



Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in France

COUNTRY France

INDUSTRY Crypto & Virtual Assets

LAST UPDATED 29 October 2026

KEY REGULATORS **Autorité des marchés financiers** · **Autorité de contrôle prudentiel et de résolution** · **Tracfin**

Key takeaways

- Since 2 July 2026, crypto exchanges, brokers and custodians serving French customers need an authorisation under the EU Markets in Crypto-Assets Regulation (MiCA), either from the French markets regulator or from another EU country's regulator with a passport into France. The old French registration no longer lets anyone operate.
- Authorised crypto firms are fully covered by French anti-money laundering rules: they must identify and verify every customer before opening an account (and one-off customers before any transaction, whatever the amount), screen against the national asset-freeze register, and report suspicions to Tracfin, the French financial intelligence unit, before executing the transaction.
- Fully online onboarding is allowed. A firm either accepts a certified digital identity at the EU "substantial" or "high" level, or combines at least two listed remote measures, such as a certified remote identity verification service and a first payment from a bank account in the customer's own name.
- Every crypto transfer, whatever its size, must carry the sender's and recipient's identity data (the "travel rule"). For transfers above €1,000 to or from a wallet the customer controls themselves, the firm must assess whether the customer actually owns that wallet.
- Stricter, harmonised EU rules arrive on 10 July 2027, when the EU Anti-Money Laundering Regulation applies and bans accounts that allow anonymity, including privacy coins.

France is open to online crypto businesses, but only through the MiCA authorisation route. The Autorité des marchés financiers (AMF) authorises crypto-asset service providers and supervises their conduct, while the Autorité de contrôle prudentiel et de résolution (ACPR) supervises their anti-money laundering and counter-terrorist financing (AML/CFT) controls. Tracfin receives suspicious transaction reports.

The biggest obstacle for a new entrant is the authorisation file itself: MiCA requires a registered office and effective management in the EU, minimum capital, and documented AML/CFT and ICT controls before the first customer is onboarded. Firms that relied on the French national regime and had no MiCA authorisation by 1 July 2026 were removed from the register automatically.

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

Regulator	Remit	Level	Official site
Autorité des marchés financiers (AMF)	MiCA authorisation of crypto-asset service providers (PSCA), conduct supervision, white list and blacklist	National	amf-france.org
Autorité de contrôle prudentiel et de résolution (ACPR)	AML/CFT and asset-freeze supervision and sanctions for crypto-asset service providers (the AMF covers those authorised only for crypto advice or portfolio management)	National	acpr.banque-france.fr
Tracfin	Financial intelligence unit: receives suspicious transaction reports	National	economie.gouv.fr/tracfin
Direction générale du Trésor	National register of asset freezes (national, EU and UN measures)	National	gels-avoirs.dgtresor.gouv.fr
Agence nationale de la sécurité des systèmes d'information (ANSSI)	Certification of remote identity verification services (PVID) and eIDAS electronic identification	National	cyber.gouv.fr

Commission nationale de l'informatique et des libertés (CNIL)	Data protection, including biometric data	National	cnil.fr
European Securities and Markets Authority (ESMA)	EU-wide interim MiCA register of authorised providers and non-compliant entities	Supranational	esma.europa.eu
Anti-Money Laundering Authority (AMLA)	EU AML/CFT rulebook and standards; took over the EBA's AML/CFT mandates on 1 January 2026	Supranational	amla.europa.eu

2 Licensing and authorisation

Under Article 59 of Regulation (EU) 2023/1114 (MiCA), only a legal person authorised as a crypto-asset service provider (prestataire de services sur crypto-actifs, PSCA) under Article 63, or a listed financial entity such as a bank or investment firm under Article 60, may provide crypto-asset services in the EU. Providers need a registered office, effective management and at least one resident director in the EU (Article 59(2)).

The French transition is over

Under article 8 III of loi n° 2023-171, the national "PSAN" registration regime (articles L54-10-1 to L54-10-6 of the Code monétaire et financier, CMF) ceased to apply at the end of the MiCA transitional period, which MiCA Article 143(3) capped at 1 July 2026. The AMF delisted PSAN without MiCA authorisation on 2 July 2026; there is no equivalence regime for third-country providers. On 6 July 2026 France had 31 authorised providers and the EU 283.

