



Observatoire ARGA

INTERNATIONAL ANALYTICAL REPORT

D-26. MiCA and Access to Financial Services

Customers with Disputed Legal Status

AML/CFT, Sanctions and De-risking

Author:

Sergey Khrabrykh - President of ARGA, PhD

Organization: Observatoire ARGA

Correspondence: 21 rue de l'Aviation, 64600 Anglet, France

Contact: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org

28 September 2026

Contents

Executive summary	3
1. Research question and method	3
2. The legal map in September 2026	4
3. What MiCA provides and what it does not guarantee	5
4. Breaking disputed status into separate facts	6
5. AML/CFT: risk, due diligence and lawful refusal	7
6. A sanctions match and a mandatory restriction	7
7. Russian nationality, residence and exemptions	8
8. Asylum and identity documents	9
9. INTERPOL and foreign criminal proceedings	10
10. PEP status, adverse media and corporate disputes	11
11. Source of funds and crypto-asset history	12
12. The travel rule and self-hosted addresses	12
13. Blockchain analytics and what an address proves	13
14. Suspension, freezing and termination	14
15. De-risking and the limits of a duty to serve	15
16. Data, automated decisions and correction	16
17. Complaints: issue, recipient and evidence	16
18. The French route and payment-service component	17
19. Judicial guidance and limits of analogy	18
20. Six practical situations	19
21. The customer dossier and review record	21
22. The decision model and implementation	22
23. ARGAs position and conclusions	23
Sources and references	24

Source cut-off: 28 September 2026. Keywords: MiCA; AML/CFT; sanctions; financial access; INTERPOL; review of restrictions.

Executive summary

A customer's disputed legal status is not an independent basis for a single, universal prohibition on financial services. The expression may refer to very different circumstances: a sanctions name match, foreign criminal proceedings, an INTERPOL notice, politically exposed person status, an unresolved asylum application, disputed beneficial ownership or an error in a commercial database. Each requires its own legal classification and assessment of evidence.

MiCA regulates crypto-asset markets and service providers, but does not give every person an unconditional right to open a crypto account. Equally, a provider's MiCA authorisation does not exempt it from AML/CFT, sanctions, transfer-information requirements or data protection. Practical problems arise when these regimes are conflated: suspicion is described as a sanction, contractual termination as confiscation, or an automated score as a mandatory state decision. [1-3]

This report proposes a sequence: identify the provider and service; establish the actual obstacle; check the applicable rule; distinguish a mandatory prohibition from manageable risk; assess the customer's evidence against the specific issue; make a targeted decision and define how it can be reviewed. Where a prohibition applies, commercial convenience cannot justify proceeding. Where none applies, a complex profile should not automatically become proof that all assets have an unlawful origin.

The date of the assessment matters. As of 28 September 2026, the maximum transitional period for previously operating providers under Article 143(3) MiCA has ended, having expired on 1 July 2026. AML/CFT mandates passed from the EBA to AMLA on 1 January 2026, while the main application date of the new AML Regulation 2024/1624 is 10 July 2027. These are separate developments. They do not mean that the entire future supervisory and substantive framework already applies. [4-6]

The practical analysis includes six hypothetical situations, a customer dossier, review of blockchain evidence, responses to withdrawal restrictions, complaint routes and a reasoned decision model. ARGAs position combines implementation of mandatory restrictions with individual assessment, accurate data and meaningful review. It is not a proposal to bypass controls. The objective is to identify the real legal obstacle and correct restrictions that arise from error or disproportionate decision-making.

1. Research question and method

The central question is how to distinguish a lawful refusal of a crypto-financial service from unjustified exclusion of a customer whose status is disputed. The answer depends on the service, the provider's jurisdiction, the restriction imposed and the evidence. The report therefore does not begin from an abstract “right to cryptocurrency”. It examines separate decisions: onboarding, transfers, custody, restrictions on disposal, termination and return of assets.

The first set of questions concerns law: whether MiCA covers the product and provider, which AML regime applies, whether a sanctions prohibition exists and who can authorise a derogation. The second concerns facts: whether the correct person has been identified, the status of criminal

proceedings, control of an address and the source of funds. The third concerns process: what the customer may be told, what evidence could change the decision and which body can address the dispute.

Priority is given to legislation, official materials from ESMA, the EBA, AMLA, the European Commission and INTERPOL, and judgments. Supervisory guidance is considered within its scope and legal function. In particular, EBA principles concerning risk management and financial access do not automatically impose a universal duty on every crypto provider to contract with every applicant. ARGAs proposed procedures are identified as an organisational model. [7-10]

The report does not estimate the proportion of unjustified refusals because it does not possess a comparable dataset of individual decisions. The six practical situations are hypothetical. Judicial decisions are examined according to their actual subject matter, including where their reasoning is useful by analogy. A banking-access or credit-scoring judgment is not described as a precedent directly compelling a crypto exchange to onboard a customer.

The model requires current information. Sanctions annexes, provider status and representatives' authority may change. Historical registration, an earlier screening result or an old letter expressing no objection offers no indefinite assurance. A new assessment should nevertheless retain relevant favourable information from the previous dossier. The history of review should show dates and reasons for changed conclusions rather than erase earlier findings.

2. The legal map in September 2026

MiCA, Regulation 2023/1114, establishes requirements for specified crypto-assets and services. Regulation 2023/1113 governs information accompanying transfers and amends the AML framework for crypto-asset service providers. Directive 2015/849, as amended, and national implementing legislation remain relevant before the new framework applies. Sanctions regulations operate independently. The GDPR governs personal-data processing during screening and decision-making within its scope. [1-4, 11, 12, 15]

Article 143(3) MiCA allowed certain existing providers to continue within the applicable transitional conditions, no later than 1 July 2026. This was not equivalent to MiCA authorisation and did not create a full EU passport. In September 2026, an old national registration alone no longer answers whether a provider may continue regulated services. The current basis must be checked: authorisation or the applicable MiCA route for an eligible financial institution. [1, 6]

AMLA received the EBA's AML/CFT mandates on 1 January 2026. This institutional handover did not immediately replace every national supervisor. Direct AMLA supervision of selected entities is scheduled to begin in 2028. A customer should not send every wallet-restriction complaint to AMLA as though it were a universal appeal tribunal. The relevant national authority, contractual party and remedy must be identified. [5]

Regulation 2024/1624 mainly applies from 10 July 2027. Its future provisions are useful for preparation, but should not be cited without qualification as obligations already applicable on 28 September 2026. A provider's decision should identify the rule currently governing the action.

Preparing internally for a future standard may be legitimate, but a corporate policy should be described as such rather than presented as an already applicable statutory prohibition. [4]

A single transaction may generate several different answers. The provider may be authorised under MiCA, while the particular recipient is sanctioned. A transfer may not be prohibited by sanctions, but mandatory information may be missing. Identity may be verified while the source of a significant amount remains unexplained. Separate classification permits a response to the actual problem instead of an indefinite restriction under the generic word “compliance”.

