



Identomat

COMPLIANCE GUIDE

# Crypto & Virtual Assets Compliance in Poland

COUNTRY **Poland**

INDUSTRY **Crypto & Virtual Assets**

LAST UPDATED **20 October 2026**

KEY REGULATORS **General Inspector of Financial Information · Polish Financial Supervision  
Authority · European Securities and Markets Authority**

---

## Key takeaways

---

- Poland has not passed the national law needed to apply the EU crypto rulebook (MiCA), so no Polish authority can issue a crypto-asset service licence as of October 2026.
- Since 2 July 2026, being listed in Poland's old virtual currency register no longer allows a firm to provide crypto services. Polish customers can be served only by a provider licensed in another EU country that has notified its home regulator.
- Every crypto business serving Polish customers must still verify identity before the account opens, and also for one-off crypto transactions worth EUR 1,000 or more, under the Polish anti-money laundering act.
- Onboarding fully online is allowed, but the law treats it as higher risk unless it is backed by an electronic identity or an EU trust service.
- Each crypto transfer must carry sender and recipient details (the "Travel Rule"). For transfers above EUR 1,000 to or from a private wallet, the provider must check that the customer controls that wallet.

The Polish market is restricted for domestic crypto firms and open, through the EU passport, to providers authorised elsewhere in the EU. The binding obligations today come from three places: the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing, the directly applicable EU Regulation 2023/1114 (MiCA), and the EU Regulation 2023/1113 on information accompanying crypto-asset transfers.

The principal authorities are the General Inspector of Financial Information (GIIF) for anti-money laundering, the Polish Financial Supervision Authority (KNF), and the European Securities and Markets Authority (ESMA) for the EU register of authorised providers. The biggest obstacle for a new entrant is the absence of a Polish licensing route: a firm that wants to operate from Poland today has to obtain authorisation in another member state.

### CONTENTS

- |                                                        |                                                              |
|--------------------------------------------------------|--------------------------------------------------------------|
| <a href="#">1 Who regulates this sector</a>            | <a href="#">7 Sector-specific obligations</a>                |
| <a href="#">2 Licensing and authorisation</a>          | <a href="#">8 Risk indicators and red flags</a>              |
| <a href="#">3 AML, KYC and customer due diligence</a>  | <a href="#">9 Enforcement and penalties</a>                  |
| <a href="#">4 Identity verification and onboarding</a> | <a href="#">10 Recent changes and what to watch</a>          |
| <a href="#">5 Digital channels: what's different</a>   | <a href="#">11 What this means for identity verification</a> |
| <a href="#">6 Data protection and biometrics</a>       | <a href="#">▪ Sources</a>                                    |

## 1 Who regulates this sector

| Authority                                                              | Remit for crypto                                                                                         | Level         | Official site                                                         |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------|
| General Inspector of Financial Information (GIIF), Ministry of Finance | Financial intelligence unit; receives reports; inspects compliance with the AML act                      | National      | <a href="https://gov.pl/web/finanse">gov.pl/web/finanse</a>           |
| Director of the Tax Administration Chamber in Katowice                 | Keeps the register of virtual currency activities; closed to new entries since 30 December 2024          | National      | <a href="https://gov.pl/web/ias-katowice">gov.pl/web/ias-katowice</a> |
| Polish Financial Supervision Authority (KNF)                           | Competent authority for e-money token issuers; named as the future MiCA authority in the unenacted bills | National      | <a href="https://knf.gov.pl">knf.gov.pl</a>                           |
| European Securities and Markets Authority (ESMA)                       | Register of MiCA-authorised providers; supervisory convergence                                           | Supranational | <a href="https://esma.europa.eu">esma.europa.eu</a>                   |
| European Banking Authority (EBA)                                       | Travel Rule Guidelines for crypto-asset transfers                                                        | Supranational | <a href="https://eba.europa.eu">eba.europa.eu</a>                     |
| President of the Personal Data Protection Office (UODO)                | Supervises processing of onboarding and biometric data                                                   | National      | <a href="https://uodo.gov.pl">uodo.gov.pl</a>                         |

Tax reporting on crypto users is handled by the National Revenue Administration (KAS), which sits within the Ministry of Finance.