Application and timeline

Applications use the AMF's PSCA forms, including a DORA cybersecurity self-assessment. MiCA Article 62 requires a description of internal control mechanisms and procedures to manage money laundering and terrorist financing risks, ICT documentation and client asset segregation procedures. The regulator has 25 working days to check completeness and 40 working days from a complete file to decide (Article 63(2) and (9)).

MiCA class (Annex IV)	Services	Minimum capital
Class 1	Order execution, placing, transfer services, reception and transmission of orders, advice, portfolio management	€50,000
Class 2	Class 1 plus custody, exchange for funds, exchange for other crypto-assets	€125,000
Class 3	Class 2 plus operating a trading platform	€150,000

A provider authorised in another Member State can serve French customers after notifying its home regulator under MiCA Article 65. ESMA's interim MiCA register (last updated 22 October 2026) and the AMF white list show who is authorised. Authorised providers taking on clients of winding-down firms must first complete AML/CFT checks.

3

AML, KYC and customer due diligence

Crypto-asset service providers authorised under MiCA Article 59, including French branches of providers based elsewhere in the EU, are obliged entities under **CMF article L561-2, 7° bis** (current version in force since 5 August 2026). Providers authorised only for crypto portfolio management or advice, and certain investment firms and fund managers offering crypto services, fall under 7° quater instead. The ACPR supervises AML/CFT compliance for 7° bis providers and the AMF for advice-only and portfolio-management-only providers (L561-36 and L561-36-1), a split that ordonnance n° 2024-937 kept in place when MiCA took effect.

No threshold for occasional customers. Before carrying out any operation for an occasional customer, a crypto-asset service provider must identify and verify that customer and any beneficial owner, whatever the amount (R561-10 II 5°). This is stricter than the €1,000 threshold in the EU Anti-Money Laundering Regulation (AMLR), which applies from July 2027 (Article 19(3)).

Customer due diligence

Before entering a business relationship, identify the customer and any beneficial owner and verify those elements on reliable evidence (L561-5). For a natural person, the identification data are surname, first names, and date and place of birth (R561-5).

Ongoing monitoring

Constant vigilance and careful examination of operations throughout the relationship, consistent with the customer's profile (L561-6).

Enhanced due diligence

Required for politically exposed persons, products or operations that favour anonymity, and operations linked to FATF or EU high-risk countries (L561-10, in force since 24 December 2025).

Beneficial owners

More than 25% of capital or votes, or control. Obligated entities keep full access to the INPI register.

Suspicious transaction reporting

Under L561-15, providers report to Tracfin, with no monetary threshold, sums and operations they know or suspect derive from an offence punishable by more than one year's imprisonment or are linked to terrorist financing. Tracfin requires the report **before** the transaction is executed, so it can exercise its right of opposition; reports go through the ERMES platform.

Asset freezes

L562-4 requires obliged entities to apply freeze measures without delay and to inform the Minister of the Economy immediately. The Direction générale du Trésor publishes the national register of freezes, covering national, EU and UN measures, with a public API (latest publication 27 October 2026). EBA Guidelines EBA/GL/2024/15 on restrictive measures apply to crypto providers from 30 December 2025; the AMF adopted them as position DOC-2025-02.

4

Identity verification and onboarding

Article R561-5-1 CMF (in force since 5 April 2021) sets the primary verification routes. A provider can verify identity through an electronic identification means certified or attested by ANSSI at the eIDAS "substantial" or "high" assurance level, or one issued under a

scheme notified to the European Commission at those levels; or, when the customer is physically present, through the original of a valid official photo identity document, keeping a copy.

Where those routes cannot be used, R561-5-2 requires **at least two** of the following measures:

- a copy of an official identity document;
- verification and certification of that copy by a third party independent of the customer;
- a first payment from or to an account in the customer's name at a bank or payment institution in the EU, the EEA or an equivalent third country;
- direct confirmation of identity from a third party meeting the reliance conditions of L561-7;
- a remote identity verification service certified by ANSSI (or a body it authorises) at the "substantial" level of the identity-proofing requirements of Implementing Regulation (EU) 2015/1502, known as PVID;
- a qualified or advanced electronic signature or seal, or a qualified electronic registered delivery service.