A practical legal map should also state the date of each conclusion. The provider's authority to operate, the customer's eligibility and a transfer's permissibility are checked at relevant decision points, not assumed permanently from onboarding. The map should remain concise enough for operational staff to use, with supporting analysis available for difficult questions. Its purpose is to prevent different legal regimes from disappearing into one undifferentiated risk score.

3. What MiCA provides and what it does not guarantee

MiCA imposes requirements concerning provider organisation, conduct toward clients, safeguarding and complaints. Articles 66, 70, 71 and 75 can matter in disputes about service quality and custody. The existence of those obligations does not establish an unconditional right for every applicant to obtain every product. Any claim to compel conclusion of a contract requires an independent legal basis. [1]

The service must be identified before the refusal is analysed. Custody and administration, exchange, execution of orders and transfers have different characteristics. A crypto-asset qualifying as a financial instrument may fall outside the relevant MiCA regime and within another framework. The marketing term “wallet” is equally inconclusive: a business may hold keys, supply software only or offer a package of distinct services.

The practical check begins with the legal entity named in the agreement and its authorised services. A global group's logo does not establish that the contracting company is authorised in the EU. It matters which entity owes the asset-return obligation, controls access and made the restriction decision. Escalation to a parent company may help organisationally, but does not replace engagement with the correct contractual party.

Authorisation is not a guarantee of returns, absolute safety or deposit-style insurance for crypto-assets. Regulated status addresses particular organisational risks and creates obligations, but does not eliminate market risk or a product's limitations. A complaint should identify the obligation allegedly breached rather than assume that a licence makes every loss automatically compensable.

An applicant and an existing client may have different contractual rights. Refusing a new product, terminating an existing service and retaining property already accepted are separate actions. Even where a provider may decline to continue the relationship, each restriction on assets needs its own basis and applicable exit obligations must be performed. A commercial closure decision does not transfer ownership of the customer's assets to the provider.

This distinction also helps define a realistic remedy. A customer may be unable to force continued trading but still have a strong claim concerning inaccurate data or lawful return of custody assets. Combining every grievance into a demand for permanent unrestricted access can obscure the strongest point. A precise claim follows the actual obligation and the particular action being challenged.

4. Breaking disputed status into separate facts

“Disputed status” is dangerously imprecise. A criminal allegation, sanctions designation, civil dispute and PEP classification are not interchangeable. Each event should have a record identifying its source, date, competent body, procedural stage, personal identifiers, legal consequence and any challenge or subsequent decision. This prevents several weak signals from becoming a false impression of one conclusively established serious fact.

Proceedings do not prove guilt, but may be relevant to risk. Acquittal, discontinuance, refusal of extradition and deletion of INTERPOL data also have different grounds and limits. Refusal to extradite because of mistreatment risk does not necessarily determine the source of particular funds. Deletion of a notice is not an acquittal. Each favourable document should be used for the proposition it actually supports.

Recognised refugee status and an asylum application are different. A residence permit, an applicant's temporary document and confirmation that an application was lodged may perform different legal functions. For a sanctions exemption, lawful presence in a broad sense may not be enough: the particular statutory category matters. For AML purposes, identity verification and the reliability of the documents remain material.

ARGA proposes separating factual from legal uncertainty. In the first case, it may be unknown whether the customer controls an address. In the second, control is established but the application of a rule is disputed. More evidence addresses the factual question; a qualified interpretation or competent authority's decision may be needed for the legal question. Repeated requests for bank statements cannot resolve a dispute over the meaning of a residence exemption.

The person's status must also be distinguished from the assets' status. A non-designated customer may receive a transfer from a prohibited counterparty. Someone mentioned in adverse media may hold well-documented lawful assets. Customer and transaction reviews complement one another. A favourable finding in one should not be transferred to the other without examining the relevant facts.

The record should avoid conclusions stronger than the evidence. “Proceedings have been opened”, “the person is wanted” and “the person committed the offence” are distinct propositions. Compliance may act preventively on risk without proving the third. It should still preserve that distinction internally and in any lawful communication rather than convert a preventive decision into an unsupported public allegation.

5. AML/CFT: risk, due diligence and lawful refusal

AML/CFT controls require customer identification and verification, establishment of beneficial ownership, understanding of the relationship's purpose and ongoing monitoring within the applicable framework. Article 14(4) of Directive 2015/849 addresses inability to meet specified due diligence requirements, including consequences for transactions or relationships and consideration of a suspicious transaction report. Implementation depends on national law and the entity concerned. [3]

Enhanced due diligence is not punishment. It responds to increased risk and may involve additional information about funds, activity and counterparties. A request should nevertheless address the identified question. Where the issue is a property sale, a twenty-year professional history may not be the most relevant evidence. Proportionality means an adequate assessment, not abandoning required checks for the customer's convenience.

EBA guidance on crypto-asset risks considers the product, customer, geography and delivery channel. An unauthorised counterparty, opaque structure or unusual route may increase risk. The overall analysis should explain the connection to the transaction. Self-custody or foreign nationality should not be declared proof of money laundering without further analysis. [7]

A provider may lawfully refuse where material information cannot be established or the risk cannot be acceptably mitigated. The opposite error is to assume that absence of a conviction requires every transaction to proceed. AML is preventive and does not require a criminal standard of proof in every decision. Its preventive purpose nevertheless does not justify describing a customer as a criminal without an appropriate basis.

The internal decision should identify what information is missing and why it matters. If an alternative document is offered, its evidential function should be assessed rather than rejected solely because it differs from a template. An objectively unavailable document is not always replaceable. But examining possible substitutes is what distinguishes individual review from automatic exclusion of a category.

The provider should also distinguish an inability to verify from a customer's unwillingness to cooperate. Both may ultimately prevent service, but they are different facts and may warrant different attempts to resolve the issue. The record should show what was requested, the customer's explanation and whether an alternative was feasible. It should not invent refusal to cooperate where the obstacle was technical or legal.

6. A sanctions match and a mandatory restriction

An automated match begins an assessment; it is not a completed legal conclusion. Names, spelling variants, birth dates, nationality, addresses and other available identifiers should be compared. If the list contains little information, uncertainty should be recorded. A provider should not confidently attribute designated status to someone solely because of a common surname. A serious match must nevertheless be resolved in time to prevent a prohibited transaction.