## 2 Licensing and authorisation

### MiCA applies, but Poland has no competent authority In force

MiCA prohibits providing crypto-asset services in the EU without authorisation under its Article 63 (Article 59(1)). Every member state must designate a competent authority by national law (Article 93). The Ministry of Finance confirmed in June 2026 that no such

authority has been designated in Poland and that no procedure exists for obtaining a CASP authorisation. KNF reported on 23 June 2026 that no national authority, including KNF, has been designated for MiCA activity other than the issuance of e-money tokens, for which KNF is already competent.

## The transitional period has ended

Firms that operated under national law before 30 December 2024 could continue until 1 July 2026 under MiCA Article 143(3). In Poland these were mainly firms entered in the register of virtual currency activities. The Katowice tax chamber has stated that from 2 July 2026 an entry in that register does not authorise any crypto activity in Poland or abroad, and that the register is a record-keeping list rather than a licence. ESMA expects unauthorised providers to stop onboarding new EU clients immediately, limit services to an orderly exit, and keep full AML controls running while they wind down.

## Serving Polish clients through the EU passport

KNF's February 2026 position states that a CASP authorised in another member state may serve Polish clients, with or without a local presence, once its home authority has forwarded its notification under MiCA Article 65. That forwarding happens within 10 working days, and the provider may start from the date it is informed of it, or at the latest on the 15th calendar day after notifying. Non-EU firms cannot provide MiCA services to, or solicit, EU clients except under the narrow reverse-solicitation regime. Offerors of crypto-assets other than asset-referenced and e-money tokens cannot file a white paper in Poland, because there is no authority to receive it.

## National legislation Bill, not enacted

The government's Crypto-Assets Market Act, which would designate KNF as the competent authority, has been passed by the Sejm three times. The first two versions were vetoed by the President in December 2025 and February 2026, and the Sejm did not override either veto. A third version, passed on 15 May 2026, has also not entered into force as of October 2026. The European Commission has opened infringement steps against Poland on MiCA-related transposition (formal notice of 7 May 2025).

3

## AML, KYC and customer due diligence

Firms that exchange virtual currencies for means of payment, exchange one virtual currency for another, intermediate in those exchanges, or keep virtual currency accounts are obliged institutions under Article 2(1)(12) of the AML act (consolidated text Dz.U. 2025

poz. 644, as amended). A "virtual currency" is a digital representation of value that is not legal tender, e-money, a financial instrument or a bill of exchange, and that is accepted as a medium of exchange (Article 2(2)(26)).

#### **When due diligence applies**

On establishing a business relationship, for occasional transactions using virtual currency worth EUR 1,000 or more, on suspicion of money laundering, and when earlier identification data is in doubt (Article 35).

#### **What it includes**

Identifying and verifying the customer and beneficial owner, assessing the purpose of the relationship, and ongoing monitoring, including source of funds where warranted (Article 34).

#### **Enhanced due diligence**

Required in higher-risk cases and for high-risk third countries and politically exposed persons, with senior management approval and source-of-wealth checks (Articles 43 to 46).

#### **Risk assessment**

A documented business-wide assessment covering customers, geography, products and delivery channels, updated at least every two years (Article 27).

**Reporting.** Obligated institutions notify GILF of circumstances that may indicate money laundering or terrorist financing (Article 74), and of a reasonable suspicion about a specific transaction before carrying it out (Article 86). GILF can then suspend the transaction or block the account (Article 12). The Ministry of Finance confirms that crypto firms must also report above-threshold transactions under Article 72. For cash payments and transfers of funds that threshold is EUR 15,000. A designated manager files these reports on the institution's behalf (Article 8).

**Beneficial ownership.** For corporate customers, the firm must obtain a confirmation or extract from the Central Register of Beneficial Owners, but may not rely on it alone (Articles 37(3) and 39(1a)).