ANSSI publishes the certification framework for these remote services (arrêté of 28 March 2021). The ACPR's identification guidelines (December 2021 version) confirm that verification may be remote, that the in-person document route excludes videoconferencing, that biometrics and video are usable within R561-5-1 or R561-5-2, and that reading the machine-readable zone alone is not verification. ACPR inspections of crypto firms found verification shortcomings, including where specialised providers were used, and detected impersonation cases.

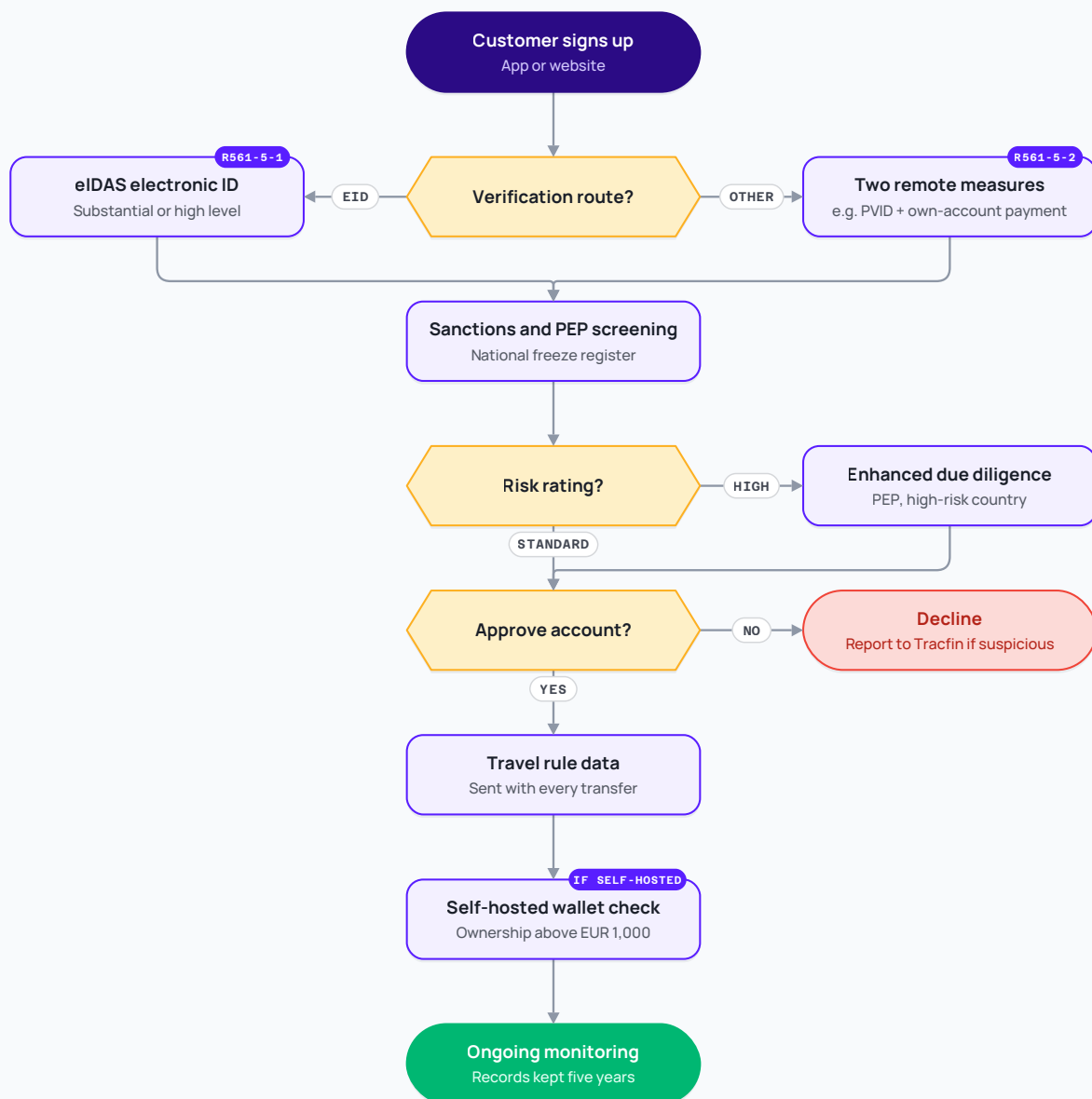


Figure 1. Remote customer onboarding at a French crypto-asset service provider.

