



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in France

COUNTRY **France**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **29 October 2026**

KEY REGULATORS **Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) · Commission nationale de l'informatique et des libertés (CNIL)**

Key takeaways

- No licence or prior registration is needed to provide mobile or internet services to the public in France, but every operator must follow the rules of the French electronic communications code, the Code des postes et des communications électroniques (CPCE), supervised by the telecoms regulator, Arcep.
- Operators must collect and keep each subscriber's civil identity (name, date and place of birth, addresses, email and phone numbers) for five years after the contract ends, and since a June 2025 law this also covers prepaid services.
- The same 2025 law requires operators to verify that identity. The decree that will set the accepted verification methods has not been published (as of October 2026), but failing to verify has been a criminal offence since 13 June 2026.
- Online and eSIM sales are allowed on the same identity rules as shop sales; the main online differences are the 14-day withdrawal right for distance contracts and how payment evidence is recorded.
- Telecom operators are not covered by French anti-money laundering (AML) law, but number spoofing and porting fraud are regulated directly: calls must carry authenticated caller numbers, and number porting needs the subscriber's personal operator code (RIO).

The French market is open to new entrants, including mobile virtual network operators (MVNOs) and fully digital brands selling SIM and eSIM subscriptions online. Arcep regulates the sector, the data protection authority CNIL enforces the security of subscriber data, and the national cybersecurity agency ANSSI sets security orientations for operators.

The biggest obstacle for a new entrant is the identity verification duty added in 2025: it is already enforceable, yet the decree that will define how verification must be done is still awaited. Onboarding flows built now need to verify identity reliably and be ready to adapt once the decree appears.

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 identity and onboarding	Level	Official site
Arcep	Sector regulator: numbering plan, number portability, caller-number authentication, investigations and sanctions under the CPCE	National	arcep.fr
CNIL	Data protection: security and retention of subscriber data, biometric processing, breach notification	National	cnil.fr
ANSSI	Cybersecurity orientations that operators must follow under art. L33-1 I e) CPCE	National	cyber.gouv.fr
DGCCRF	Consumer protection: distance contracts, withdrawal right, telecom consumer contract rules	National	economie.gouv.fr/dgccrf
European Union	European Electronic Communications Code (transposed into the CPCE), GDPR and the eIDAS Regulation on digital identity wallets	Supranational	eur-lex.europa.eu

Judicial authorities, police and emergency services may access operators' complete, up-to-date subscriber lists for judicial missions or emergencies (art. L33-1 V CPCE).

Licensing and authorisation

Under article L33-1 I of the CPCE (version in force since 11 March 2023), establishing and operating public networks and providing electronic communications services to the public "sont libres", subject to rules on security and integrity (including incident notification), confidentiality, lawful interception, emergency calls, user information and control by Arcep. The version in force until 28 May 2021 made this freedom subject to a prior declaration to Arcep; ordonnance n° 2021-650 of 26 May 2021, which transposed the European Electronic Communications Code, removed that requirement. A fixed or mobile operator, including an MVNO, is now an operator by virtue of the activity it carries on.

Telephone numbers are allocated by Arcep from the national numbering plan, which it establishes and manages (art. L44 I CPCE), and each allocation carries an annual tax set by the same article. Operators holding numbers must offer number portability (art. L44-4 CPCE). Use of radio frequencies requires an authorisation granted by Arcep (art. L42-1 CPCE).

Identity framework (AML rules do not apply)

Electronic communications operators are not among the persons subject to the French AML and counter-terrorist financing regime listed in article L561-2 of the Code monétaire et financier (version in force since 5 August 2026). They have no customer due diligence, beneficial ownership or suspicious transaction reporting duties under that regime.

Subscriber identity is instead governed by the data retention provisions of the CPCE, which serve criminal procedure, public security and national security purposes:

Civil identity, five years

Operators must keep the user's civil identity until five years after the end of the contract or of the prepaid interpersonal communications service (art. L34-1 II bis 1° CPCE).

Verification duty

The same provision, as amended by loi n° 2025-532 of 13 June 2025, provides that a Conseil d'État decree sets the conditions in which operators verify civil identity data.

