



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Estonia

COUNTRY **Estonia**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Consumer Protection and Technical Regulatory Authority · Information System Authority · Data Protection Inspectorate**

Key takeaways

- Anyone may offer telephone, mobile or internet services in Estonia after filing an economic activity notice; a radio frequency licence or a numbering licence is needed only when the service uses spectrum or Estonian numbers.
 - Estonia has no SIM registration law. Anonymous prepaid SIM cards are lawful, while an operator may refuse a contract to an applicant who does not provide identification data. The law does not prescribe how identity is checked, in a shop or online.
 - Telecom operators are not covered by the anti-money laundering (AML) law, so there are no customer due diligence or suspicious transaction reporting duties for the telecom service itself.
 - Digital channels change number porting more than onboarding: from 1 November 2026 a mobile number moves on the next working day after the customer has the new SIM card, eSIM ports move fastest, and customers must receive text message updates throughout.
 - Expect change: a bill before Parliament would end blanket retention of call and location data (proposed for 1 December 2026, not yet law), and caller ID spoofing rules apply from 1 April 2027.
-

The Estonian market is open to new entrants, including mobile virtual network operators (MVNOs) and app-based providers: market entry is by notification rather than licence, and online sales of SIM cards and eSIM profiles are not restricted.

The Consumer Protection and Technical Regulatory Authority (TTJA) regulates electronic communications, the Information System Authority (RIA) supervises cybersecurity, and the Data Protection Inspectorate handles personal data breaches.

The biggest obstacle for a new network operator is not identity verification but security approval: hardware and software used in the network needs a TTJA permit on national security grounds, and larger operators carry the heaviest cybersecurity duties.

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

Estonia is a unitary state, so every telecom rule and authorisation is national. The Electronic Communications Act (elektroonilise side seadus, ESS) is the core statute; the Cybersecurity Act (küberturvalisuse seadus, KÜTS) adds network and information security duties.

Authority	Remit in telecom	Level	Official site
Consumer Protection and Technical Regulatory Authority (Tarbijakaitse ja Tehnilise Järelevalve Amet, TTJA)	Supervision under the ESS; frequency and numbering licences; number portability database; national security permits for network equipment; out-of-court processor of most ESS misdemeanours	National	ttja.ee
Information System Authority (Riigi Infosüsteemi Amet, RIA)	Cybersecurity Act supervisor; receives incident reports; gives opinions on network hardware and software; runs the national electronic identity (eID) infrastructure	National	ria.ee
Data Protection Inspectorate (Andmekaitse Inspektsioon)	Notification of personal data breaches by communications undertakings; data protection supervision	National	aki.ee

Ministry of Justice and Digital Affairs	Telecom policy and regulations; manages radio frequencies and numbering together with TTJA	National	justdigi.ee
Estonian Competition Authority (Konkurentsiamet)	General competition law only	National	konkurentsiamet.ee

Security authorities, the police and prosecutors have statutory access powers but do not license or supervise the sector.

2 Licensing and authorisation

Any person may start providing a communications service. Under ESS §§ 3 and 4, a provider of a publicly available electronic communications service submits an economic activity notice (majandustegevusteade) describing the service, its geographic area and its website, filed only through the Estonian information gateway or a notary. TTJA forwards the notice to the Body of European Regulators for Electronic Communications (BEREC). Providers of number-independent interpersonal communications services, such as many messaging apps, are exempt from the notice.

Two individual authorisations sit on top of the notice (ESS § 3(3)): a frequency licence from TTJA when the service needs radio spectrum, and a numbering licence when the provider uses Estonian numbers. An MVNO that uses a host network's spectrum but its own number range therefore needs the notice and a numbering licence, not a frequency licence. Frequency licences for mobile broadband bands are awarded by public competition, for which the minister may set a one-off fee of up to EUR 3,000,000 (ESS § 9¹, version in force October 2026).