**Sanctions.** EU restrictive measures apply directly. GILF also keeps a national list of persons and entities subject to special restrictive measures (Article 12(1)(8)).

**Governance.** The firm must appoint a management board member responsible for AML, plus a compliance manager. It must also keep a written internal procedure, run staff training and operate an anonymous whistleblowing channel (Articles 6 to 8 and 50 to 53).

For a natural person, identification means recording the following (Article 36):

- name and citizenship;
- PESEL number, or date and country of birth where no PESEL has been issued;
- series and number of the identity document;
- address, where held;
- for a sole trader, also the business name, NIP and business address.

Verification confirms those data against an identity document, a current register extract, or other documents, data or information from a reliable and independent source. Where available, these include electronic identification means and trust services under the EU eIDAS Regulation (Article 37(1)). Firms may copy identity documents for due diligence purposes, and must tell the customer about the processing before onboarding (Article 34(4) and (5)).

Verification must be completed before the relationship is established. It may be completed during establishment only where needed for business continuity and the risk is low (Article 39). A firm that cannot complete due diligence must not open the relationship, must end an existing one, and must consider reporting to GIIF (Article 41). A firm may rely on another obliged institution's due diligence, but remains responsible for it (Article 47). It may also outsource due diligence to an agent treated as part of the firm under a written contract (Article 48). Politically exposed person status may be checked through a signed declaration given under penalty of perjury (Article 46(1)).