In force, decree pending

Account and payment data, one year

Other information given at subscription or account creation, and payment information, is kept until one year after the contract ends or the account is closed (art. L34-1 II bis 2°).

Connection data, one year

Technical data identifying the source of a connection or the terminal used is kept for one year from the connection, for serious crime and security purposes (art. L34-1 II bis 3°).

Where national security faces a serious threat, the Prime Minister may also order operators by decree to retain traffic and location data (R10-13 V) for one year (art. L34-1 III). The current order, décret n° 2026-920 of 30 September 2026, applies from 21 October 2026.

The 2025 amendment added prepaid services and the verification duty. The amendment followed a Senate inquiry finding that drug traffickers make massive use of prepaid SIM cards to stay undetectable. In decision n° 2025-885 DC of 12 June 2025, the Conseil constitutionnel held that the provision was adopted by a constitutional procedure; it did not rule on its substance.

4

Identity verification and onboarding

Data to collect

Article R10-13 I of the CPCE (in force since 21 October 2021, décret 2021-1361) defines the civil identity that must be kept: surname, first name, date and place of birth (for a company account, the company name and the same details for the person acting for it); postal addresses; email addresses of the user and associated accounts; and phone numbers. Article R10-13 II adds the login identifier, pseudonyms and the latest data used to verify or change the password, including through a two-factor system.

How identity must be verified

The CPCE does not yet list accepted documents or remote methods. Article L34-1 II bis 1° leaves this to a decree, which will also name the State services exempt from verification. The decree had not been published as of October 2026. No French telecom rule names identity documents, liveness checks or certified providers, or prescribes an identity assurance level.

Until the decree appears, a defensible approach is to check an identity document against the person (online, by document capture with face match and liveness) and keep evidence of the check, while minimising the data stored.