Where an asset-freeze regime applies, the analysis addresses the assets belonging to, owned, held or controlled by the relevant persons within the applicable instrument, and the prohibition on making funds or economic resources available. Regulation 269/2014 and its annexes require their own assessment. Exceptions and authorisation conditions cannot be inferred merely from a transfer's humanitarian purpose. [11]

Freezing is not confiscation and does not transfer ownership to the provider. It restricts disposal under the relevant regime. Payment of basic needs or legal expenses depends on the specific derogation, conditions and competent authority. An exception appearing in legislation does not always mean that a customer or platform can apply it without prior authorisation.

Jurisdiction also matters. An EU operator implements applicable EU and national requirements; foreign connections may create additional obligations. A multinational group's policy may be broader than the mandatory regime. The provider should distinguish that policy from a legal prohibition. It may influence a contractual decision, but should not automatically be described as a state obligation to freeze property.

After a false match is resolved, linked systems need correction. If only one customer record is changed, automated monitoring may restore the error at the next update. The decision should retain identifiers and the reason for excluding the match without creating permanent immunity from future screening. A new designation or changed information requires fresh analysis, while recurrence of an already disproved signal requires use of the earlier result.

EBA Guidelines 2024/14 and 2024/15 address internal arrangements for implementing restrictive measures within their specified scope. They support governance and controls, but do not themselves designate a customer. The applicable mandatory measure must be established from the relevant legal act and annexes. [10]

The scope of the restriction should be communicated internally to staff who execute it. A targeted asset measure and a prohibition on providing a service are not technically identical. Incorrect implementation may either leave a prohibited route open or unnecessarily block unrelated actions. Legal classification therefore needs a clear operational translation, not merely a warning banner attached to the customer.

7. Russian nationality, residence and exemptions

Article 5b of Regulation 833/2014 requires careful classification. Following the 2025 amendments, paragraph 2 covers crypto-asset services within the MiCA definition and specified payment and electronic-money services for the relevant Russian persons. An older explanation limited to crypto custody should not be used as a complete statement of current scope. A service prohibition and an individual asset freeze under another regulation remain distinct regimes. [12, 14]

Paragraph 3 provides exemptions for specified nationality categories and temporary or permanent residence permits in the EU, EEA or Switzerland. The document's validity and legal nature must be checked. An Article 5b exemption does not remove an independent personal designation or AML/CFT obligations. Conversely, a Russian passport does not justify ignoring an applicable exemption and treating the service prohibition as unconditional.

A residence-extension document requires examination under national law. Expiry of a plastic card does not invariably end residence rights, but an application receipt is not invariably equivalent to the permit described in the sanctions provision. The customer should provide the document, information about its effect and, where needed, official clarification. The provider assesses its legal function rather than only whether it fits an upload field designed for a standard card.

Regulation 2026/1848 further amended restrictions concerning ownership, control and governing-body positions held by relevant Russian persons in crypto-service providers. This concerns the provider's structure and should not be conflated with an individual customer's access to service. The contracting company's status and structure require one assessment; the customer's eligibility requires another. Exceptions must be examined under the current wording of the relevant provision. [13]

ARGA proposes two independent conclusions: applicability of personal restrictive measures and applicability of service restrictions. If neither prohibits the operation, or a relevant exemption applies, AML assessment remains separate. If any mandatory prohibition persists, lawful origin of the funds does not by itself remove it. This sequence guards against both over-refusal and an incorrectly authorised transaction.

The relevant status should be checked when it changes, not only at onboarding. A renewed permit may resolve an earlier question; loss of an applicable status may create a new one. The provider's system should be able to process both directions. A one-way mechanism that adds restrictions but cannot recognise verified favourable changes is not a reliable implementation of a status-dependent rule.

8. Asylum and identity documents

Asylum may explain missing documents from the country of origin, address changes and an interrupted banking history. Those circumstances warrant careful examination but do not prove financial wrongdoing. Documents issued by the host state, official decisions and competent-authority confirmations may have independent evidential value. Acceptance should be assessed under applicable law and identity-verification reliability, rather than the convenience of a standard document list.

Identity, residence rights and source of funds are separate propositions. A protection decision may establish status and the context of persecution, but cannot replace a property-sale contract. A bank statement shows money movements but does not automatically establish residence. Assigning documents to the facts they prove reduces irrelevant requests and helps the customer understand the remaining gap.

The EBA has highlighted unjustified exclusion of vulnerable customers and the need to consider individual risk profiles. Its financial-access guidance offers risk-management approaches, but its addressees and scope must be checked. Using those approaches as an ARGA model for crypto services does not create a general wallet-opening entitlement that the law does not provide. It supports examination of alternatives to complete refusal where the law permits them. [9]

Possible alternatives include a restricted service range, verified funding channels or additional checks on particular operations. They must reduce the specific risk and be operationally realistic. A limit is not a solution where the service is expressly prohibited for the person. Nor should conditions be made so narrow that a nominally available product is unusable without an explanation of the underlying reason.

Contacting authorities in the alleged country of persecution to verify a document can create danger. It should not be routine without assessment of its legal basis and consequences. Reliable host-state channels and lawfully available evidence should be preferred where suitable. Protecting the applicant is compatible with due diligence: it requires a safe verification source, not unconditional acceptance of every copy.

The provider should document why an alternative source is reliable. A letter from an authorised host-state body, for example, may answer a particular identity or status question while leaving financial history unresolved. A structured assessment recognises that contribution instead of treating the entire customer as either fully verified or wholly unverifiable. This is particularly useful where displacement has fragmented the available evidence.

9. INTERPOL and foreign criminal proceedings

An INTERPOL Red Notice is a request for international police cooperation, not an international arrest warrant or a conviction. Published information may be a material screening signal, but should not be expanded into automatic sanctions freezing. The specific legal basis for restricting property must be established: an operative judicial order, sanctions measure, AML requirement or contractual decision. [16]

A customer dossier should distinguish domestic proceedings, an international notice and its public display. Disappearance from INTERPOL's website does not by itself prove deletion of all data. A CCF decision or official communication has different evidential significance. The provider should consider the document within its scope, date and subject matter, while checking whether independent grounds for review remain.

INTERPOL's Refugee Resolution provides safeguards concerning requests from the country of feared persecution under the confirmed conditions. It does not mean that every asylum applicant is automatically exempt from all notices or financial checks. Recognised refugee status, a pending application and a decision on particular data must be distinguished. This report does not propose that a financial provider replace INTERPOL's or an asylum authority's competence. [17]

Deletion of data may materially change the risk profile. It may nevertheless leave separate questions about money flows or a civil dispute unresolved. A favourable internal opinion should identify exactly which adverse factor has been removed and which questions remain. This avoids both disregarding the favourable decision and presenting it as universal proof that every asset is lawful.

Foreign allegations should be assessed with their procedural context. Relevant matters include access to defence, the case stage, judicial decisions and independent support for claimed political or corporate motivation. The customer's assertion of persecution does not alone establish abuse.