National security permit for network equipment

ESS §§ 87³ to 87⁵ require every communications undertaking to notify TTJA of the hardware and software used in its network and to obtain a usage permit for it. TTJA asks the security authorities and RIA whether the equipment threatens national security; equipment from a supplier based outside the EU, NATO or the OECD weighs against approval. A permit runs for eight years, and operators subject to these duties commission an independent audit every three years, carried out by a certified information systems auditor.

Providers established outside Estonia

Since 19 July 2026, a provider established outside the EU that offers electronic communications services in Estonia must appoint a legal representative in the EU for criminal-evidence orders, and an Estonian provider active in other member states must designate an establishment or representative (ESS § 4¹, transposing Directive (EU) 2023/1544). TTJA supervises this duty.

3

Identity framework (AML rules do not apply)

The Money Laundering and Terrorist Financing Prevention Act (rahapesu ja terrorismi rahastamise tõkestamise seadus) lists its obliged entities in § 2: credit and financial institutions, gambling operators, real estate intermediaries, traders accepting cash payments of EUR 10,000 or more, and several professions. Communications undertakings are not on the list. A telecom operator therefore has no AML customer due diligence, beneficial ownership or suspicious transaction reporting duties for its telecom service, although it falls within the Act for any listed activity it also carries out, such as accepting a cash payment of EUR 10,000 or more as a trader.

Customer identity in telecom is governed instead by the ESS, and the Act deliberately leaves room for anonymity:

Contract customers

An operator offering a network connection must conclude a contract with any applicant, but may refuse when the applicant has not provided the data needed to identify them or gives false data (ESS § 93(2)). The Act sets no list of documents or verification method.

Anonymous prepaid

The ESS expressly recognises anonymous prepaid mobile service. For it, the operator records the date, time and cell of first activation (ESS § 111¹(2)(10)), and the number cannot be ported out if the customer cannot be identified.

SIM and device integrity

Cloning or altering a SIM card is prohibited, a SIM may be used only on the terms of the subscription contract, and only the manufacturer or its authorised agent may change a handset's IMEI code (ESS § 87¹).

Retained identity data

Telephone and mobile operators must keep subscriber name and address with each number, plus IMSI and IMEI identifiers, for one year (ESS § 111¹(2) and (4)), and answer authorised requests within ten hours if urgent (ESS § 112).

Sanctions screening is a general obligation under directly applicable EU sanctions regulations rather than a telecom-specific duty, and the ESS adds no screening requirement of its own.

4 Identity verification and onboarding

Because the ESS prescribes no accepted documents, no assurance level and no biometric check, identity verification in Estonian telecom is a business and fraud-risk decision for the operator, bounded by three legal points: the right to refuse a contract when identification data is missing or false, the duty to keep the subscriber data linked to each number, and the porting rules that tie a number transfer to an identified customer.

In practice the operator chooses the method. Estonia's state eID tools (the ID card, Mobile-ID and the digital ID) support remote identification and qualified signatures, and Mobile-ID itself depends on the operator's SIM: RIA has announced that, because of the revised EU eIDAS Regulation, Mobile-ID users must replace their SIM card before 19 May 2027 to keep using the service, and Mobile-ID must then be activated again on the new card.

Number porting as an identity control

Porting is where Estonian telecom law most directly protects against account takeover. Under Regulation No. 44 on number portability as amended by Regulation No. 23 of 16 June 2026 (in force 1 November 2026), the recipient operator files the porting request through the central number booking database only after the customer has received the new SIM card, the donor operator confirms within one working hour, and the number moves at 03:00 on the next working day. The recipient operator must keep the customer informed by text message from the start of the process through each stage. A port is refused if the customer has no contract for the number, gives incomplete or false information, or uses a prepaid card and cannot be identified (Regulation No. 44, § 4).