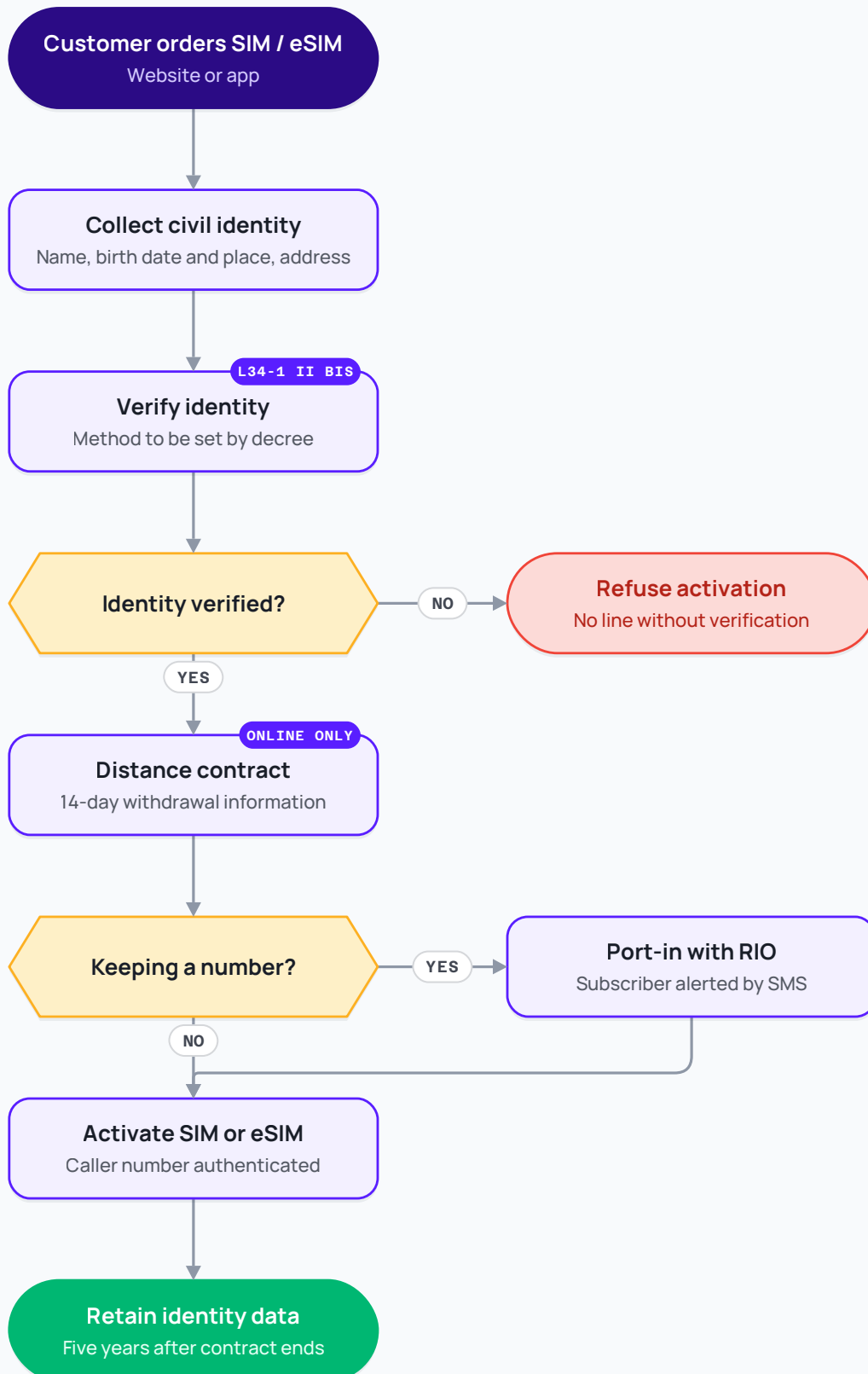


Figure 1. Online SIM or eSIM subscription and number porting in France.

Number porting as an identity control

Porting is driven by the relevé d'identité opérateur (RIO), a code attached to each number. Under Arcep decision n° 2022-2148 of 6 December 2022 (published in the Journal officiel on 5 May 2023), a mobile subscriber obtains the RIO by calling the free number 3179 from the line itself; the receiving operator checks the RIO's format and key before sending the request, and porting messages to residential subscribers must tell anyone who did not request the porting to contact their operator. Arcep states that the RIO aims to limit wrongful porting. The receiving operator handles the request and the port terminates the old contract (art. L44-4 CPCE).

5 Digital channels: what's different

Bottom line: the identity rules are channel-neutral, so a SIM or eSIM can be sold entirely online, but the online operator must still verify identity remotely without a prescribed method, and distance-selling rules change the contract and porting timeline.

Requirement	In person / shop	Online / remote	Difference
Permission to sell and activate	Free provision of services (L33-1)	Same; no channel restriction	Same
Civil identity collected	R10-13 I data set	Same data set	Same
Identity verification	Required; method set by future decree	Required; method set by future decree	Same
Payment evidence kept	Type, reference, amount, plus date, time and place	Type, reference and amount	Differs
Withdrawal right	No statutory withdrawal right	14 days from conclusion of the contract	Differs
Porting a number	RIO from 3179; one working day	RIO from 3179; porting starts after the withdrawal period unless the customer asks otherwise	Differs

Identity data retention	Five years after contract ends	Five years after contract ends	Same
Biometric data	Special-category data under GDPR art. 9 if used	Same; explicit consent and a non-biometric alternative	Same

Remote verification with no prescribed method

Article L34-1 II bis 1° applies whatever the sales channel, and the criminal offence in article L39-3 I 3° (failing to verify and keep civil identity data) has applied since 13 June 2026 even though the implementing decree is still awaited. Online, the operator chooses its own remote method and must be able to show that it verified the person.

Distance contracts and porting

A consumer has 14 days to withdraw from a contract concluded at a distance, running from conclusion for service contracts (art. L221-18 Code de la consommation). Arcep decision n° 2022-2148 provides that where a withdrawal right applies, the one-working-day porting time starts only once it expires, unless the subscriber expressly asks otherwise. An online port-in therefore takes longer by default than one signed in a shop.

What is changing

The verification decree **Adopted, decree not yet published** will set the verification conditions for all sales channels. Separately, Regulation (EU) 2024/1183 requires larger private providers, explicitly including telecommunications, that must use strong user authentication for online identification to accept European Digital Identity Wallets at the user's request by 24 December 2027; use of the wallet stays voluntary (art. 5a(15))

Applies from 24 Dec 2027.

