Identomat

COMPLIANCE GUIDE

Insurance & Insurtech Compliance in France

COUNTRY France

INDUSTRY Insurance & Insurtech

LAST UPDATED 29 October 2026

KEY REGULATORS Autorité de contrôle prudentiel et de résolution (ACPR) · Tracfin · ORIAS

Key takeaways

- Every insurer and most insurance intermediaries in France must run anti-money laundering checks, not only life insurers. Non-life policies, small life policies and borrower insurance qualify for lighter checks, but the duty still applies.
- Insurers need a licence from the French prudential and resolution authority (ACPR) before selling, and brokers, agents and companies that sell insurance alongside another product (embedded insurance) must register with the intermediaries register, ORIAS.
- Selling a policy fully online is allowed. The customer's identity can be checked with a high-assurance digital identity (such as through FranceConnect+), or with two remote measures combined, such as a certified remote identity verification service plus a first payment from the customer's own bank account.
- For life policies, the person who will receive the money (the beneficiary) must be identified when the policy is taken out and verified at the latest when the claim is paid, including a check on whether that person holds or held public office.
- New EU anti-money laundering rules apply from 10 July 2027. They limit EU-wide obligations to life and investment-linked insurance, so the treatment of non-life cover in France may change.

France is open to online insurance distribution, including insurtechs and embedded insurance sold through retailers, platforms and comparison sites. There is no separate online licence: the same insurer authorisation and intermediary registration apply whatever the channel, and distance sales carry their own information and withdrawal rules.

The ACPR licenses and supervises insurers and enforces their anti-money laundering duties; Tracfin, the French financial intelligence unit, receives suspicious transaction reports; ORIAS keeps the register of intermediaries. The biggest practical hurdle for a new entrant is designing a remote onboarding flow that meets the French list of accepted verification methods, which is narrower than "document plus selfie" and treats video calls differently from physical presence.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 AML, KYC and customer due diligence
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 insurance	Level	Official site
ACPR	Licensing of insurers, prudential and conduct supervision, AML/CFT supervision and sanctions for insurers, mutuals, provident institutions and intermediaries	National	acpr.banque-france.fr
Tracfin	Financial intelligence unit: receives suspicious transaction reports, may oppose a transaction	National	economie.gouv.fr/tracfin
ORIAS	Single register of insurance, banking and finance intermediaries; checks eligibility at registration and each year	National	orias.fr
Direction générale du Trésor	National asset freeze register (national, EU and UN measures)	National	gels-avoirs.dgtresor.gouv.fr
ANSSI	Certifies remote identity verification providers (PVID) and electronic identification means	National	cyber.gouv.fr
CNIL	Data protection, including biometric data used in onboarding	National	cnil.fr

AMLA	EU AML/CFT standard-setter since 1 January 2026; drafts the technical standards under the EU AML Regulation	Supranational (EU)	amla.europa.eu

The Autorité des marchés financiers (AMF) supervises some intermediaries' activities alongside the ACPR.

2 Licensing and authorisation

Insurers

An insurance undertaking with its head office in France may start operations only after obtaining an administrative licence (agrément) from the ACPR, granted per class of insurance; it may carry out only those classes, and no single undertaking may be licensed for both life and capitalisation business and property and other non-life risks (Code des assurances, art. L321-1, in force since 10 October 2021, read with L310-1). Insurers with their head office in another EU Member State may operate in France from their head office or EU branches under the passport conditions of the code (L310-2 I 2°). There is no separate digital insurance licence.

Intermediaries and embedded insurance

Insurance intermediaries, including ancillary intermediaries, must register on the public single register, renewable yearly (Code des assurances, art. L512-1). ORIAS checks professional capacity, good repute, liability insurance and any required financial guarantee.

Two definitions in article L511-1 matter for digital models:

Comparison and quote sites

Ranking insurance contracts by price or criteria on a website counts as distribution where the customer can conclude the contract through the site.

Embedded insurance

An ancillary intermediary's main activity is not insurance and it distributes only cover complementing a good or service it supplies.