Equally, an accusing authority's statement should not be repeated as final guilt without qualification. A reliable dossier preserves the distinction between allegation and established fact.

The financial issue should remain identifiable throughout the review. A provider is not ordinarily deciding an extradition case, and a financial complaint should not become an unstructured retrial of every allegation. The useful question is how the available procedural evidence changes the specific risk or restriction. This keeps the assessment proportionate while allowing serious evidence of misuse to have real weight.

10. PEP status, adverse media and corporate disputes

PEP status triggers the AML measures applicable to that category rather than establishing unlawful wealth. The assessment addresses approval of the relationship, sources of wealth and funds, and enhanced monitoring where required. Family and close-associate connections are assessed within the statutory definitions. A prominent entrepreneur should not be classified as a PEP simply because their name frequently appears in the media. [3]

An adverse article requires identification of its primary source. Ten sites repeating one report do not provide ten independent confirmations. Date, procedural updates, identity and the nature of the claims matter. A report of a lawsuit is not a merits judgment; an arrest is not a conviction. An old headline omitting a later acquittal can systematically distort a profile.

Corporate conflict may generate competing fraud allegations and disputes over signing authority. The provider's immediate question may be who can operate the company's account rather than who is criminally responsible. Registration information, corporate resolutions, judicial measures and contractual authority should be examined. An unsupported shareholder letter may not justify handing over control, but may warrant a targeted review of potential unauthorised disposal.

ARGA recommends separating risk indicators from established restrictions in the staff interface. "Mentioned in a dispute" should not appear equivalent to "transaction prohibited". Every indicator should identify its source, confirmation level and review date. This reduces the likelihood of frontline staff making legal decisions from the colour of an automated customer card.

Where a publication is corrected or disproved, decisions dependent on it should be updated. The provider need not erase accurate history where retention is lawful, but should reflect subsequent developments. A precise record may state that allegations were made and later proceedings ended on a specified ground. This is more accurate than retaining the allegation without context or deleting every trace regardless of legal relevance.

The customer should also avoid overclaiming the effect of a favourable development. A civil settlement may end a dispute without establishing that every allegation was false. The provider can recognise that the litigation is resolved while preserving any independently relevant facts. Accurate description on both sides makes review more productive than competing claims that the entire history must either be accepted or erased.

11. Source of funds and crypto-asset history

The source of a particular amount differs from the general source of wealth. Property sales, salary, dividends and investment gains require different evidence. Crypto-assets add the connection between acquisition, custody, transfers and the current holding. The purpose is to explain a verifiable economic history, not create the largest possible archive without a clear connection to the amount under review.

A practical package works backwards from the current asset. It identifies network, asset type, quantity and address or provider account, then establishes the preceding receipt and acquisition basis. Exchange purchases may be supported by account records and a link to the funding payment instrument. A property sale may require the contract, payment evidence and subsequent transfer sequence. Dates and amounts should reconcile, allowing for fees and value changes.

Current portfolio value is not the initial investment. Price appreciation may explain the difference, but the calculation should be reproducible. The customer identifies quantities, acquisition dates and events changing the quantity held. “I made money in crypto” explains neither the initial capital nor title. Conversely, requiring bank income equal to today's market value may be methodologically mistaken where documented appreciation accounts for the increase.

Gifts, inheritances and family transfers are not automatically suspicious. They change the questions: who transferred the assets, on what basis, how the relationship is established and whether the donor's source requires further investigation. A family connection does not remove a sanctions prohibition or prove provenance. The depth of review depends on the particular risk and applicable requirements.

Where history is incomplete, the customer should identify gaps honestly and offer alternative evidence. Fabricated statements or a fictional retrospective contract make the position worse. The provider assesses what is genuinely necessary, whether independent verification is possible and whether a material uncertainty remains. No assurance should be given that a narrative letter cures every evidential gap. A good explanation organises evidence; it does not manufacture a missing fact.

A reconciliation schedule can be useful for a complex history. It connects opening quantities, acquisitions, disposals, fees and the closing balance, with supporting documents for material events. The schedule is an analytical aid rather than independent proof. Its value depends on the records beneath it and on explicit treatment of any assumptions, missing periods or valuation choices.

12. The travel rule and self-hosted addresses

Regulation 2023/1113 establishes information requirements for specified crypto-asset transfers within its substantive and territorial scope. They are not confined to large amounts. The EUR 1,000 threshold for particular self-hosted-address measures should not be turned into a general exemption for smaller transfers from information requirements. [2, 8]

For transfers exceeding that threshold to or from a self-hosted address, the relevant provider takes adequate measures to assess ownership or control by its customer in the circumstances addressed by

Articles 14(5) and 16(2). This does not mean that all self-hosted addresses are prohibited. Nor does cryptographic evidence of control prove the lawful origin of all assets where provenance requires separate assessment.

A provider should not demand a seed phrase or private key to establish control. Safe verification methods should be used within the applicable rules and technical architecture, without giving an employee power to dispose of the property. The method depends on address type, technical constraints and security. A public address, signature or other evidence may establish different propositions; the limits should be understood.

Missing originator or beneficiary information requires a process for detection, request and assessment. Rejection, suspension or another permitted response depends on the provider's role and the Regulation's conditions. Assets should not automatically be sent back to any address supplied: return can itself be a transfer requiring checks, including sanctions. The technical sending address is not always the correct address for returning a customer's assets.

Well-organised information exchange reduces mistaken restrictions. If a counterparty sends a misspelt name, the customer record and transfer message should be reconciled lawfully, retaining the original and correction. A formatting issue does not necessarily indicate a false identity. Repeated omissions and refusal to provide required information may have a different risk significance and warrant further examination.

The process should explain which participant must resolve the missing field. The customer may not control information transmitted by another provider, while the receiving provider may need to contact its counterparty through the appropriate channel. Assigning responsibility accurately prevents repetitive demands for information that the customer has already supplied but that has not been carried through the transfer process.

13. Blockchain analytics and what an address proves

A blockchain entry establishes a particular network event, but not necessarily the participant's identity or economic purpose. Analytics adds attribution and inferences about relationships between addresses. The decision should distinguish the observed transaction, an assigned label and a conclusion about control. Probabilistic clustering should not become legally established ownership without explanation.

A direct receipt from a confirmed prohibited person and a remote connection through a public service have different evidential weight. The number of intervening transactions does not itself create a safe boundary. Type of connection, chronology, amount, service characteristics and other facts matter. This report proposes no universally acceptable number of hops; the examined rules do not establish such a general test.

An automated label should have a basis available to the reviewer. If the vendor changes an attribution, the date and reason matter. An old analytics snapshot should not preserve an erroneous conclusion after a verified correction. A customer may produce regulated-intermediary records showing that an address belonged to pooled infrastructure rather than a personal counterparty. That explanation can be material but must itself be assessed.