6 Data protection and biometrics

The GDPR and loi n° 78-17 of 6 January 1978 apply to all subscriber data, and article L34-1 bars any use of retained data for other purposes.

Retention periods are fixed by law rather than left to the operator: five years for civil identity, one year for account, payment and connection data (art. L34-1 II bis). In January 2026 the CNIL found that Free Mobile kept data on millions of former subscribers without justification and for an excessive period, and ordered it to sort and purge that data.

Biometric data used to uniquely identify a person, such as a face template compared with an identity document photo, may not be processed unless an exception applies (art. 9 GDPR; art. 6 loi 78-17). The CNIL's recommendation on multi-factor authentication (20 March 2025) states that, unless a legal text requires or explicitly authorises it, biometrics rest only on consent and "ne peut être imposé sans alternative" (cannot be imposed without an alternative). No French telecom rule requires biometric checks, so an online face-match journey needs explicit consent and a non-biometric route. Verification whose sole purpose is to confirm that a person is who they claim to be is outside the AI Act's high-risk biometric category (Regulation (EU) 2024/1689, Annex III, point 1(a)).

An impact assessment is required for large-scale processing of biometric data (art. 35(3)(b) GDPR), and the CNIL's list of processing requiring one already names operators' customer databases as large-scale location data processing.

7 Sector-specific obligations

Caller-number authentication

Article L44 IV of the CPCE requires operators to ensure that customers using a French number as caller ID are its assignee or have the assignee's consent, to use an authentication mechanism confirming the authenticity of calls and messages, and to interrupt calls or messages that fail authentication. Arcep's guidance (updated 27 March 2026) states that only the highest attestation level of the STIR/SHAKEN-based mechanism, where the operator has verified the caller's right to use the number, meets the legal requirement.

SIM replacement and port-out

No CPCE provision addresses SIM replacement specifically (as of October 2026). The CNIL describes SIM swapping as a fraudster impersonating the customer with the operator, claiming loss or theft of the SIM to obtain a new one, and advises customers to contact their operator quickly after an unexplained loss of network access. The CNIL's 2025 recommendation also treats an SMS one-time code, including on an eSIM, as a possession factor whose reliability must be assessed case by case. Controls rest on the operator's security duty under article 32 GDPR and the integrity rules in article L33-1 I a) CPCE; the RIO process governs port-out.

Porting compensation

Article L224-42-1 of the Code de la consommation sets minimum compensation: for each day of porting delay, at least one fifth of the monthly subscription price, payable by the operator responsible.

8

Risk indicators and red flags

TELECOM IDENTITY AND FRAUD INDICATORS

- **Prepaid lines for criminal use:** anonymous prepaid SIMs used to stay undetectable, the risk behind the 2025 verification duty.
- **Caller ID spoofing:** reports to Arcep rose from 531 in 2023 to over 19,000 in 2025.
- **Impersonated trusted numbers:** calls displaying a bank's or a public authority's number.
- **Porting without the holder's knowledge:** a port request the subscriber did not start ("abus de portage").
- **SIM swap:** a replacement SIM requested on a claimed loss or theft, followed by the customer's loss of network access.
- **Data from breaches:** leaked subscriber data and IBANs used to pass identity questions at customer service.

9

Enforcement and penalties

Arcep administrative sanctions (art. L36-11 CPCE, version in force since 23 May 2024): after formal notice, the restricted committee can suspend or withdraw rights of use of numbers or frequencies and impose a fine proportionate to the seriousness of the breach and the benefit gained, up to 3% of the previous year's turnover excluding tax, or 5% for a repeat breach of the same obligation. Where turnover cannot be determined, the cap is €150,000, or €375,000 for a repeat breach.

Criminal penalties (art. L39-3 I CPCE, version in force since 13 June 2026): one year's imprisonment and a €75,000 fine for an operator or its agents who fail to erase or anonymise data when required, fail to retain technical data, or fail to verify and keep civil identity data under L34-1 II bis 1°. Individuals also face a ban of up to five years on the professional activity concerned.

Data protection fines (art. 83 GDPR): up to €10 million or 2% of worldwide turnover for breaches of security and breach-notification duties, and up to €20 million or 4% for breaches of core principles.