5

Digital channels: what's different

Bottom line: French AML rules are channel-neutral in what they require, but they prescribe exactly which evidence counts online: a certified eIDAS identity, or two listed remote measures, never a scan of an ID document on its own.

Requirement

In person

Online / remote

Difference

Authorisation	MiCA authorisation	MiCA authorisation; no separate online licence	Same
When identity is verified	Before the relationship starts	Before the relationship starts	Same
Accepted evidence	Original official photo ID plus a copy	eIDAS substantial or high eID, or two R561-5-2 measures	Differs
Video identification	Not relevant	Only within an R561-5-1 or R561-5-2 route, such as a certified PVID service	Differs
Risk treatment of the channel	Risk-based	Not higher risk in itself; higher if the remote solution does not meet EBA remote onboarding guidelines	Differs
IP address and device signals	Not applicable	Inconsistent IP, shared devices or anonymisers are risk factors	Differs
Travel rule and self-hosted wallets	Applies	Applies	Same
Asset-freeze screening and reporting	Required	Required	Same
Record retention	Five years	Five years	Same

Two measures, not one

Without a certified eIDAS identity, a remote flow must combine two R561-5-2 measures, for example an ID document copy plus a first payment from an own-name bank account. An ANSSI-certified PVID service counts as one measure.

Remote onboarding quality is a risk factor

EBA risk factor guidelines for crypto providers (EBA/GL/2024/01, still in force under AMLA) treat remote solutions that do not meet the EBA remote onboarding guidelines (EBA/GL/2022/15) as higher risk, as are darknet-linked IPs, anonymisers, shared devices and inconsistent IP data.

What is changing

AMLA's final draft standards on customer due diligence **Final draft, not yet adopted**, sent to the Commission on 1 October 2026, cover non-face-to-face verification and electronic identification.

6 Data protection and biometrics

The General Data Protection Regulation (GDPR) and the loi Informatique et Libertés apply, supervised by the CNIL. Due diligence data meet the legal obligations in L561-5 and R561-5 and are kept for five years after the relationship ends (L561-12; Article 26 of Regulation (EU) 2023/1113 for travel rule records). Customers exercise their right of access to data processed solely for AML purposes through the CNIL, which releases them only if this would not reveal a suspicious transaction report (L561-45); telling a customer about a report is prohibited (L561-18).

Biometrics

Face matching processes biometric data "for the purpose of uniquely identifying a natural person", which GDPR Article 9(1) and article 6 of the loi Informatique et Libertés prohibit unless an exception applies. The CNIL considers that, unless a legal text makes biometrics mandatory or expressly authorises them, only explicit consent (Article 9(2)(a)) can be relied on, that biometrics cannot be imposed without an alternative, and that templates should preferably stay on devices under the user's exclusive control (recommendation on multi-factor authentication, 20 March 2025). French AML rules do not require biometrics, so an eIDAS identity or two R561-5-2 measures without face matching can serve as that alternative. Large-scale processing of biometric data requires a data protection impact assessment (GDPR Article 35(3)(b)). One-to-one verification that a person is who they claim to be is excluded from the AI Act's high-risk biometric category (Regulation (EU) 2024/1689, Annex III, point 1(a)).

Travel rule data and blockchains

Travel rule data may be processed only to prevent money laundering and terrorist financing; commercial use is prohibited, and new clients must receive GDPR information before the relationship or occasional transaction starts (Regulation (EU) 2023/1113, Article 25). The European Data Protection Board advises against storing personal data on a blockchain (Guidelines 02/2025, version 2.0, adopted 7 July 2026), and the CNIL recommends that any personal data recorded on-chain take the form of a cryptographic commitment.