3 AML, KYC and customer due diligence

Who is in scope

Article L561-2 of the Code monétaire et financier (CMF), in force since 5 August 2026, lists as obliged persons: insurance undertakings covered by articles L310-1 and L310-2 of the Code des assurances (2°), provident institutions (2° bis), mutuals carrying out insurance operations (2° ter), occupational retirement providers (2° quater to sexies) and insurance intermediaries defined in L511-1 (3° bis), **except intermediaries that act under the full responsibility of the insurer or the insurance broker**. France does not limit the duty to life business, and EU insurers operating in France under L310-2 are covered.

Core obligations

Identify and verify

Before the relationship, identify the customer and any beneficial owner and verify them on reliable written evidence (L561-5 I).

Beneficiaries of life policies

For life and capitalisation contracts, also identify and verify the beneficiaries and their beneficial owners (L561-5 III).

Know the relationship

Record the purpose and nature of the relationship, keep it current and monitor operations against it (L561-5-1, L561-6).

Records

Five years after the relationship ends, or after each operation (L561-12).

Identification data are names and date and place of birth (R561-5); a company's beneficial owner holds more than 25% of capital or votes or otherwise controls it (R561-1). If due diligence cannot be completed, the insurer must not contract or continue, and may report to Tracfin (L561-8).

Simplified due diligence: the insurance list

Simplified measures are allowed where the risk is low or the product is on the regulatory low-risk list and there is no suspicion (L561-9). Article R561-16 (in force since 6 February 2023) lists, among others:

- life or capitalisation contracts with an annual premium of no more than €1,000 or a single premium of no more than €2,500;

- contracts outside the life-death, nuptiality-natality, investment-linked, tontine, capitalisation and collective classes, that is the non-life classes 1 to 18 of article R321-1 Code des assurances;
- retirement contracts with no surrender clause, not usable as collateral and paid out as an annuity at retirement;
- borrower insurance contracts (L113-12-2 Code des assurances).

This is not an exemption: the insurer documents the condition, checks the risk stays low and monitors for unusual transactions (R561-14).

Enhanced due diligence

Additional measures apply where the customer, its beneficial owner, or the beneficiary of a life or capitalisation contract (or that beneficiary's beneficial owner) is a politically exposed person; where the product or operation presents a particular risk, notably by favouring anonymity; and where the operation involves a country on the FATF or EU high-risk lists (L561-10). Since 24 December 2025, the article also requires the intensity and frequency of these measures to match the risk profile of the customer, beneficial owner and life-policy beneficiary. Absent suspicion, the PEP measures need not be applied where the relationship covers only products on the low-risk list. Remote onboarding is not a trigger.

Suspicious transaction reports

Insurers must report to Tracfin sums or operations suspected to derive from an offence punishable by over one year's imprisonment or linked to terrorist financing (L561-15). Tracfin expects the report before execution, so it can oppose the transaction (three exceptions allow a later report); there is no threshold, and reports go through the ERMES platform.

Asset freezes and beneficial owners

Obliged persons must apply national, EU and UN freeze measures without delay and inform the Minister of the Economy immediately (L562-4); the DG Trésor publishes them in the national freeze register. Since 31 July 2024, AML-obliged persons keep full access to the beneficial ownership register held by INPI, while other users need a legitimate interest.

4 Identity verification and onboarding

Accepted verification methods

Article R561-5-1 CMF (in force since 5 April 2021) sets the primary routes. An insurer verifies a natural person's identity by: (1) an electronic identification means certified or attested by ANSSI at eIDAS "substantial" or "high" level, or a means from a scheme notified to the European Commission at those levels; (2) an electronic identification means presumed reliable under article L102 of the Code des postes et des communications électroniques; or (3) if the customer is physically present, the original of a valid official photo document plus a copy.

Where these cannot be used, article R561-5-2 requires **at least two** of the following, chosen so that together they verify every identification element:

#	Measure (R561-5-2)	Typical digital use
1°	Copy of an official photo ID or registry extract	Uploaded image of an ID card or passport
2°	Verification and certification of that copy by an independent third party	Third-party document certification
3°	First payment from or to an account in the customer's name at an EU/EEA (or equivalent) obliged institution	First premium by direct debit or transfer from the customer's own account
4°	Direct confirmation of identity from a qualifying third party under L561-7	Bank or group entity confirmation
5°	A service certified by ANSSI (or an authorised body) at "substantial" level of the identity-proofing requirements of Implementing Regulation (EU) 2015/1502	Certified remote identity verification provider (PVID)
6°	Advanced or qualified electronic signature or seal based on a qualified certificate, or qualified registered electronic delivery	Qualified e-signature of the policy

The ACPR's identification guidelines (16 December 2021) confirm that checks may be remote, that physical presence for the original document "exclut le recours à la vidéoconférence", and that a bank details slip (RIB) alone does not satisfy the first-payment measure.