Recent actions. On 13 January 2026 the CNIL fined Free Mobile €27 million and Free €15 million after an October 2024 intrusion exposed data on 24 million subscriber contracts, including IBANs. It found weak authentication of remote VPN access, ineffective anomaly detection, an incomplete breach notice to subscribers and, for Free Mobile, excessive retention. On 29 January 2026 Arcep opened an administrative investigation into all operators holding French numbers (decision n° 2026-0113-RDPI) to trace spoofed calls and check compliance with authentication duties.

Cumulative proceedings. In decision n° 2026-1210 QPC of 25 June 2026 (Orange), the Conseil constitutionnel struck down the provisions of article L34-5 CPCE letting the CNIL, Arcep and the consumer authority each pursue the same automated direct-marketing breach. Until repeal on 31 October 2027, no authority may pursue a person already prosecuted or definitively sanctioned by another for the same facts.

10 Recent changes and what to watch

- **24 December 2027** **Applies from 24 Dec 2027** : telecom providers (other than micro and small enterprises) that must use strong user authentication for online identification must accept European Digital Identity Wallets on request (art. 5f(2) Regulation (EU) 2024/1183).
- **24 December 2026** **Due 24 Dec 2026** : each Member State must provide at least one European Digital Identity Wallet.
- **21 October 2026** **In force** : décret n° 2026-920 orders operators to retain traffic and location data for one year for national security.
- **October 2026** **Bill, not enacted** : the bill on critical infrastructure resilience and cybersecurity (projet de loi n° 1112), transposing EU cybersecurity rules, remains at first reading in the Assemblée nationale after Senate adoption on 12 March 2025.
- **25 June 2026** **Repeal effective 31 Oct 2027** : decision n° 2026-1210 QPC bars cumulative CNIL, Arcep and consumer-authority proceedings for the same direct-marketing breach.
- **13 June 2026** **In force** : failing to verify and keep subscriber civil identity became a criminal offence (art. L39-3 I 3° CPCE); the decree setting verification conditions is still awaited.

- **29 January 2026** **Investigation open** : Arcep investigation into number spoofing across all number-holding operators.
- **1 January 2026** **In force** : unauthenticated international calls showing French mobile numbers must be masked.
- **15 June 2025** **In force, decree pending** : loi n° 2025-532 extended identity retention to prepaid services and added the verification duty (art. L34-1 II bis 1° CPCE).

11

What this means for identity verification

- **Verify, do not just collect.** Since 13 June 2026, recording self-declared details is not enough; the flow must check that the identity is real and belongs to the customer, in shops and online.
- **Build for a pending decree.** Choose methods that are likely to satisfy a future list (document check, face match with liveness, national digital identity) and keep the flow configurable.
- **Capture exactly the R10-13 data set.** Name, date and place of birth, addresses, email and phone numbers; for business lines, the company and its representative.
- **Separate evidence from retention.** Keep identity data five years after the contract ends; use biometrics only on explicit consent, with a non-biometric route, and keep images only as long as the check requires.
- **Re-verify at high-risk moments.** SIM or eSIM replacement and port-out requests are the points where account takeover happens; authenticate the subscriber and notify the existing line.
- **Plan for digital identity wallets.** Accepting EU wallets becomes mandatory for larger operators using strong authentication by December 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:

- Remote identity verification for online SIM and eSIM orders, with ID document capture and verification (including NFC), face match and biometric liveness.
- Collection of the civil identity data set operators must retain, with phone and email verification.
- Re-verification of the subscriber before SIM or eSIM replacement and other high-risk account changes.
- No-code workflow builder to adapt verification steps once the French verification decree is published, with an audit trail for each check.
- Cloud, on-premises or hybrid deployment to fit operators' data retention and security 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

- **Code des postes et des communications électroniques, art. L33-1** [rules for networks and services] (version in force since 11 March 2023), Légifrance, legifrance.gouv.fr
- **CPCE, art. L34-1** [protection of privacy; data retention] (version in force since 15 June 2025, loi n° 2025-532 art. 29), Légifrance, legifrance.gouv.fr
- **CPCE, art. R10-13** [data operators must retain] (version in force since 21 October 2021, décret n° 2021-1361), Légifrance, legifrance.gouv.fr
- **CPCE, art. L36-11** [Arcep sanctions] (version in force since 23 May 2024), Légifrance, legifrance.gouv.fr