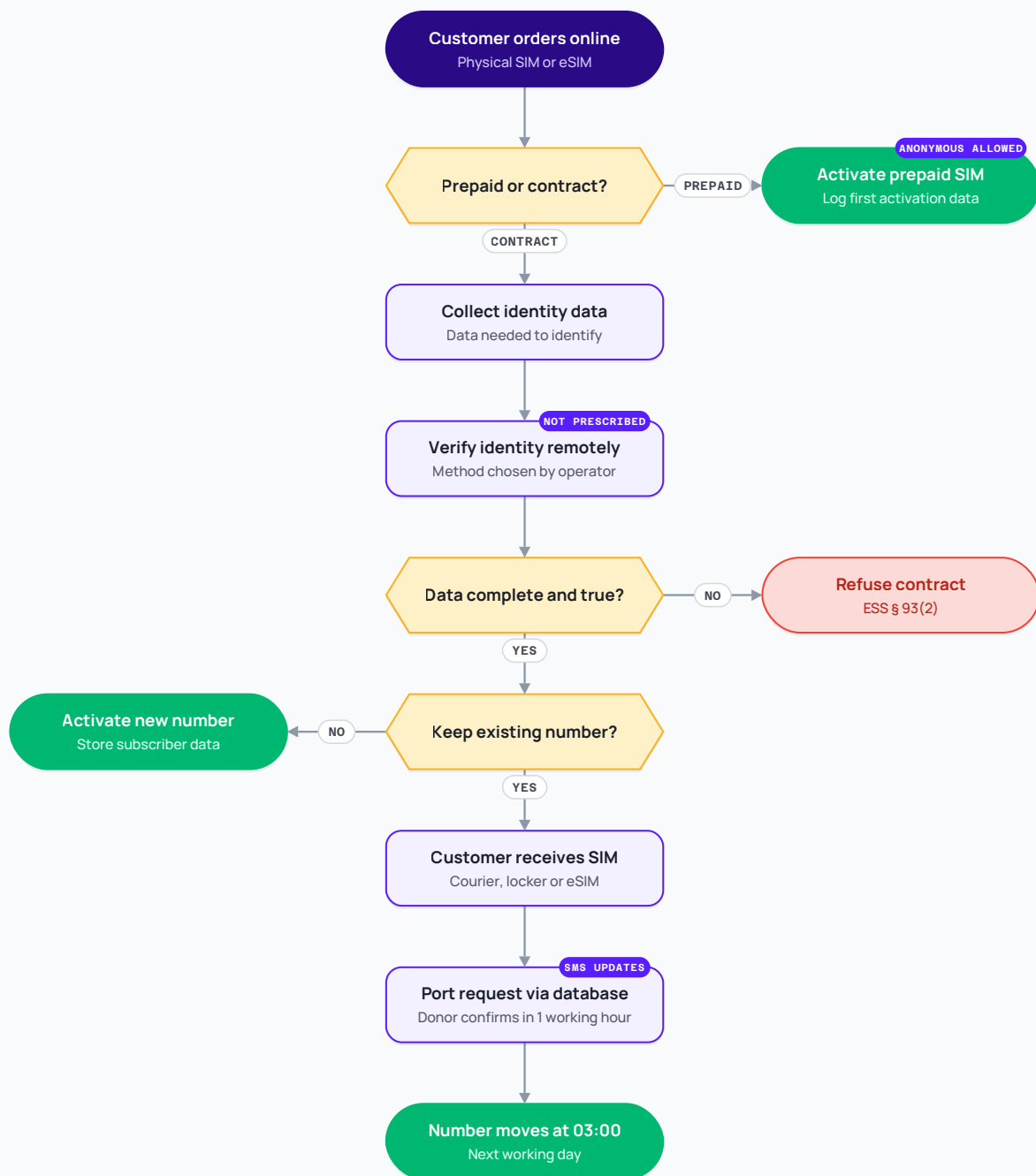


Figure 1. Online SIM or eSIM onboarding with number porting in Estonia (rules from 1 November 2026).

Bottom line: Estonian telecom identity rules are channel-neutral, but number porting is not: from 1 November 2026 the porting clock starts when the customer has the new SIM card, so an eSIM sold online ports faster than a physical card sent by courier.