Certified remote identity verification (PVID)

ANSSI's PVID framework (v1.1, 1 March 2021) covers automated, operator-led and hybrid services: face comparison, liveness detection with declared error rates, minimum video quality and document security or chip checks. ANSSI lists certified providers.

Timing and the beneficiary

Where risk is low, verification may be completed while the relationship is set up (L561-5 IV): for a contract, by its conclusion; for an insurance beneficiary, by payment of the benefit (R561-6). Above the R561-16 premium thresholds, life beneficiaries are identified at subscription (by name, or by enough detail when designated by category) and verified at payout (R561-10-3). An assignee and any new beneficiary must be identified and verified (R561-11-1).

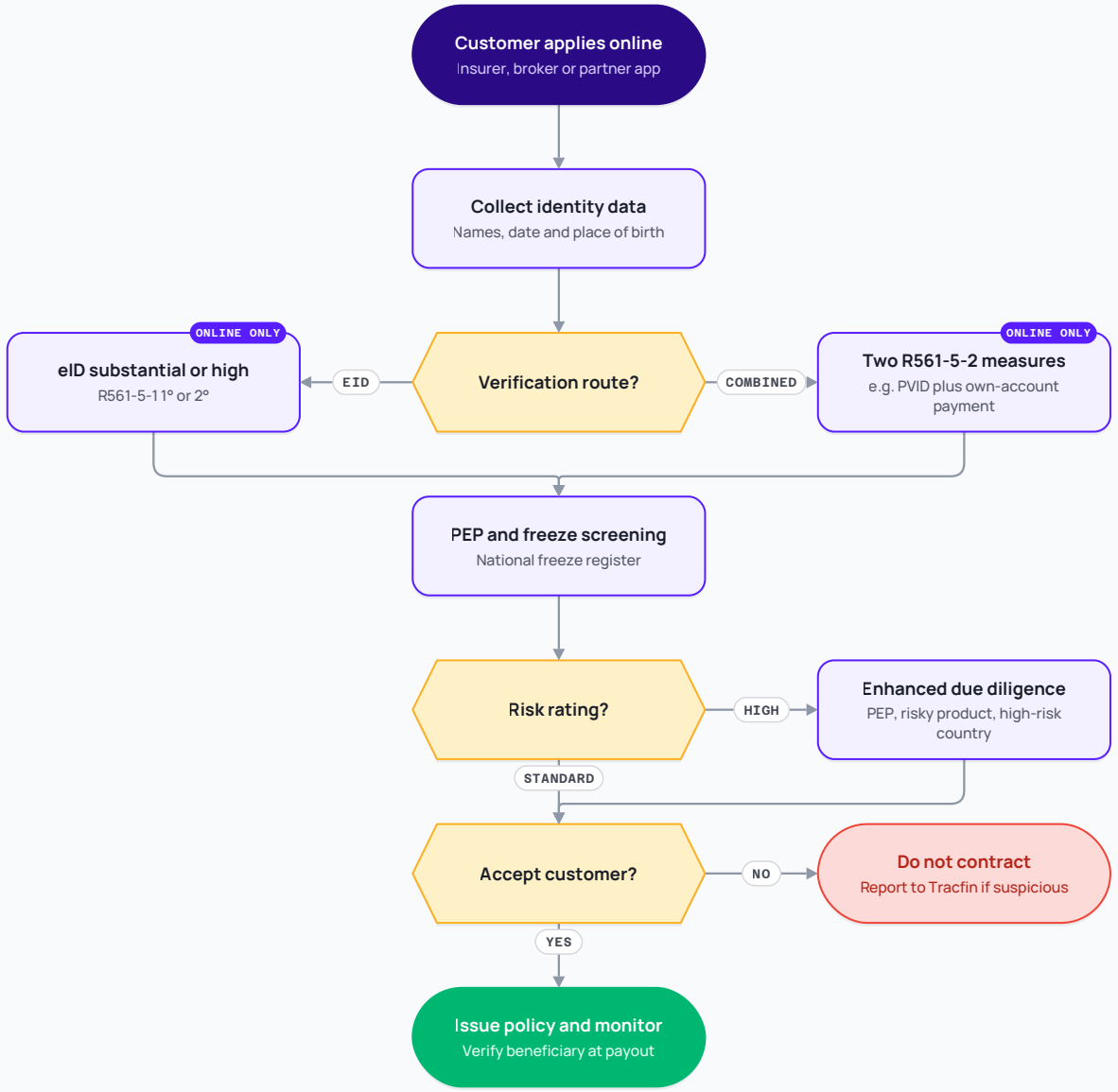


Figure 1. Remote onboarding for a French life or savings insurance policy (CMF R561-5-1, R561-5-2, R561-6).

Reliance on third parties

Insurers may rely on identification by another qualifying obliged entity, including a group entity, under a written contract, but remain responsible (L561-7, R561-13).

5 Digital channels: what's different

Bottom line: the due diligence duties are channel-neutral, but the verification route is not: a customer who is not physically present must be verified by a qualifying electronic identity or by two combined remote measures, and a video call does not count as physical presence.

Requirement	In person	Online / remote	Difference
Primary verification method	Original photo ID shown, copy taken (R561-5-1 3°)	eID at substantial/high level (R561-5-1 1°, 2°)	Differs
Fallback method	Not needed when the original is shown	At least two R561-5-2 measures combined	Differs
Video calls	Physical presence required for the original-document route	Video conferencing does not count as presence (ACPR guidelines)	Differs
Enhanced due diligence trigger	PEP, risky product, high-risk country (L561-10)	Same list; remote onboarding is not a trigger in itself	Same
Verification timing	Before the relationship; deferral if low risk (L561-5 IV)	Same rule	Same
Life beneficiary checks	Identify at subscription, verify at payout (R561-10-3)	Same rule	Same
Reliance on a third party	Allowed, insurer remains liable (L561-7)	Same rule	Same
Distance-selling rules	Do not apply	Apply, including a 14-day renunciation right (L112-2-1)	Differs

Building a compliant remote flow