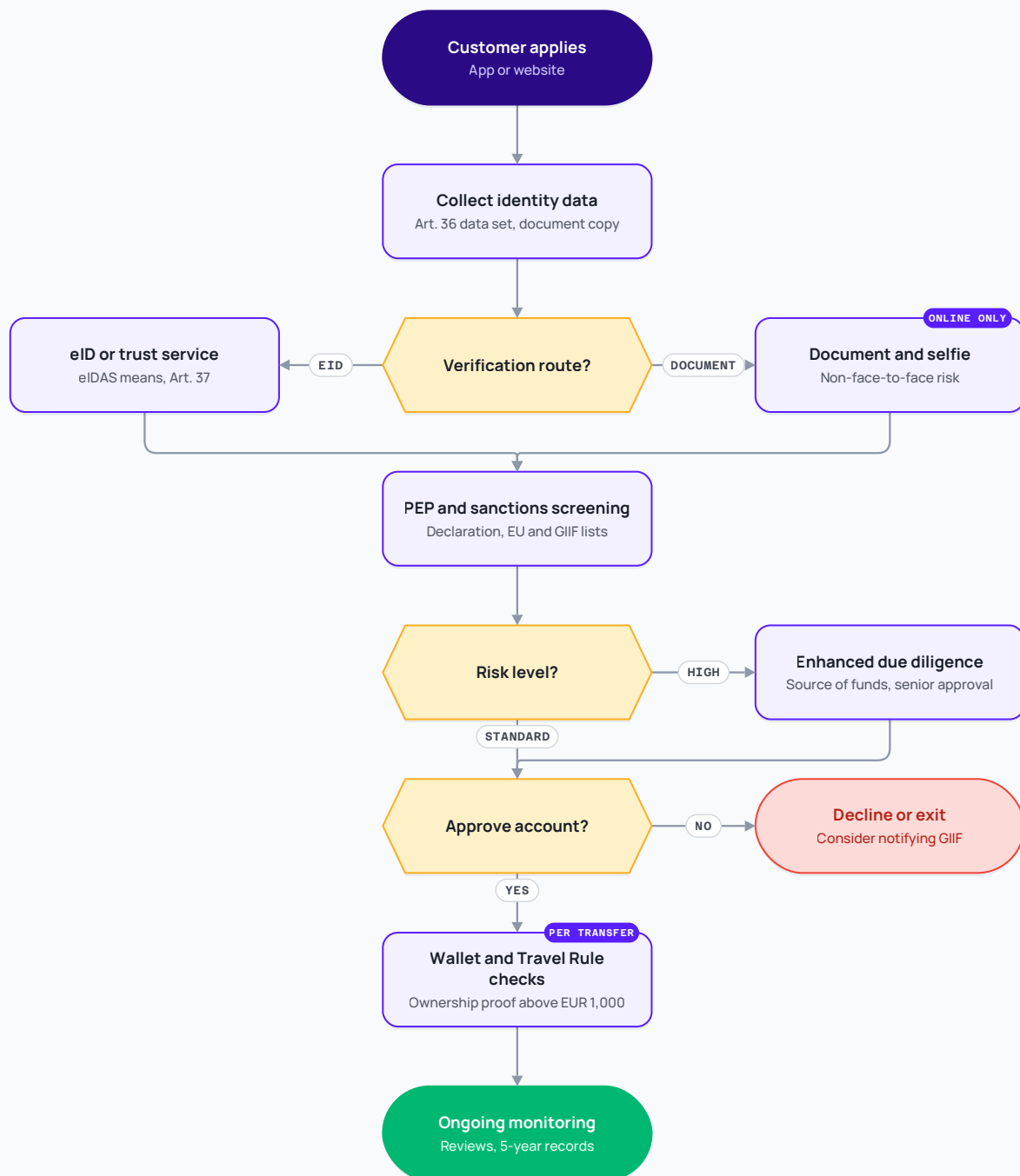


Figure 1. Remote customer onboarding and first transfer at a CASP serving Polish clients.

**Bottom line:** the AML act is channel-neutral on what must be verified and when, but onboarding without the customer present is a higher-risk factor unless it is offset by electronic identification or trust services.

| Requirement                                | In person                                                           | Online / remote                                                                      | Difference |
|--------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------|------------|
| <b>Due diligence triggers</b>              | Relationship; occasional virtual currency transaction of EUR 1,000+ | Same triggers                                                                        | Same       |
| <b>Risk classification</b>                 | Assessed on standard factors                                        | Higher-risk factor unless mitigated by eID or trust services                         | Differs    |
| <b>Accepted verification sources</b>       | ID document, register extract, reliable independent data            | Same list, including eID means and eIDAS trust services                              | Same       |
| <b>Timing of verification</b>              | Before the relationship starts                                      | Before the relationship starts                                                       | Same       |
| <b>Reliance and outsourcing</b>            | Permitted; firm remains liable                                      | Permitted; firm remains liable                                                       | Same       |
| <b>Record retention</b>                    | 5 years after the relationship ends                                 | 5 years, expressly including data from eID and trust services                        | Same       |
| <b>Serving Polish clients cross-border</b> | Requires MiCA authorisation; no Polish route                        | EU-authorised CASP may passport without local presence; non-EU firms may not solicit | Differs    |
| <b>Private (self-hosted) wallets</b>       | Not applicable to counter services                                  | Ownership or control check for transfers above EUR 1,000                             | Differs    |

## Remote onboarding as a risk factor

Article 43(2) (7) lists establishing or maintaining a relationship without the customer's physical presence as a higher-risk indicator. It applies where that risk "has not been mitigated in another way", including by electronic identification means and trust services under the eIDAS Regulation. Document-and-selfie onboarding is therefore lawful, but should be supported by a documented risk assessment and proportionate extra controls. The AML act sets no liveness or video-identification standard.

## Private wallets and the Travel Rule

Under Regulation 2023/1113 and the EBA Travel Rule Guidelines (EBA/GL/2024/11, applicable from 30 December 2024), the originator's CASP must send the required information no later than the start of the on-chain transaction. Where a transfer involves a self-hosted address, the CASP collects the counterparty information from its own customer. For amounts above EUR 1,000, it must check that the customer owns or controls the address using at least one accepted method:

- a supervised or unsupervised remote verification;
- a test transfer of a set small amount;
- a signed message from the wallet's key;
- another reliable technical means.

Verified addresses may be whitelisted.