An unsolicited receipt at a public address does not necessarily demonstrate the owner's intention to interact with the sender. Nevertheless, the legal status of the received assets cannot be ignored where a mandatory measure applies. The analysis should separately consider customer initiative, ability to dispose, links to other activity and the relevant regime. This may change the assessment of the person's conduct without removing a restriction on the particular amount.

For a disputed result, ARGA proposes recording the analytical chain: the underlying transaction, label source, method of inference, confidence, alternative explanation and human decision. Algorithmic trade secrecy does not relieve the organisation of understanding the evidence behind a significant restriction. Not every detail must be disclosed to the customer, but internal controls must be capable of testing the conclusion.

The review should preserve the version of the analytical result used at the time. A later change may legitimately alter the decision, but the provider needs to explain what changed. This is particularly important where different vendors classify the same address differently. Disagreement is not resolved by choosing the more adverse label automatically; it requires examination of the evidence and the limits of each attribution.

14. Suspension, freezing and termination

A temporary technical hold, AML restriction, sanctions freeze and judicial attachment have different bases. The customer's first task is to establish which applies, to the extent disclosure is lawful. The provider must know its precise internal classification even where details cannot be shared. "Required by the regulator" should not be used where no such requirement exists.

Every restriction should identify its subject, start date, accountable person and review trigger. An account-wide block may be necessary but should not automatically be the only option. Where the issue concerns one transfer, the provider should consider whether independent lawful functions can remain available. Targeted treatment cannot override an express prohibition or open an alternative route for disposal of frozen assets.

A suspicious transaction report and a duty to withhold an operation do not always have identical effects or duration across national systems. It would be wrong to claim that reporting creates an indefinite return prohibition everywhere. National law, competent-authority directions and transaction circumstances must be checked. The customer also cannot demand disclosure of the report or its contents where tipping-off rules apply.

Article 75 MiCA requires custody and administration providers to have procedures for returning client crypto-assets or means of access as soon as possible. This does not displace a sanctions freeze, judicial order or other lawful obstacle. Once the obstacle is removed, however, the provider should implement the return. A closed-account label does not explain why assets lawfully returnable remain inaccessible. [1]

Exit requires agreement on the lawful recipient, network, transfer details and checks. A secure confirmation process is important, particularly after contact information changes. The customer should not hand control to another person to circumvent a restriction. The correct objective is a

lawful return to the owner or another entitled person, with completion, fees and any residual balance documented.

The provider should also identify assets in pending orders or intermediate operational accounts. A customer may see a zero withdrawable balance while assets remain within an unsettled process. Closing the relationship requires an accurate reconciliation, subject to legal restrictions. A decision letter and an actual settlement are separate deliverables, and both may matter to resolving the dispute.

15. De-risking and the limits of a duty to serve

Not every refusal is unjustified de-risking. A provider may end a relationship because of a confirmed prohibition, inability to complete checks, unmanageable risk or a lawful commercial reason. The problem arises where an entire category is excluded without individual consideration and the outcome is attributed to an AML rule that does not require that result. EBA materials identify the resulting risks to access and effective risk management. [9]

The provider's strongest argument is limited resources and responsibility for errors. Serving complex cross-border profiles may genuinely exceed a small organisation's capabilities. The answer is not to require acceptance of every risk. It is to distinguish lack of commercial capacity, legal impossibility and factual suspicion accurately. Those grounds have different implications for contractual rights, explanations and treatment of assets already accepted.

The customer's strongest argument is inability to challenge an undefined label or access their property. It is particularly strong where a false match is documented or a current judicial decision has been ignored. A right to correction does not, however, automatically confer every product. The eventual refusal may remain lawful on another independently supported basis.

The right to a basic payment account under Directive 2014/92 has a particular scope and conditions. It does not automatically extend to crypto trading, token custody or every service of a financial group. A basic-account route may matter for essential needs, but it is a separate remedy subject to its own AML and sanctions framework. [24]

ARGA recommends internal consideration of less restrictive measures where no direct prohibition applies and applicable law permits them. Consideration does not require choosing an ineffective alternative. If it fails to mitigate material risk, refusal may be justified. The dossier should record the alternative and why it was rejected, making individual assessment verifiable rather than merely asserted.

Commercial policy should remain transparent within the organisation. If a business chooses not to serve a market because the required expertise is unavailable, that conclusion should not become an unsupported assertion that every customer in that market is suspicious. Accurate classification allows appropriate exit, reporting and data treatment without confusing a business choice with a legal finding about the individual.

16. Data, automated decisions and correction

Within its scope, the GDPR requires lawful, accurate, minimised and appropriately retained personal data. An AML obligation may provide a basis for necessary processing, but does not remove other requirements. Article 10 provides a specific regime for data concerning criminal convictions and offences. Public availability of an allegation should not be treated as permission for unrestricted circulation of a criminal profile. [15]

A customer may exercise access and rectification rights subject to lawful restrictions. A targeted request should identify the error: another person's birth date, incorrect nationality, a missing procedural update or mistaken address attribution. A demand to erase everything may conflict with mandatory retention. Correcting context or restricting processing in the circumstances provided by law may better fit the objective.

Article 22 addresses certain decisions based solely on automated processing that produce legal or similarly significant effects. Not every computer-generated suggestion automatically falls within the prohibition. The model's actual role, consequences and applicable exceptions matter. A nominal staff signature does not necessarily amount to meaningful human involvement where the employee cannot examine or change the result. [15, 21]

In SCHUFA, the Court considered automated production of a score to which a third party attributed a determining role. This is relevant to analysis of dependence on an external risk rating, but is not a direct ruling on a particular blockchain vendor. The factual questions remain who decided and whether a person could genuinely review and reject the machine's result. [21]

Trade secrecy and monitoring security are relevant to disclosure, but do not provide absolute immunity from review. Dun & Bradstreet Austria explains the importance of understandable information about the logic of the relevant automated processing and the role of competent bodies where protected interests conflict. The customer does not necessarily need source code; they need information enabling understanding and challenge of the particular result within the law. [22]

A correction process should reach both the underlying data and dependent decisions. Updating a birth date while leaving the same match and block unchanged does not fully address an identity error. Conversely, accurate data do not require deletion simply because the customer dislikes a lawful risk conclusion. The decision-maker should state whether the dispute concerns a factual error, a disputed inference or the legality of the resulting action.

17. Complaints: issue, recipient and evidence

Article 71 MiCA requires complaint-handling procedures, including free submission. Delegated Regulation 2025/294 specifies organisational requirements. For an existing client, this is a significant route but not a guarantee of success. The legal entity, applicable procedure and requested outcome should be identified first: correct a match, assess documents, explain the lawfully disclosable basis or implement a lawful return. [1, 18]

A strong complaint provides a short chronology and connects each exhibit to an issue. Instead of demanding that “everything be unblocked immediately”, it identifies the restriction date, assets,

materials already supplied and why the previous basis requires review. Urgent living expenses should be evidenced where relevant, but not presented as an automatic exception to every prohibition.