Document upload with a selfie is, on its own, only measure 1° of R561-5-2. It becomes compliant when combined with a second measure: the most common pairings are a PVID-

certified service (5°) or a qualified electronic signature (6°), or a first premium paid from an account in the customer's name (3°). For the eID route, FranceConnect+ is open to obliged persons that must verify identity under L561-5; its identity providers must be qualified at "substantial" or "high" level, and currently are L'Identité Numérique La Poste and France Identité, which ANSSI certified at eIDAS "high" level on 7 February 2024.

Remote onboarding tool governance

The EBA Guidelines on remote customer onboarding (EBA/GL/2022/15, applicable since 2 October 2023, kept in force by AMLA) require insurers to assess the solution before use, check document authenticity, run liveness detection when unattended, and stop or redirect when evidence is ambiguous.

Pending

From 10 July 2027, the EU AML Regulation accepts an identity document plus reliable independent sources, or eIDAS identification at "substantial" or "high" level (art. 22(6)) `Adopted, applies 10 Jul 2027`.

6 Data protection and biometrics

The GDPR and the loi n° 78-17 of 6 January 1978 (Informatique et Libertés, art. 6) prohibit processing biometric data to identify a person uniquely unless an article 9(2) GDPR exception applies; a face match counts when specific technical processing allows or confirms identification (GDPR art. 4(14), recital 51). The CNIL considers that, unless a legal text requires or explicitly authorises it, biometrics rest on explicit consent and "ne peut être imposé sans alternative" (recommendation on multi-factor authentication, 20 March 2025). An eID or a non-biometric R561-5-2 combination provides that alternative.

Insurer-specific CNIL positions (July 2021): AML/CFT processing rests on legal obligation; fraud detection on legitimate interest, with no fully automated decision; health data for contracts outside social protection, such as borrower insurance, need explicit consent. The social security number (NIR) may be used for AML only where it appears on a freeze or sanctions list (décret n° 2019-341, art. 2 D 11°). Access to data processed solely for AML is exercised through the CNIL, not the insurer (L561-45 CMF).

Large-scale processing of biometric or health data requires an impact assessment (GDPR art. 35(3)(b)); the PVID framework caps biometric retention at 96 hours.