Requirement	In person / shop	Online / remote	Difference
Authorisation to sell service	Economic activity notice	Economic activity notice	Same
Identity data for a contract	May refuse if missing or false	May refuse if missing or false	Same
Verification method	Not prescribed	Not prescribed	Same
Anonymous prepaid	Permitted	Permitted	Same
Activation records	Time and cell of first use	Time and cell of first use	Same
When porting can start (from 1 Nov 2026)	SIM handed over in the shop	After SIM delivery, or at once for eSIM	Differs
Customer notification of port	Text messages at each stage	Text messages at each stage	Same

Remote onboarding is permitted without a prescribed method

Nothing in the ESS requires a customer to appear in person, and the refusal ground in § 93(2) applies to any channel. An operator selling online may choose document capture, an eID login, a qualified signature or a combination, and may also sell anonymous prepaid service online. The law sets no tiered limits on anonymous service.

The SIM in the customer's hands is the porting trigger

The amended Regulation No. 44 links the porting request to the customer having the recipient operator's SIM card. The Ministry of Justice and Digital Affairs explains that when the customer starts the port by phone or self-service, the SIM is sent by courier or parcel locker and the number moves early on the next working day after collection, while an eSIM

can be delivered digitally at once, so the number moves on the night after the donor confirms. For a digital MVNO, delivery logistics therefore set the porting timeline.

Spoofed calls and text messages

Government Regulation No. 93 of 2 October 2026 **Adopted, effective 1 Apr 2027** prohibits call traffic with false or unauthorised caller numbers, including international calls showing an Estonian number without a legal basis, and requires number-based communications providers to take reasonable measures to detect and, where possible, block it. Mobile operators must also take proportionate measures so that a text message sender number is valid, attributable to the sender, or used by someone entitled to it.

6 Data protection and biometrics

The EU General Data Protection Regulation applies directly to identity data captured at onboarding. The ESS adds a sector layer on top of it.

Confidentiality. Operators must keep confidential all data learned in providing the service, including usage details and the time and manner of messages, and may disclose it only to the customer, to third parties with the customer's consent, or under the statutory request powers (ESS § 102).

Breach notification. A communications undertaking must notify the Data Protection Inspectorate of a personal data breach at the first opportunity, notify affected customers where the breach may harm their data or privacy unless it proves the data was rendered unintelligible, and keep a register of breaches (ESS § 102¹).

Biometrics. Neither the ESS nor the number portability rules mention biometric checks. An operator that adds a selfie match or liveness check to online onboarding does so under the general data protection regime, which treats biometric data used to identify a person as a special category requiring a specific legal basis, and should be able to justify why a less intrusive method would not do.

Retention. Subscriber, traffic and location data listed in ESS § 111¹ must currently be kept for one year within the EU. The Supreme Court has held that this blanket retention conflicts with EU law and that the traffic and location data may not be requested for criminal investigations, though subscriber identity queries are unaffected; a replacement regime is before Parliament (see section 10).

Cybersecurity Act duties

Public electronic communications network and service providers fall within the Cybersecurity Act. Those with 50 or more employees and an annual turnover or balance sheet above EUR 10 million are essential entities; smaller providers are important entities (KüTS § 3). Each must register with RIA, apply security measures, and report significant incidents: an early notice within 24 hours of becoming aware, an incident report within 72 hours, and a final report within one month of the incident report (KüTS § 8). Since 16 October 2026 the Act also covers near-miss incidents in its voluntary reporting and incident register.

Emergency access and caller location

Providers of number-based interpersonal communications must route free calls to the emergency number 112 and pass the caller's number, IMEI and location to the Emergency Response Centre (ESS § 88). Mobile operators must deliver public warning messages to all devices in a defined area, and from 1 October 2026 designated vital mobile operators must be ready to provide national roaming to each other's customers in a declared emergency or state of war (ESS §§ 105¹ and 88¹).