## Pending changes

The EU AML Regulation 2024/1624 **Adopted, applies from 10 July 2027** covers crypto-asset service providers and states that eIDAS electronic identification can reduce onboarding risk to standard or even low.

## 6 Data protection and biometrics

---

The GDPR applies directly, supervised in Poland by UODO. The AML act supplies the legal basis to process identity document data and make copies for due diligence. It requires the customer to be informed of that processing before onboarding (Article 34(4) and (5)). Records, including information obtained through electronic identification and trust services, must be kept for five years from the end of the relationship or the occasional transaction. GLIF may require a further period of up to five years (Article 49).

The AML act does not address face images or liveness data specifically. Firms using biometric matching should treat it as sensitive processing under the GDPR, define its purpose and retention separately from the five-year AML record, and keep only what is needed to evidence the check. Any request to a counterparty for missing Travel Rule data must also use secure channels consistent with the GDPR, according to the EBA Guidelines.

## 7 Sector-specific obligations

---

### Travel Rule data handling

For natural persons, the originator information includes:

- full name as shown on the identity document or eID;
- address, with an ISO country code;
- an official document number, customer identification number, or date and place of birth.

A receiving CASP that detects missing data should set a deadline of no more than three working days within the EU, or five for transfers from outside it, extendable to seven for complex chains. It should then reject, return, suspend or execute the transfer on a risk basis. A counterparty that repeatedly fails to send the data should be reported to the competent authority within three months of being identified (EBA/GL/2024/11).

### Tax reporting of users In force

Poland's implementation of the EU tax-transparency Directive (DAC8), enacted as the Act of 13 February 2026, requires reporting crypto-asset service providers to collect and pass to the tax administration information on their users' transactions. Examples are buying, selling and exchanging one crypto-asset for another. Onboarding must therefore capture tax residence data in addition to AML identity data.

### Marketing claims

GIIF has warned that firms entered in the virtual currency register may not describe their activity as licensed or supervised under Polish law. Doing so may trigger action for misleading consumers (Communication No. 77).

## Risk indicators and red flags

### CRYPTO-ASSET TYPOLOGIES (EBA TRAVEL RULE GUIDELINES; AML ACT)

- **Mixing and obfuscation:** use of mixers, IP anonymisers or stealth addresses.
- **Pass-through chains:** funds or crypto-assets received and moved on quickly, lengthening the transfer chain.
- **Tainted addresses:** wallets or addresses known to be linked to suspicious activity.
- **Unregulated counterparties:** CASPs in countries with no licensing regime or no Travel Rule in place.
- **Sanctions exposure:** parties in jurisdictions under restrictive measures or with a high risk of evasion.
- **Repeat missing data:** counterparties that repeatedly send transfers without required originator data.
- **Unauthorised providers:** exposure to firms without MiCA authorisation, which the Katowice tax chamber classes as higher risk.
- **Anonymity-enhancing products:** services that hinder identification of the customer (AML act, Article 43(2) (6)).

## Enforcement and penalties

GIIF controls compliance with the AML act. According to the Ministry of Finance, GIIF had inspected 18 virtual currency firms since 2019 and directed customs and tax offices to inspect a further 87 in 2025. Administrative penalties are set out in Chapter 13 of the act. For a failure such as not applying due diligence, the Ministry describes the fine as up to twice the benefit gained or loss avoided. Where that amount cannot be established, the cap is the equivalent of EUR 1,000,000.

Under MiCA, any provider serving clients in Poland without authorisation is in breach of Article 59 regardless of the missing Polish act. ESMA has said national authorities may take coordinated action against unauthorised CASPs after the transitional period. Proposed national criminal penalties for unauthorised crypto services are contained in the unenacted Crypto-Assets Market Act and do not apply.