7 Sector-specific obligations

Politically exposed beneficiaries at payout

Insurers must determine, at the latest at payout or assignment, whether a life or capitalisation beneficiary (or its beneficial owner) is a politically exposed person; if so, a member of the executive body must be informed before payment and monitoring strengthened (R561-20-3). A person remains a PEP for one year after leaving office (ACPR, July 2024).

Finding deceased policyholders and beneficiaries

Life insurers and provident institutions must check at least yearly, using death data from the national register of natural persons (RNIPP), whether insured persons, subscribers or beneficiaries have died (L132-9-3 Code des assurances), and publish yearly the number and amount of unsettled contracts (L132-9-3-1).

Digital operational resilience (DORA) and identity vendors

Regulation (EU) 2022/2554 has applied since 17 January 2025 to insurers and to insurance intermediaries other than micro, small and medium-sized enterprises (art. 2). An outsourced identity verification or screening service is an ICT third-party service: the insurer stays fully responsible (art. 28(1)), records the contract in its register of information (art. 28(3)) and includes the mandatory contractual terms (art. 30). Major ICT incidents are reported to the ACPR (art. 19; ACPR Instruction 2025-I-10, from 1 July 2025), alongside any GDPR breach notification to the CNIL within 72 hours.

8 Risk indicators and red flags

INSURANCE TYPOLOGIES FROM TRACFIN AND THE ACPR

- **Life policies and tax fraud**: repatriation of undeclared funds from abroad and disguised gifts; life insurance is rated moderate risk.
- **Early surrender, advances and pledges**: surrenders hiding corporate asset abuse or abuse of an elderly person's weakness; pledges activated to repay property loans early.
- **30-day renunciation**: premiums paid in, then recovered through the withdrawal right.
- **Cyber ransom cover**: ransomware payments under cyber policies may finance terrorism or breach freeze measures; rated high terrorist-financing risk.
- **Staged motor claims**: vehicles bought with cash abroad, then deliberately damaged in France.
- **Group policies for fictitious staff**: collective insurance fraud through shell companies or fictitious employees.
- **Forged or diverted ID copies**: remote onboarding with falsified documents, or a first payment from an account not held by the verified customer.
- **Identity theft in health claims**: stolen identities and bought prescriptions used against supplementary health insurers.

The insurance sector filed 13,002 suspicious transaction reports with Tracfin in 2024 (11,440 in 2023): 11,172 from insurers, 1,273 from mutuals and provident institutions and 557 from intermediaries.

9 Enforcement and penalties

The ACPR supervises AML/CFT and EU restrictive-measure compliance (L561-36, L561-36-1). Its Commission des sanctions may impose, by severity (L612-39 CMF, in force since 10 April 2026):

Tier	Sanction
Disciplinary	Warning; reprimand (blâme)

Restrictions	Ban on certain operations or other limits on activity, and temporary suspension of executives, each for up to ten years
Management	Forced resignation of executives
Licence	Partial or total withdrawal of authorisation, or removal from the list of authorised persons
Financial	Instead of or in addition: a fine of up to €100 million or 10% of annual net turnover for breaches of the AML/CFT chapters of the CMF and EU AML and restrictive-measure rules

In its decision of 12 October 2023, the Commission des sanctions imposed a reprimand and a €3.5 million fine on the life insurer Abeille Vie (formerly Aviva Vie), published by name for five years. Failings covered customer knowledge updates, PEP identification, enhanced due diligence, automated detection of unusual transactions, timely reporting and control of outsourced activities. On 13 November 2023, it fined Mutuelle de Poitiers Assurances, a non-life insurer, €600,000 with a reprimand for a structurally deficient asset-freeze system, stressing an "obligation de résultat" that applies to non-life insurers too.

The CNIL fined an online motor insurance intermediary €180,000 for exposing customers' driving licences (2019) and a mutual insurer €1.75 million for retention and information failures (2021).