The customer should not demand a suspicious transaction report or information covered by tipping-off restrictions. Those restrictions also do not necessarily remove every contractual or procedural communication duty. Legal staff should identify what may be disclosed, such as review status, documents needed and available complaint routes. The boundary follows applicable law and circumstances rather than a universal template. [3, Article 39]

The next recipient depends on competence. A financial regulator addresses supervision; a data-protection authority addresses personal-data processing; a sanctions authority addresses its regime and authorisations; a court considers the relevant claim and available interim relief. Not every supervisor can award damages or compel immediate performance of a private contract. The requested outcome should match the body's powers.

Before litigation, jurisdiction, governing law, evidence, cost and urgency should be assessed. Public pressure can worsen the position by exposing sensitive information without resolving the legal obstacle. A practical strategy preserves evidence and directs a specific demand to the proper party. Lack of a detailed answer does not alone prove illegality, though it may matter alongside duration, duties and the evidence presented.

The complaint should also distinguish the remedy sought now from a broader dispute. An urgent request for lawful return, for example, need not depend on establishing entitlement to continued trading. Separating those issues can make the immediate decision clearer. It does not waive other claims; it identifies the action that the particular recipient is currently able and legally permitted to take.

18. The French route and payment-service component

In France, the former PSAN status must be distinguished from the current PSCA/CASP regime under MiCA. The AMF has explained the end of transition and provides information concerning the relevant providers. The customer should check the legal entity and permitted services rather than rely only on a historical entry or advertising. For a provider established elsewhere in the EU, the basis for cross-border services must also be established. [25]

A crypto offering may include a payment account, card or transactions involving an electronic money token. These components are not necessarily absorbed entirely by MiCA. PSD2 and other rules may require separate classification. EBA materials on the interaction between PSD2 and MiCA, including its 12 February 2026 opinion concerning the end of the supervisory transition on 2 March 2026, illustrate why the actual model must be checked. CASP authorisation should not be treated as a universal payments licence. [19, 20]

A complaint should distinguish crypto and fiat balances, contractual providers and restriction grounds. A bank may reject an incoming payment after a crypto provider has completed its part. A platform may restrict crypto operations while some payment functions remain available. The

demand belongs with the entity controlling the relevant action and owing the corresponding obligation. A shared brand does not eliminate separate legal persons.

Approaching the AMF or another competent body is not a guaranteed way around mandatory sanctions. A request to deal with frozen funds follows the separate sanctions route. A data dispute may engage the CNIL within its competence. Selecting a French authority does not remove the need to establish where the contractual provider is incorporated and supervised.

A representative's dossier should contain authority to act, identity documents and the material needed for the restriction issue. Where the customer has protection status, personal information should be transmitted narrowly and securely. Multiple parallel letters with inconsistent accounts may create new concerns. A shared chronology allows different bodies to address their own issues without uncontrolled circulation of the entire criminal or immigration file.

The EBA's February 2026 opinion is a supervisory position with specified scenarios and conditions, not a blanket suspension of PSD2. Where the payment component is material, the provider's current status and applicable supervisory treatment should be verified. The customer should not infer either automatic illegality or automatic permission merely from the fact that an EMT-related service is involved.

19. Judicial guidance and limits of analogy

In *Safe Interenvíos*, C-235/14, decided on 10 March 2016, the Court of Justice considered banks' AML checks on a payment institution under earlier legislation. The distinction between permissible control and measures that must reflect the established risk and proportionality is important. The judgment does not create an automatic bank-account right for every crypto provider or customer. Its different legal period and facts must be respected. [23]

ARGA's practical inference is that the chosen measure should be explained against a specific risk. If a provider relies only on industry or category membership, individual circumstances and possible mitigation should be examined. This is an analytical application of a broader principle, not a claim that the Court has already held the crypto-account restriction in question unlawful.

In *SCHUFA*, C-634/21, decided on 7 December 2023, the Court addressed automated credit scoring under Article 22 GDPR. Formal separation between the score producer and the recipient decision-maker does not necessarily remove the relevant safeguards where the score has a determining role. A platform dispute requires evidence of the decision's actual dependence on the model rather than the mere presence of software. [21]

In *Dun & Bradstreet Austria*, C-203/22, decided on 27 February 2025, the Court examined meaningful information about the logic of automated processing. A useful benchmark is an explanation that allows the person to understand the particular processing and challenge the result. Third-party rights and trade secrets require appropriate resolution of the conflict, including through a competent authority or court. The judgment does not create unconditional access to every financial-crime detection rule. [22]

The three cases support distinct procedural elements: proportionate assessment, real human decision-making and meaningful explanation. They do not displace sanctions, current national AML law or the contract. A claim should connect the principle to a fact: which measure is excessive, which data error matters or why human involvement was merely formal. A collection of quotations without that connection offers limited practical assistance.

The strongest counterargument should be addressed expressly. A provider may show that the relevant action was legally mandatory, that the model was only one input or that disclosure would contravene a specific restriction. The customer's case should respond to those propositions with facts rather than assume that every unfavourable outcome is automated or disproportionate. This makes judicial analogies narrower but more credible.

20. Six practical situations

Situation 1. A false sanctions match

A customer's withdrawals are stopped after a name match. Their birth date and nationality differ from available identifiers for the listed person. The customer supplies an identity document and a comparison of discrepancies, requesting review of identity and preservation of the result in the profile. The provider examines the applicable entry rather than first demanding proof of the customer's entire wealth.

If the match is excluded and no other basis exists, the restriction is reviewed and its technical recurrence addressed. An independently unusual transaction can still be considered separately. Correcting a sanctions error does not immunise the customer from future checks, but should not disappear into another undefined request without an identifiable issue.

The decision record should show which identifiers resolved the match and when. This permits later staff to distinguish repetition of the same error from genuinely new information. It also allows the customer to frame a focused challenge if the identical restriction returns without any changed facts.

Situation 2. A refugee and deleted INTERPOL data

A customer supplies a protection decision and official confirmation that specified INTERPOL data have been deleted. A commercial database still shows the old wanted-person record. The provider verifies authenticity and scope, corrects the outdated context and separately assesses the proposed transfer's source. The deletion decision is not described as an acquittal in the domestic proceedings.

If the outdated entry was the only obstacle, retaining the previous refusal requires a new independent basis. If a judicial property measure remains in force, it is analysed separately. A favourable document should change the part of the assessment to which it relates without being given universal legal effect.

