersecurity regime and supervisor; TKG 2021 § 44 was amended to match.
- **14 September 2026** `Bill, not enacted` Government bill 594 d.B., amending the Gambling Act and TKG 2021, went to the National Council's Finance Committee. It would

let the TKK order internet access providers to block or redirect illegal gambling sites, with a compliance deadline of no more than two weeks; the TKG changes are drafted to take effect at the end of 31 December 2026.

- **3 November 2025** `In force` NÜV 2022 amendments (BGBl. II No. 164/2025) on keeping the old contract and on porting without portability information.
- **1 September and 31 December 2024** `In force` Anti-spoofing duties for calls (KEM-V 2009 § 5a) applied to mobile and then all Austrian numbers.

11 What this means for identity verification

- **Follow the IVO steps exactly.** An online flow that skips any IVO § 5 step, such as active liveness or the machine-readable zone cross-check, does not meet the photo-ident standard.
- **Documents.** Accept state-issued photo IDs meeting the FM-GwG § 6 (2) criteria, including foreign passports.
- **Alternative routes.** A bank's electronic identity confirmation is a lawful substitute; any other method, such as ID Austria, must be at least as accurate as the IVO methods.
- **Minimal data, short retention.** Register name, academic degree and date of birth; delete biometrics immediately; keep abort reasons for three months; delete master data after the contract ends.
- **Re-verification triggers.** There is no periodic re-check, but number porting needs proof of the right of use, and a port requested without portability information must be refused if the customer's authority is in doubt.
- **Vendor contracts.** A processor running photo-ident must meet IVO standards under a written agreement; the operator stays responsible.

IDENTOMAT

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:

- Remote SIM and eSIM onboarding with ID document capture and verification, including security-feature checks and machine-readable zone reading.
- Biometric liveness detection and face match against the ID photo, as the photo-ident procedure requires.
- Configurable no-code workflows that abort and log failed checks, with an audit trail for each verification.
- KYB and representative verification for business customers, and phone and email verification for account and porting flows.
- Cloud, on-premises or hybrid deployment to fit operators' data protection and retention requirements.

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 2021 (TKG 2021) [Telecommunications Act 2021], BGBl. I No. 190/2021**, §§ 6, 44, 119, 160, 163 to 166, 174, 188, 189, 217, consolidated version of 11 November 2026, RIS, ris.bka.gv.at
- **Identifikationsverordnung (IVO) [Identification Regulation], BGBl. II No. 7/2019**, §§ 1 to 8, consolidated version of 11 November 2026, RIS, ris.bka.gv.at
- **Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V 2009) [Communications Parameters, Fees and Value-Added Services Regulation 2009]**, §§ 3, 5, 5a, 5b,

5c, 128, as amended by BGBl. II No. 66/2026, consolidated version of 11 November 2026, RIS, ris.bka.gv.at

- **Nummernübertragungsverordnung 2022 (NÜV 2022) [Number Portability Regulation 2022], BGBl. II No. 184/2022**, as amended by BGBl. II No. 164/2025, consolidated version of 11 November 2026, RIS, ris.bka.gv.at
- **Finanzmarkt-Geldwäschegesetz (FM-GwG) [Financial Markets Anti-Money Laundering Act]**, §§ 1, 2 and 6, consolidated version of 11 November 2026, RIS, ris.bka.gv.at
- **Sanktionengesetz 2024 (SanktG 2024) [Sanctions Act 2024]**, § 12, consolidated version of 11 November 2026, RIS, ris.bka.gv.at
- **Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) [Network and Information Systems Security Act 2026], BGBl. I No. 94/2025**, §§ 3, 3a, 24, consolidated version of 11 November 2026, RIS, ris.bka.gv.at
- **Government bill 594 d.B. (XXVIII. GP), Bundesgesetz, mit dem das Glücksspielgesetz und das Telekommunikationsgesetz 2021 geändert werden** [amending the Gambling Act and TKG 2021], Parliament of Austria, status as of 14 September 2026, parlament.gv.at
- **RTR, SMS-Regulierung [SMS regulation]**, information page, RTR, rtr.at
- **RTR, 10. Novelle der KEM-V: Neue Regulierung unterbindet Betrug mit alphanumerischen SMS-Absenderkennungen**, RTR.Telekom.Post Newsletter 01/2026, 10 April 2026, rtr.at
- **RTR, 9. Novelle der KEM-V 2009 [ninth amendment, anti-spoofing]**, 20 December 2023, with explanatory notes, rtr.at
- **Bundesministeriengesetz 1986 (BMG) [Federal Ministries Act]**, Annex, part B no. 9, consolidated version of 11 November 2026, RIS, ris.bka.gv.at
- **Federal Ministry for Housing, Arts, Culture, Media and Sport, Das Fernmeldebüro**, bmwkms.gv.at; Fernmeldebüro, fb.gv.at
- **Regierungsvorlage 1043 d.B. (XXVII. GP), Erläuterungen [explanatory remarks to TKG 2021]**, remarks on § 166(2), Parliament of Austria, parlament.gv.at
- **Regierungsvorlage 15 d.B. (XXVI. GP), Erläuterungen [explanatory remarks to the 2018 amendment introducing TKG 2003 § 97(1a)]**, Parliament of Austria, parlament.gv.at
- **Bundesverwaltungsgericht (Federal Administrative Court), W295 2297643-1, 24 September 2025**, appeal against a Fernmeldebüro penalty decision, RIS, ris.bka.gv.at
- **Bundeskriminalamt, Cybercrime Report 2025**, Federal Ministry of the Interior, 2026, sections 2.6, 3.3 and 4.3, bundeskriminalamt.at
- **ID Austria, Private ID Austria Service Provider**, official list, id-austria.gv.at
- **RTR, Kommunikationsbericht 2025 [Communications Report 2025]**, III-379 d.B. (XXVIII. GP), section 6.2 (p. 171) and section 6.3, parlament.gv.at