10 Recent changes and what to watch

- **2 December 2027:** AI Act high-risk rules apply to AI used for life and health insurance risk assessment and pricing; biometric verification that only confirms a claimed identity is not high-risk (Regulation (EU) 2024/1689, Annex III, as amended by Regulation (EU) 2026/1744) `Adopted, applies 2 Dec 2027`.
- **10 July 2027:** EU AML Regulation (EU) 2024/1624 applies and Directive (EU) 2024/1640 must be transposed `Adopted, applies 10 Jul 2027`. It covers insurers only for life and investment-related business (art. 2(1)(6)(b)); France may extend scope under Directive 2024/1640 (art. 3).
- **1 October 2026:** AMLA submits final draft standards on customer due diligence, including non-face-to-face verification, to the European Commission `Final draft, not yet adopted`. Proposed to apply six months after entry into force.
- **11 August 2026:** new telephone selling rules for insurers and intermediaries (L112-2-2 Code des assurances) `In force`.

- **19 June 2026:** distance insurance sales rules rewritten by ordonnance n° 2026-2 (L112-2-1) `In force`. Includes a 14-day renunciation right.

11 What this means for identity verification

- **Plan two routes.** An eID route (FranceConnect+) and a combined R561-5-2 route; document capture and selfie alone are one measure.
- **Prefer certified components.** A PVID-certified service or a qualified e-signature is a recognised second measure; a first premium from the customer's own account also counts, a RIB alone does not.
- **Scale by product.** Small life policies, non-life and borrower cover can use simplified measures with documented justification and monitoring; larger life and capitalisation contracts need full CDD and beneficiary handling.
- **Re-verify at payout.** Build a beneficiary verification and PEP check into the claims and surrender journey, plus identification of any assignee.
- **Keep evidence, not templates.** Retain CDD records for five years after the relationship ends, delete biometric data within certified limits, and offer a non-biometric route.

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 KYC onboarding with ID document capture and verification, including NFC chip reading, face match and biometric liveness.
- AML screening against sanctions and PEP lists at subscription and again before a life-policy payout.
- E-signatures and configurable workflows that combine verification measures by product and risk level.
- KYB and beneficial owner verification for corporate policyholders and distribution partners.
- Ongoing monitoring with an audit trail for each check, on cloud, on-premises or hybrid deployment.

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 monétaire et financier, art. L561-2 (Personnes assujetties)**, version in force since 5 August 2026, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, arts. L561-4-1 to L561-14-2 (Obligations de vigilance à l'égard de la clientèle)**, including L561-5, L561-5-1, L561-6, L561-7 (in force since 3 May 2025), L561-8, L561-9, L561-10 (in force since 24 December 2025) and L561-12, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, arts. L561-1 to L561-50**, including L561-15, L561-36 and L561-36-1 (in force since 1 July 2026), Légifrance, legifrance.gouv.fr

- **Code monétaire et financier, arts. R561-1 to R561-65**, including R561-1, R561-5, R561-5-1, R561-5-2, R561-6, R561-10-3, R561-11-1, R561-12-1, R561-13, R561-14, R561-16 and R561-20-3, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, art. L612-39 (Liste des sanctions)**, version in force since 10 April 2026, Légifrance, legifrance.gouv.fr
- **Code des assurances, art. L321-1 (Agrément administratif)**, Légifrance, legifrance.gouv.fr
- **Code des assurances, art. L511-1 (Distribution d'assurances)**, Légifrance, legifrance.gouv.fr
- **Code des assurances, art. L512-1 (Obligation d'immatriculation)**, Légifrance, legifrance.gouv.fr
- **Code des assurances, arts. L112-2-1 and L112-2-2 (fourniture à distance)**, versions in force since 19 June 2026 and 11 August 2026, Légifrance, legifrance.gouv.fr
- **Code des assurances, arts. L132-9-3 and L132-9-3-1**, Légifrance, legifrance.gouv.fr
- **ACPR, Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle [Guidelines on identification, identity verification and customer knowledge]**, 16 December 2021, paras 14, 32, 35, 46 to 48, acpr.banque-france.fr
- **ACPR, Les personnes politiquement exposées [Politically exposed persons]**, July 2024, acpr.banque-france.fr
- **ACPR, press release on the Commission des sanctions decision against Abeille Vie**, 20 October 2023, acpr.banque-france.fr
- **Tracfin, Quand et comment déclarer un soupçon ? [When and how to report a suspicion]**, economie.gouv.fr
- **Tracfin, Activity 2024 Review, Volume II**, July 2025, pp. 37 to 38, economie.gouv.fr
- **ANSSI, Prestataires de vérification d'identité à distance (PVID)**, cyber.gouv.fr
- **ANSSI, PVID – Référentiel d'exigences [Requirements framework], v1.1**, 1 March 2021, sections IV.3.1 to IV.3.5, cyber.gouv.fr
- **ORIAS, Qu'est-ce que l'ORIAS ? [What is ORIAS?]**, orias.fr
- **Direction générale du Trésor, Le registre national des gels se transforme [The national freeze register]**, 18 March 2021, tresor.economie.gouv.fr
- **France Identité, press kit on the general launch of France Identité**, February 2024, france-identite.gouv.fr
- **EBA, Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15)**, 22 November 2022, applicable from 2 October 2023, paras 13 to 49, eba.europa.eu
- **AMLA, EBA and AMLA complete handover of AML/CFT mandates**, 19 January 2026, amla.europa.eu
- **AMLA, Press release: AMLA finalises key standards for the private sector**, 1 October 2026, amla.europa.eu
- **Regulation (EU) 2024/1624 (AML Regulation)**, arts. 2(1)(6), 22(6), 44, 47 and 90, EUR-Lex, eur-lex.europa.eu
- **Directive (EU) 2024/1640 (sixth AML Directive)**, arts. 3 and 78, EUR-Lex, eur-lex.europa.eu