## Recent changes and what to watch

---

- **2 July 2026** **In force** : entries in the Polish virtual currency register no longer authorise crypto activity; firms need MiCA authorisation.
- **1 July 2026** **In force** : the MiCA transitional period ended; ESMA expects unauthorised providers to wind down in an orderly way.
- **15 May 2026** **Bill, not enacted** : the Sejm passed a third Crypto-Assets Market Act designating KNF; it has not entered into force.
- **29 April 2026**: the European Commission sent Poland a reasoned opinion on implementing Regulation 2023/1113; further infringement steps on MiCA are possible.
- **13 February 2026** **In force** : the DAC8 implementing act introduced reporting of crypto-asset users to the tax administration.
- **February 2026**: KNF confirmed that EU-authorised CASPs may serve Polish clients and that domestic firms would lose their basis to operate after 1 July 2026.
- **10 July 2027** **Adopted, applies from 10 July 2027** : the EU AML Regulation replaces much of the national due diligence framework.

## What this means for identity verification

---

Onboarding flows for Polish customers need to capture the Article 36 data set, including PESEL where issued, the identity document number and citizenship. Verification must be finished before the account becomes active. eIDAS-based electronic identification and qualified trust services are named in the act as both verification sources and risk mitigants. Document-and-selfie checks are permitted, but a firm should record why the residual non-face-to-face risk is acceptable.

Beyond onboarding, crypto adds transfer-level identity work: originator and beneficiary data on every transfer, and proof of control of private wallets above EUR 1,000. Re-verification is required when data is in doubt, when a suspicion arises, and when customer or beneficial-owner details change (Article 35). Evidence from every channel, including eID results, must be retrievable for five years. Tax residence collection for DAC8 should be designed into the same flow.

## 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 before account activation, with ID document capture (including NFC), face match and biometric liveness.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for corporate clients alongside Central Register checks.
- No-code workflows that add enhanced due diligence steps and keep 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

- Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu [Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing], consolidated text Dz.U. 2025 poz. 644 as amended (codified text as at 8 October 2026), Articles 2, 8, 12, 27, 33 to 53, [eli.gov.pl](https://eli.gov.pl)
- Ministry of Finance, answer to parliamentary question No. 16605 on crypto-asset regulation, 9 June 2026, [sejm.gov.pl](https://sejm.gov.pl)
- Ministry of Finance, answer to parliamentary question No. 12336, 30 September 2025, [sejm.gov.pl](https://sejm.gov.pl)
- KNF, Informacja dot. zakończenia okresu przejściowego dla dostawców usług w zakresie kryptoaktywów [Information on the end of the transitional period], 23 June 2026, [knf.gov.pl](https://knf.gov.pl)

- UKNF, Stanowisko w związku z brakiem wyznaczenia w Polsce organu właściwego w zakresie nadzoru nad rynkiem kryptoaktywów [Position on the absence of a competent authority], February 2026, [knf.gov.pl](https://knf.gov.pl)
- Tax Administration Chamber in Katowice, Informacja dla klientów podmiotów wpisanych do Rejestru Działalności w zakresie Walut Wirtualnych [Information for clients of registered virtual currency firms], June 2026, [gov.pl](https://gov.pl)
- GIIF, Komunikat nr 77 w sprawie statusu podmiotów prowadzących działalność w zakresie walut wirtualnych [Communication No. 77], 14 February 2024, [gov.pl](https://gov.pl)
- Ministry of Finance, Rada Ministrów przyjęła projekt ustawy o zmianie ustawy o wymianie informacji podatkowych z innymi państwami [DAC8 implementing bill], 17 December 2025, [gov.pl](https://gov.pl)
- ESMA, Public Statement on unauthorised CASPs as the MiCA transitional period ends, ESMA75-113276571-1710, 23 June 2026, [esma.europa.eu](https://esma.europa.eu)
- EBA, Guidelines on information requirements in relation to transfers of funds and certain crypto-assets (Travel Rule Guidelines), EBA/GL/2024/11, 4 July 2024, sections 4.3 to 4.8, [eba.europa.eu](https://eba.europa.eu)
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, EUR-Lex, [eur-lex.europa.eu](https://eur-lex.europa.eu)
- Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, EUR-Lex, recitals 14 and 66, [eur-lex.europa.eu](https://eur-lex.europa.eu)