Personal data breaches must be notified to the CNIL within 72 hours of awareness (GDPR Article 33). Crypto-asset service providers are also within the Digital Operational Resilience Act (DORA), whose separate major ICT incident reports start with an initial notification no later than 24 hours after awareness.

7 Sector-specific obligations

Travel rule

Regulation (EU) 2023/1113 has applied since 30 December 2024. Every transfer must carry the originator's name, ledger address or account, and address with official document and customer numbers (or date and place of birth), plus the beneficiary's name and address or account; the originator's data are verified before transfer (Article 14(1), (2) and (6)). Unlike transfers of funds, crypto transfers carry these requirements regardless of amount (recital 30). The EBA travel rule guidelines (EBA/GL/2024/11) apply from 30 December 2024; both the ACPR and the AMF (position DOC-2024-08) apply them.

Self-hosted wallets

For transfers to or from a self-hosted address, the provider must obtain and hold the originator and beneficiary information. Above **€1,000**, it must take adequate measures to assess whether the address is owned or controlled by its customer (Articles 14(5) and 16(2)). French law adds a risk-based layer for all self-hosted transfers: providers must assess the risk and apply enhanced measures (L561-10-4, in force since 30 December 2024), choosing among verifying the identity of the originator or beneficiary, collecting more information on the origin and destination of the assets, and enhanced ongoing monitoring (R561-21-1).

Anonymity-enhancing coins

From 10 July 2027, AMLR Article 79 bans anonymous crypto-asset accounts and accounts allowing anonymisation or obfuscation, including through anonymity-enhancing coins. Until then, products favouring anonymity trigger enhanced due diligence (L561-10).

Tax reporting of users

France applies Directive (EU) 2023/2226 (DAC8) through articles 1649 AC bis to 1649 AC sexies of the Code général des impôts; décret n° 2025-1276 (in force since 25 December 2025) sets the due diligence. Providers must obtain a self-certification of each user's tax residence when the relationship starts, and from existing users before 1 January 2027, and

check that it is plausible against the documents collected for AML due diligence (décret article 15).

8

Risk indicators and red flags

CRYPTO-ASSET TYPOLOGIES (ACPR, TRACFIN AND EBA)

- **Mixers and tumblers:** funds that pass through services that break traceability.
- **Privacy coins:** assets with optional or mandatory anonymity features.
- **Anonymised access:** VPNs, proxies, Tor or a darknet-linked IP address.
- **IP mismatch:** an IP address in a different country from the declared residence.
- **Shared devices:** one IP address or device used by several unrelated customers.
- **Peeling and smurfing:** funds split across many addresses or small transfers.
- **Illicit sources:** links to ransomware, hacks, scams or darknet markets.
- **Money mules:** vulnerable customers making frequent or high-value transfers.

Tracfin's 2024-2025 threat assessment calls crypto-assets an established part of illegal financial networks, also used to evade sanctions. Its "rug pull" scam warning signs include social-media promotion, promised safe returns, sudden token price rises and AMF-blacklisted assets.

9

Enforcement and penalties

For AML/CFT and asset-freeze breaches, the ACPR's Commission des sanctions applies L612-39 (L561-36-1):

- disciplinary sanctions graded by seriousness: warning, reprimand (blâme), ban on certain operations, temporary suspension or dismissal of managers, and partial or total withdrawal of authorisation;
- instead of or in addition, a financial penalty of up to **€100 million or 10% of annual net turnover** for breaches of the AML/CFT chapters of the CMF and of EU AML/CFT and restrictive-measures rules.

For MiCA conduct and authorisation breaches, the AMF Commission des sanctions can impose a warning, reprimand, temporary or permanent ban, and a fine of up to **€100 million**

or ten times the profit made (L621-15 III a), which covers authorised crypto-asset service providers listed in L621-9 II 21°).

ACPR inspections of crypto providers reported in October 2025 found weak customer data, risk profiles and transaction monitoring, with outcomes from follow-up letters to disciplinary measures and register removals. The AMF blacklist is the most visible action against online operators: on 8 July 2026 it added seven unauthorised crypto-asset websites.