- CPCE, art. L39-3 [criminal penalties] (version in force since 13 June 2026), Légifrance, legifrance.gouv.fr
- CPCE, art. L44 and L44-4 [numbering, caller authentication, number portability] (L44 in force since 2 July 2025; L44-4 since 28 May 2021), Légifrance, legifrance.gouv.fr
- CPCE, art. L42-1 [authorisations to use radio frequencies] (version in force since 1 January 2023), Légifrance, legifrance.gouv.fr
- Décret n° 2026-920 du 30 septembre 2026 [order to retain certain categories of traffic and location data for one year], Journal officiel, Légifrance, legifrance.gouv.fr
- Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic, art. 29, Journal officiel, Légifrance, legifrance.gouv.fr
- Code de la consommation, art. L221-18 [withdrawal period for distance contracts] (in force since 1 July 2016), Légifrance, legifrance.gouv.fr
- Code de la consommation, art. L224-42-1 [compensation for porting delay or loss] (in force since 28 May 2021), Légifrance, legifrance.gouv.fr
- Code monétaire et financier, art. L561-2 [persons subject to AML obligations] (version in force since 5 August 2026), Légifrance, legifrance.gouv.fr
- Conseil constitutionnel, Décision n° 2025-885 DC du 12 juin 2025 [Loi visant à sortir la France du piège du narcotrafic], paras. 258 to 270, conseil-constitutionnel.fr
- Conseil constitutionnel, Décision n° 2026-1210 QPC du 25 juin 2026, Société Orange SA [cumulative proceedings and sanctions for automated direct marketing], conseil-constitutionnel.fr
- Arcep, Décision n° 2022-2148 du 6 décembre 2022 [procedures for number portability], published in the Journal officiel of 5 May 2023, arcep.fr; Journal officiel version, legifrance.gouv.fr
- Arcep, "Comment conserver mon numéro fixe ou mobile lors d'un changement d'opérateur" (updated 9 July 2026), arcep.fr
- Arcep, "Authentification des numéros de téléphone fixe ou mobile : que dois-je faire en tant qu'opérateur téléphonique ?" (updated 27 March 2026), arcep.fr
- Arcep, press release "Protection des consommateurs" (29 January 2026), arcep.fr
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 6 (in force since 1 June 2019), Légifrance, legifrance.gouv.fr
- CNIL, Recommandation relative à l'authentification multifacteur (adopted 20 March 2025), sections 2.3, 3.3 and 3.4, cnil.fr
- CNIL, list of processing operations requiring a data protection impact assessment (délibération n° 2018-327 of 11 October 2018, as amended by délibération n° 2019-011 of 31 January 2019), cnil.fr; amending deliberation, legifrance.gouv.fr
- Regulation (EU) 2024/1689 (AI Act), Annex III, point 1(a), EUR-Lex, eur-lex.europa.eu
- CNIL, "Violation de données : sanction de 42 millions d'euros à l'encontre des sociétés FREE MOBILE et FREE" (14 January 2026), cnil.fr

- CNIL, "Fuite de données sur internet et vol de votre IBAN : comment vous protéger si vous êtes concerné ?" (8 August 2025), cnil.fr
- Sénat, Rapport d'information n° 802 (2025-2026) [monitoring of the application of laws], filed 26 June 2026, senat.fr
- Sénat, amendment n° 194 to the bill "Sortir la France du piège du narcotrafic" (2024-2025, text 254), senat.fr
- Assemblée nationale, legislative dossier: projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, assemblee-nationale.fr
- Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (European Digital Identity Framework), arts. 5a(1), 5a(15) and 5f(2), EUR-Lex, eur-lex.europa.eu
- Commission Implementing Regulation (EU) 2024/2977 (28 November 2024, OJ L of 4 December 2024), EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2016/679 (GDPR), arts. 4(14), 9, 32, 35 and 83, EUR-Lex, eur-lex.europa.eu