- **Code monétaire et financier, art. L561-45 (Droit d'accès indirect aux données)**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, art. L562-4 (gel des avoirs)**, version in force since 26 February 2022, Légifrance, legifrance.gouv.fr
- **Code des assurances, arts. L310-1 and L310-2**, Légifrance, legifrance.gouv.fr
- **Code des assurances, art. R321-1 (branches d'assurance)**, Légifrance, legifrance.gouv.fr
- **Loi n° 78-17 du 6 janvier 1978 (Informatique et Libertés), art. 6**, version in force since 1 June 2019, Légifrance, legifrance.gouv.fr
- **Décret n° 2019-341 du 19 avril 2019 (uses of the NIR), art. 2 D 8°, 11°, 14° and 15°**, version in force since 1 January 2026, Légifrance, legifrance.gouv.fr
- **CNIL, Recommandation relative à l'authentification multifacteur [Recommendation on multi-factor authentication]**, adopted 20 March 2025, sections 3.3 to 3.5, cnil.fr
- **CNIL, Les grands traitements du secteur de l'assurance et leurs bases légales [Main insurance processing and legal bases]**, 16 July 2021, cnil.fr
- **CNIL, Le principe de minimisation et les traitements du NIR et des données de santé dans le secteur de l'assurance [Minimisation, NIR and health data in insurance]**, 16 July 2021, cnil.fr
- **CNIL, Délibération SAN-2019-007**, 18 July 2019, Légifrance, legifrance.gouv.fr
- **CNIL, Délibération SAN-2021-010**, 20 July 2021, Légifrance, legifrance.gouv.fr
- **CNIL, Violations de données personnelles : les règles à suivre [Personal data breaches]**, cnil.fr
- **ACPR, Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme [Sector risk analysis]**, June 2023, pp. 5, 26 to 28 and 96 to 101, acpr.banque-france.fr
- **ACPR, press release on the Commission des sanctions decision against Mutuelle de Poitiers Assurances**, 21 November 2023, acpr.banque-france.fr
- **Tracfin, LCB-FT : activité des professions déclarantes, bilan 2024 [Reporting professions' activity, 2024], Volume I**, Fiche 4 Assurances, pp. 36 to 37, economie.gouv.fr
- **INPI, FAQ on access to beneficial ownership data**, inpi.fr
- **FranceConnect, partner documentation: eligibility and identity providers**, partenaires.franceconnect.gouv.fr and identity providers
- **Regulation (EU) 2024/1689 (AI Act)**, Annex III points 1(a) and 5©, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2026/1744 (Digital Omnibus on AI)**, 8 July 2026, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2022/2554 (DORA)**, arts. 2, 19, 28, 30 and 64, EUR-Lex, eur-lex.europa.eu
- **ACPR, Instruction n° 2025-I-10 relative aux déclarations des incidents majeurs liés aux TIC [major ICT incident reporting]**, 23 June 2025, in force 1 July 2025, acpr.banque-france.fr
- **Regulation (EU) 2016/679 (GDPR)**, arts. 4(14), 9 and 35, recitals 51 and 85, EUR-Lex, eur-lex.europa.eu