The CNIL fined a company selling cryptocurrency wallets €750,000 on 10 October 2024 for data security and retention failings.

10 Recent changes and what to watch

- **10 July 2027:** **Adopted, applies 10 Jul 2027** The AMLR applies directly, harmonising due diligence and banning accounts in anonymity-enhancing coins.
- **21 October 2026:** **Proposal, not legislation** French authorities proposed stronger ESMA supervision of significant providers, a DeFi framework and clearer staking and lending rules in the MiCA review.
- **7 October 2026:** **Consultation response** AMLA asked for staking, lending, DeFi control and unauthorised stablecoins to be addressed in the MiCA review.
- **1 October 2026:** **Final draft, not yet adopted** AMLA submitted final draft standards on customer due diligence, business relationships and group-wide controls to the European Commission.
- **2 July 2026:** **In force** The national PSAN regime ended; providers without MiCA authorisation were delisted and must wind down.
- **1 January 2026:** **In force** AMLA took over the EBA's AML/CFT mandates; existing EBA guidelines remain in force until replaced. DAC8 crypto tax reporting applies from the same date.
- **25 December 2025:** **In force** Décret n° 2025-1276 sets DAC8 tax due diligence; existing users must provide tax-residence self-certifications before 1 January 2027.

11 What this means for identity verification

- **Two routes.** Offer certified eIDAS identity where available and a two-measure fallback, such as a document check plus an own-name bank payment, or a certified PVID service.
- **A document copy is one measure only** and always needs a second.

- **Verify every occasional customer**, whatever the amount.
- **Biometrics need explicit consent**, a non-biometric route and an impact assessment; keep templates on the device where possible.
- **Capture travel-rule and tax data at onboarding**: address, document number or date and place of birth, and tax residence.
- **Check self-hosted wallets**: ownership above €1,000, risk-based measures below it.
- **Use IP and device signals** as risk inputs, and re-verify when data are doubtful or risk changes.

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 onboarding combining ID document capture and verification (including NFC) with face match and biometric liveness, to support a two-measure verification route.
- AML screening against sanctions, asset-freeze, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYC questionnaires and proof of address to collect the customer data that travel rule messages and enhanced due diligence require.
- KYB and beneficial owner verification for corporate customers, with configurable risk-based workflows in a no-code workflow builder.
- Cloud, on-premises or hybrid deployment with an audit trail for each check.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), Articles 59, 62, 63, 65, 111, 143, 149 and Annex IV, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, recital 30, Articles 14, 16, 25, 26 and 40, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2024/1624 (AMLR), Articles 19, 22, 79 and 90, EUR-Lex, eur-lex.europa.eu
- Directive (EU) 2023/2226 (DAC8), Article 2, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2016/679 (GDPR), Articles 9, 33 and 35, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2024/1689 (AI Act), Annex III, point 1(a), EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2022/2554 (DORA), Article 2(1) (f), EUR-Lex, eur-lex.europa.eu
- Commission Delegated Regulation (EU) 2025/301 [time limits for major ICT incident reports], Article 5, EUR-Lex, eur-lex.europa.eu
- Loi n° 78-17 du 6 janvier 1978 (Informatique et Libertés), article 6, Légifrance, legifrance.gouv.fr
- Code monétaire et financier, article L561-45 [indirect right of access through the CNIL], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, article L561-18 [confidentiality of suspicious transaction reports], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, article L561-2 [obliged entities], version in force since 5 August 2026, Légifrance, legifrance.gouv.fr
- Code monétaire et financier, articles L561-5, L561-6, L561-10 and L561-12 [customer due diligence, vigilance, retention], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, articles R561-5, R561-5-1 and R561-5-2 [identification and verification measures], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, article L561-15 [suspicious transaction reporting], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, articles L561-36 and L561-36-1 [AML/CFT supervision], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, article L562-4 [asset freezes], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, articles L561-10-3 and L561-10-4 [correspondent relationships, self-hosted addresses], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, article R561-10 [occasional customers], version in force since 25 December 2024, Légifrance, legifrance.gouv.fr
- Code monétaire et financier, article R561-21-1 [enhanced measures for self-hosted addresses], Légifrance, legifrance.gouv.fr
- Code monétaire et financier, article L621-9 [AMF supervisory scope], Légifrance, legifrance.gouv.fr