The customer need not publish the complete asylum file to establish that a commercial record is outdated. A targeted evidential package can identify the relevant decision, its operative scope and the conflicting database statement. Disclosure should remain sufficient for verification while minimising unnecessary exposure of sensitive protection material.

Situation 3. A Russian passport and extended residence

A Russian national's earlier residence card has expired, while a host-state document confirms extension of a particular status. The platform automatically applies a passport-based restriction. The task is to establish the document's legal effect and whether Article 5b(3) applies, alongside independent personal sanctions screening.

A positive conclusion cannot rest only on “the customer lives in Europe”, and a negative one cannot rest only on the old card's date. Material legal uncertainty should generate a targeted clarification request, not another chain of unrelated financial documents. Residence status requires legal assessment rather than image-recognition output alone.

If the document does not fall within the applicable exemption, the customer's circumstances may still matter to another lawful route, but cannot be used to invent an exception. The decision should explain internally which category is met or missing. That precision determines whether new evidence, a new status or a competent-authority decision could change the result.

Situation 4. A transfer from the customer's own address

A customer sends assets from a self-hosted address to their CASP account. The provider requests information under Regulation 2023/1113 and the relevant evidence of control. The customer offers a safe method that does not disclose a private key and supplies acquisition history. Address control and source of funds are treated as separate questions.

If the platform's standard verification method is incompatible with the wallet architecture, a lawful alternative should be considered. Incompatibility does not prove third-party control, but the required assessment still must be completed. Technical form should not replace legal purpose, and surrender of an access secret should not be treated as ordinary verification.

The provider records what the alternative establishes and what remains unverified. It should not overstate a successful control check as proof of the entire financial history. Conversely, a provenance concern should not be disguised as a failure to control the address after control has been adequately established.

Situation 5. A company with competing directors

Two people seek control of a corporate account. One produces a new registry extract; the other supplies a judicial order restricting the underlying corporate resolution. The provider examines authority, jurisdiction and the order's scope. It does not choose the winner based on who contacted support first or made the stronger accusation.

A targeted temporary measure may be required to prevent unauthorised disposal within the law and contract. Unaffected operations can be assessed separately where safely separable. The uncertainty may concern authority to instruct rather than unlawful origin of the company's assets.

The review should identify what evidence would resolve the authority issue, such as an operative court decision or verified change in representation. It should also preserve assets without deciding the entire shareholder dispute beyond the provider's role. This keeps the restriction connected to the legal question it is intended to address.

Situation 6. An analytics label and termination

A provider decides to terminate because of substantial indirect exposure to a risky service. The customer supplies records showing use of a regulated intermediary's pooled address. The label, connection and actual influence of the score need review. A public accusation of money laundering based on one label is not justified.

Even if a lawful commercial termination decision remains, the provider must separately determine the return process and any obstacle to it. Without such an obstacle, “high risk” should not become indefinite retention. Relationship decisions and property restrictions require independently supported grounds.

If the external vendor corrects the label, the provider should reconsider decisions dependent on it and preserve the change. It may still identify another legitimate reason for exit, but should not continue citing a disproved attribution. Accurate reasons matter both to the customer's challenge and to the provider's own control of model risk.

21. The customer dossier and review record

A dossier should help reach a decision rather than advertise the volume of work performed. ARGA proposes a one-page chronology covering onboarding, the screening event, restriction date, provider requests, customer responses and subsequent changes. It should then state the requested remedy. Each exhibit should identify the fact it supports and the original concern it addresses.

Review question	Useful evidence	Evidential limit
Identity	Document and identifier comparison	Does not establish asset provenance
Residence	Current document and legal regime	Does not remove personal sanctions
Procedural status	Court, CCF or protection decision	Limited to its actual subject matter
Source of funds	Contracts, statements and acquisition history	Must connect to the amount concerned
Address control	Safe verification and technical evidence	Does not establish lawful origin
Corporate authority	Registry, resolutions and judicial measures	Does not replace transaction review

The representative should resolve inconsistencies before submission. Name variants are explained through transliteration and documents; amount differences through fees, exchange rates and quantities. Incompleteness should be acknowledged. Translations should preserve legally important qualifications and the operative part. Extracting a favourable sentence while omitting its conditions can undermine the entire package.

The provider records each material issue as established, disproved, unresolved or legally immaterial. It then identifies what changes in the decision. Where a new judgment is supplied, “our position

remains unchanged” without internal assessment of its significance is not a sound process. The external response may be constrained by law, but an internal rationale should still exist.

The package should be sent securely to the appropriate recipient. The entire immigration or criminal file need not be circulated to every employee in a group. Receipt, the submitted version and dates should be preserved. This may later establish that material evidence was available before a refusal or continued restriction.

A concise cover note can distinguish the primary request from supporting matters. For example, the central issue may be correction of a false identity match, while source-of-funds documents are supplied only because the provider separately requested them. Without that distinction, a strong factual correction may become buried in a broad reassessment that never addresses the original mistake.

22. The decision model and implementation

A decision should identify the action: refusal of a new product, transfer suspension, restriction on disposal, conditional continuation or termination. It should then state the factual and legal basis. “Unacceptable risk” alone does not show what is prohibited or what event would change the outcome. The internal record should be intelligible to a person who did not conduct the original review.

A positive decision may contain proportionate conditions where lawful: a defined service range, further checks on specified receipts or an updated residence document by a relevant date. A condition should be achievable and connected to risk. A low limit cannot replace mandatory identification, and a promise of careful use cannot legitimise a prohibited service.

A negative decision should distinguish a remediable obstacle from a final commercial conclusion. Where a particular document is missing, its function and permissible alternatives should be identified to the extent disclosure allows. A sanctions prohibition requires an internal assessment of competent authority and possible authorisation conditions. A policy decision not to serve the profile does not automatically create a governmental prohibition on returning property.

Implementation is separate from signature. A corrected marker must be reflected in operational restrictions; an approved withdrawal must complete the necessary process; a terminated contract requires reconciliation and records. Residual balances, fees, outstanding orders and assets in intermediate addresses matter. A legally sound letter without actual restoration of permitted action does not resolve the customer's problem.

ARGA proposes measuring time to resolve false matches, reconsideration after new evidence, reasons for repeated restrictions and lawful return time after obstacles disappear. Metrics should not encourage premature closure. Mandatory prohibitions and external directions that the provider cannot lift should be recorded separately. The objective is to identify the provider's own delays and errors, not artificially eliminate complex cases from its statistics.

The model should preserve accountability through handovers. A specialist may approve correction while the operational system remains unchanged because another team owns the release. Assigning

an implementation owner and completion evidence closes that gap. The customer should receive any lawful confirmation needed to understand whether the decision is pending, approved but unimplemented or fully completed.