Lawful access

Operators must give surveillance and security authorities real-time network access, keep the related logs and requests for five years, and enable real-time location of mobile devices for the police (ESS §§ 112 and 113). Interception costs are compensated; retention costs are not (ESS §§ 111¹(10) and 114).

Risk indicators and red flags

TELECOM FRAUD AND IDENTITY-ABUSE INDICATORS

- **Spoofed national numbers:** international calls presenting an Estonian caller number without a legal basis.
- **Hidden call origin:** routing that conceals where a call really starts, or international calls handed on domestically without controls.
- **Spoofed text senders:** messages whose sender number is invalid or not linked to the real sender.
- **Cloned or altered SIMs:** one identity module appearing in parallel, or SIM use outside the contract terms.
- **Changed IMEI codes:** devices whose equipment identity has been altered by someone other than the manufacturer.
- **Port requests without the SIM:** pressure to move a number before the customer holds the new SIM card.
- **Mobile-ID SIM replacement lures:** contacts exploiting the 2027 SIM swap to get users to confirm actions they did not start.

Enforcement and penalties

TTJA enforces the ESS through precepts and as the out-of-court processor of most ESS misdemeanours (ESS § 188(3)). Fines are set per offence, with separate maximums for individuals (in fine units) and for legal persons (in euros):

Breach	Provision	Maximum for a legal person
National security duties for network equipment and audits	ESS § 170 ³	EUR 50,000
Number portability requirements	ESS § 164	EUR 3,200
Data retention duties	ESS § 184 ¹	EUR 3,200
Confidentiality of customer data, or failure to notify a breach	ESS § 187	EUR 2,000

Cybersecurity duties, essential entity	KüTS § 18 ²	EUR 10 million or 2% of global turnover, whichever is higher
Cybersecurity duties, important entity	KüTS § 18 ³	EUR 7 million or 1.4% of global turnover, whichever is higher

The cybersecurity fines cover security measures and every reporting step, so an operator's largest financial exposure now sits in the Cybersecurity Act rather than the ESS.

10 Recent changes and what to watch

- **Data retention bill 1007 SE** *Bill, first reading completed 1 Oct 2026* : would replace blanket retention with retention of subscriber-identification and IP data only, a six-month quick-freeze order, and government-ordered targeted retention for serious crime or national security; proposed entry into force 1 December 2026, with parts in 2027 and 2028.
- **Cybersecurity Act amendment, 16 October 2026** *In force* : redefines a cyber incident and adds near-miss incidents to voluntary reporting and to RIA's incident register.
- **Caller and sender spoofing rules, Regulation No. 93** *Adopted, effective 1 Apr 2027* : operators must detect and where possible block spoofed calls and take measures on spoofed text message senders.
- **Faster number porting, Regulation No. 23** *Adopted, effective 1 Nov 2026* : mobile ports move on the next working day after SIM receipt, with one-hour response times and text message updates to the customer.
- **Mobile-ID SIM replacement** *Deadline 19 May 2027* : users must switch to a new SIM to keep Mobile-ID, a high-volume SIM change that operators need to authenticate carefully.
- **EU representative for e-evidence, ESS § 4¹** *In force since 19 Jul 2026* : non-EU providers serving Estonia must name an EU legal representative.
- **NIS2 transposition** *In force since 1 Jan 2026* : telecom providers became essential or important entities with 24-hour, 72-hour and one-month reporting.

11 What this means for identity verification

No mandated standard, so the design is the operator's. With no SIM registration law and no prescribed method, the verification level for contract customers is a risk choice. The

legal anchors are the right to refuse where identification data is missing or false, and the duty to keep accurate subscriber data linked to each number for one year.

Plan for anonymous and identified customers in parallel. Anonymous prepaid remains lawful, and the pending retention bill would keep it while requiring operators to store end-user data where they hold it. Products should be able to upgrade an anonymous customer to an identified one, because porting out and many contract features depend on identification.