- **Code monétaire et financier, article L621-15** [AMF sanctions], version in force since 27 June 2026, Légifrance, legifrance.gouv.fr
- **Décret n° 2025-1276 du 19 décembre 2025** [DAC8 reporting and due diligence for crypto-asset service providers], Légifrance, legifrance.gouv.fr
- **Rapport au Président de la République relatif à l'ordonnance n° 2024-937 du 15 octobre 2024**, Légifrance, legifrance.gouv.fr
- **Code monétaire et financier, article L612-39** [ACPR sanctions], version in force since 10 April 2026, Légifrance, legifrance.gouv.fr
- **Loi n° 2023-171 du 9 mars 2023, article 8** [end of the PSAN regime], Légifrance, legifrance.gouv.fr
- **Arrêté du 28 mars 2021 relatif à la certification de conformité des services d'entrée en relation d'affaires à distance**, Légifrance, legifrance.gouv.fr
- **AMF, Liste des PSAN radiés** [delisted PSAN], updated 10 July 2026, amf-france.org
- **AMF, Crypto-assets: end of the PACTE law and MiCA transitional period**, 6 July 2026, amf-france.org
- **AMF, PSCA authorisation application forms**, 12 December 2025, amf-france.org
- **AMF, warning on unauthorised crypto-asset entities**, 8 July 2026, amf-france.org
- **AMF, application of EBA guidelines on restrictive measures to crypto-asset service providers (DOC-2025-02)**, 7 April 2025, amf-france.org
- **AMF, position DOC-2024-08** [EBA travel rule guidelines], 19 December 2024, amf-france.org
- **ACPR, Avis de conformité aux orientations EBA/GL/2024/11** [travel rule guidelines], December 2024, acpr.banque-france.fr
- **ACPR, Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle**, paragraphs 32 to 48, page updated 24 September 2026, acpr.banque-france.fr
- **ACPR, Tracfin and DG Trésor, Principes d'application sectoriels relatifs aux PSAN**, November 2022, acpr.banque-france.fr
- **Banque de France, Révision du règlement MiCA : les autorités françaises publient leurs propositions conjointes**, 21 October 2026, banque-france.fr
- **Tracfin, Quand et comment déclarer un soupçon ?**, economie.gouv.fr
- **Tracfin, AML/CFT: Threat Assessment 2024-2025 (Volume III)**, French edition 29 September 2025, pages 7 and 20, economie.gouv.fr
- **ACPR and AMF, Forum Fintech 2025, LCB-FT workshop**, 9 October 2025, slides 46 to 49, acpr.banque-france.fr
- **AMLA, AMLA identifies AML/CFT priorities for the review of MiCA**, 7 October 2026, amla.europa.eu
- **CNIL, Recommandation relative à l'authentification multifacteur** [sections 3.3 and 3.4], adopted 20 March 2025, cnil.fr
- **CNIL, Premiers éléments d'analyse : Blockchain (chaîne de blocs)**, September 2018, page 8, cnil.fr
- **CNIL, Les sanctions prononcées par la CNIL** [entry of 10 October 2024], cnil.fr

- EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, version 2.0, adopted 7 July 2026, paragraph 48, edpb.europa.eu
- Direction générale du Trésor, Registre national des gels, gels-avoirs.dgtresor.gouv.fr
- INPI, FAQ on beneficial owners and register access, inpi.fr
- ESMA, Markets in Crypto-Assets Regulation (Interim MiCA Register), last update 22 October 2026, esma.europa.eu
- EBA, Guidelines amending the ML/TF risk factors guidelines (EBA/GL/2024/01), Guideline 21, 16 January 2024, eba.europa.eu
- EBA, Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15), 22 November 2022, eba.europa.eu
- AMLA, EBA and AMLA complete handover of AML/CFT mandates, amla.europa.eu
- AMLA, AMLA finalises key standards for the private sector, 1 October 2026, amla.europa.eu