23. ARGA's position and conclusions

ARGA supports effective sanctions and AML/CFT implementation together with individual assessment and meaningful correction. Financial access does not entitle a person to demand a prohibited transaction. Regulatory caution does not entitle a provider to attribute criminal status through an automated label. A sustainable model distinguishes these boundaries and identifies the basis of each particular action.

The first proposal is separate recording of legal prohibitions, evidential gaps and corporate policy. The second is internal consideration of material new documents. The third is verifiable human review of disputed attribution and significant automated restrictions. The fourth is an independent lawful-return procedure on termination. None requires disclosure of protected suspicious transaction reports.

Supervisors could publish more anonymised examples distinguishing false matches, genuine prohibitions and unmanageable risk. For protection-status cases, guidance on acceptable documents should reflect national legal regimes. For blockchain analytics, expectations concerning attribution quality, label correction and alternative explanations would be useful. Guidance should preserve effective controls without becoming a manual for avoiding them.

The model's main limitation is that it cannot supply a universal answer. Some providers cannot safely serve a complex profile; some customers lack sufficient evidence; some transactions are prohibited irrespective of their economic justification. Those limits do not prevent precise identification of the reason and appropriate route. Uncertainty should have a defined subject and a resolution process rather than remain an indefinite formula for refusal.

The practical result can be tested through five questions: has the person been identified; has the service been classified; is the current basis of restriction established; has material evidence been considered; and has the decision been implemented? For a customer with disputed status, this sequence turns an abstract request to restore access into organised legal work. For a provider, it makes caution demonstrable and distinguishes lawful control from mechanical exclusion.

Sources and references

Source cut-off: 28 September 2026. Square-bracket numbers refer to the list below. Legislation is read with applicable amendments; official guidance does not replace the governing legal text.

- [1] Regulation (EU) 2023/1114 (MiCA), 31 May 2023. Articles 2, 59-61, 66, 70-71, 75 and 143.
<https://eur-lex.europa.eu/eli/reg/2023/1114/oj>
- [2] Regulation (EU) 2023/1113, 31 May 2023. Information accompanying transfers; especially Articles 14-17 and 38. <https://eur-lex.europa.eu/eli/reg/2023/1113/oj>
- [3] Directive (EU) 2015/849, 20 May 2015, as amended. Articles 13-14, 18-23, 33 and 39; applicable national implementation must also be checked. <https://eur-lex.europa.eu/eli/dir/2015/849/oj>
- [4] Regulation (EU) 2024/1624, 31 May 2024. Article 90: main application date 10 July 2027.
<https://eur-lex.europa.eu/eli/reg/2024/1624/oj>
- [5] AMLA. EBA and AMLA complete handover of AML/CFT mandates; AMLA materials on direct supervision from 2028. https://www.amla.europa.eu/eba-and-amla-complete-handover-amlcft-mandates_en
- [6] ESMA. Statement on the end of transitional periods under MiCA. 17 April 2026. https://www.esma.europa.eu/sites/default/files/2026-04/ESMA75-113276571-1679_Statement_on_the_end_of_transitional_periods_under_MiCA.pdf
- [7] EBA. Guidance to crypto-asset service providers on managing ML/TF risks. Final risk-factor guidance, January 2024. <https://eba.europa.eu/publications-and-media/press-releases/eba-issues-guidance-crypto-asset-service-providers>
- [8] EBA. Guidelines on information requirements under Regulation 2023/1113: Travel Rule Guidelines. July 2024; applicable from 30 December 2024. <https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf>
- [9] EBA. Guidelines on policies and controls for effective ML/TF risk management when providing access to financial services. 2023. <https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/anti-money-laundering-and-countering-financing-6>
- [10] EBA. Guidelines 2024/14 and 2024/15 on internal policies, procedures and controls for Union and national restrictive measures. 14 November 2024. <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-terrorism/guidelines-internal-policies-procedures-and-controls-ensure-implementation-union-and-national>
- [11] Council Regulation (EU) No 269/2014, 17 March 2014, as amended. Asset freezes and relevant derogations. <https://eur-lex.europa.eu/eli/reg/2014/269/oj>
- [12] Council Regulation (EU) No 833/2014, 31 July 2014, as amended; especially Article 5b. Read with Regulation (EU) 2025/2033 and subsequent amendments. <https://eur-lex.europa.eu/eli/reg/2014/833/oj>
- [13] Council Regulation (EU) 2026/1848, 23 July 2026, amending Regulation 833/2014; amendment of Article 5b(2a). <https://eur-lex.europa.eu/eli/reg/2026/1848/oj>
- [14] European Commission. FAQs on provision of payment services, Article 5b(2). 13 March 2026. Interpretive guidance read subject to subsequent legislation.
https://finance.ec.europa.eu/publications/provision-payments-services_en
- [15] Regulation (EU) 2016/679 (GDPR), 27 April 2016. Articles 5-6, 10, 15-18, 22-23 and 32.
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [16] INTERPOL. About Red Notices. Official explanation of purpose and legal character.
<https://www.interpol.int/en/How-we-work/Notices/Red-Notices>
- [17] INTERPOL. Refugee Resolution GA-2017-86-RES-09. Official explanation of safeguards and status confirmation. <https://www.interpol.int/Who-we-are/Legal-framework/INTERPOL-Refugee-Resolution>

- [18] Commission Delegated Regulation (EU) 2025/294, 1 October 2024. Requirements, templates and procedures for handling CASP complaints. https://eur-lex.europa.eu/eli/reg_del/2025/294/oj
- [19] Directive (EU) 2015/2366 (PSD2), 25 November 2015. Payment-service scope and authorisation framework. <https://eur-lex.europa.eu/eli/dir/2015/2366/oj>
- [20] EBA. Opinion on the end of the transition period under the No-Action Letter on PSD2 and MiCA. 12 February 2026. <https://www.eba.europa.eu/publications-and-media/press-releases/eba-advises-national-authorities-actions-take-end-transition-period-under-its-no-action-letter>
- [21] CJEU. SCHUFA Holding (Scoring), C-634/21, 7 December 2023. ECLI:EU:C:2023:957. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0634>
- [22] CJEU. Dun & Bradstreet Austria, C-203/22, 27 February 2025. ECLI:EU:C:2025:117. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0203>
- [23] CJEU. Safe Interenvíos, C-235/14, 10 March 2016. ECLI:EU:C:2016:154. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0235>
- [24] Directive 2014/92/EU, 23 July 2014. Access to payment accounts with basic features, especially Articles 15-19. <https://eur-lex.europa.eu/eli/dir/2014/92/oj>
- [25] AMF. End of the transitional period for digital asset service providers on 1 July 2026. Official reminder, 5 February 2026. <https://www.amf-france.org/en/news-publications/news/amf-reminds-digital-asset-service-providers-transitional-period-allowing-them-continue-providing>