Treat the SIM handover as a verification point. From 1 November 2026 the port starts once the customer holds the new SIM. For online sales, confirming the recipient's identity at courier delivery, at parcel-locker collection or before issuing an eSIM profile is the practical defence against fraudulent ports, alongside the mandatory text message updates.

Use biometrics only where justified. Face match and liveness detection are lawful but not required; record the legal basis and limit image retention.

Re-verification triggers. Port-out requests, SIM replacements (including the Mobile-ID SIM change before 19 May 2027), eSIM transfers and changes of contact details are the events where a fresh identity check does most to prevent account takeover.

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 identity verification for contract and eSIM customers, with ID document capture (including NFC), face match and biometric liveness.
- Re-verification before port-out, SIM replacement or eSIM transfer to reduce account takeover risk.
- Phone and email verification at signup and before sensitive account changes.
- No-code workflow builder to run anonymous prepaid and identified contract journeys side by side, with an audit trail for each check.

[Request a meeting](#)

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

- **Elektroonilise side seadus [Electronic Communications Act]**, consolidated text in force 1 to 31 October 2026, RT I, 11.07.2026, 85, §§ 3, 4, 4¹, 9¹, 87¹, 87³ to 87⁵, 88, 88¹, 89, 93, 102, 102¹, 111¹, 112 to 114, 164, 170³, 184¹, 187, 188, Riigi Teataja, riigiteataja.ee
- **Elektroonilise side seadus [Electronic Communications Act]**, consolidated text from 1 November 2026, Riigi Teataja, riigiteataja.ee
- **Nõuded numbri liikuvuse tagamiseks sideettevõtja vahetamisel [Requirements for number portability when changing operator]**, Regulation No. 44 of 14 June 2011, consolidated text RT I, 05.10.2021, 5, §§ 3 to 6, Riigi Teataja, riigiteataja.ee
- **Regulation No. 23 of 16 June 2026 amending Regulation No. 44**, RT I, 01.07.2026, 2, in force 1 November 2026, Riigi Teataja, riigiteataja.ee
- **Government Regulation No. 93 of 2 October 2026 amending Regulation No. 140 (Requirements for communications services and technical requirements for networks)**, RT I, 07.10.2026, 3, in force 1 April 2027, Riigi Teataja, riigiteataja.ee
- **Küberturvalisuse seadus [Cybersecurity Act]**, consolidated text from 16 October 2026, RT I, 06.10.2026, 2, §§ 3, 3¹, 8, 18² and 18³, Riigi Teataja, riigiteataja.ee
- **Küberturvalisuse seaduse muutmise seadus [Act amending the Cybersecurity Act]**, passed 23 September 2026, RT I, 06.10.2026, 1, Riigi Teataja, riigiteataja.ee
- **Rahapesu ja terrorismi rahastamise tõkestamise seadus [Money Laundering and Terrorist Financing Prevention Act]**, English translation of the text in force from 21 July 2026, § 2, Riigi Teataja, riigiteataja.ee
- **Bill 1007 SE, Act amending the Code of Criminal Procedure, the Code of Misdemeanour Procedure, the Electronic Communications Act and other Acts (retention and use of communications data)**, initiated 14 September 2026, bill text and explanatory memorandum, Riigikogu, riigikogu.ee
- **Valitsus kiitis heaks sideandmete eelnõu [Government approves communications data bill]**, Ministry of Justice and Digital Affairs, 27 August 2026, justdigi.ee
- **Mobiilioperaatori vahetus saab peagi toimuda tundidega [Changing mobile operator will soon take hours]**, Ministry of Justice and Digital Affairs, 2026, justdigi.ee
- **Riigikohus: riik ei saa sidefirmade kogutud andmeid kuritegude uurimiseks välja nõuda [Supreme Court: the state cannot demand data retained by telecom firms to investigate crimes]**, Supreme Court of Estonia, 18 June 2021, case 1-16-6179, riigikohus.ee
- **RIA: Mobile-ID users will need to replace their SIM cards to continue using the service**, Information System Authority, August 2026, ria.ee