Observatoire ARGA

INTERNATIONAL ANALYTICAL REPORT

D-18. False Positives
in Automated Sanctions and AML Screening

European Union and United Kingdom

Author:

Sergey Khrabrykh - President of ARGA, PhD

Organisation: 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

24 September 2026

Contents

Sources current to 24 September 2026. Keywords: sanctions screening; AML; false positives; data accuracy; GDPR; rectification; liability.

1. Principal findings

A false positive in automated screening occurs when a system identifies a person, organisation or transaction as potentially meeting a risk criterion, but subsequent review does not confirm the relevant connection. In sanctions screening, a typical example is a match between a customer's name and that of another person included on an applicable list. The legal problem, however, extends beyond a technical match: a correctly identified person may be assigned an incorrect sanctions status, while a valid preliminary alert may turn into an unjustified prolonged restriction. A system's quality therefore cannot be assessed solely by the number of matches or the speed at which they are closed.

The report's central finding is that a preliminary alert, an established fact and a legal consequence constitute three separate levels. A match requires investigation; identification of a person requires determination of the applicable regime; restricting a service requires its own basis. OFSI guidance expressly distinguishes a name match from a match with a sanctions target. The European EBA Guidelines provide for alert analysis and the use of additional identification data. Neither approach turns the result of a string search into a final legal decision. [1, Section 4.2 of EBA/GL/2024/15; 2, Section 2.2]

Correcting an error also involves several levels. An inaccurate entry in a commercial database, an erroneous link between an entry and a customer, an incorrect interpretation of a particular prohibition and a restriction retained by a bank require different responses. Updating the source database does not establish that recipients have corrected their copies or reviewed their decisions. In the EU, Articles 16, 18 and 19 GDPR connect rectification, temporary restriction of processing and notification of recipients; the right to erasure does not, however, override lawful record-retention obligations. [7]

The potential liability of a screening information provider depends on its actual role, the applicable law and the connection between an infringement and its consequences. A provider operating its own information database may act as an independent controller of personal data; a technical service provider carrying out instructions may act as a processor. The bank retains its own obligations concerning the use of information and sanctions controls. Using an external database does not transfer all responsibility to its developer, and the bank's involvement does not relieve the provider of its own obligations. [1, paragraphs 26-30; 7, Articles 4, 24, 28, 82]

Reducing false alerts cannot be achieved simply by disabling sensitive checks. Such a measure may increase missed matches. A sustainable result requires more accurate identification, current lists, the context of the transaction and substantive review of disputed decisions. Public materials establish these legal and organisational relationships, but provide no basis for identifying a single percentage

of erroneous restrictions across the market or determining the frequency of infringements by each provider.

2. Research question and limits of the evidence

This study asks: under what conditions does an automated sanctions or AML alert become an unlawful information-based or operational restriction, and how are the duties to correct it allocated? The analysis focuses on financial institutions, payment service providers and commercial information systems. Its principal legal framework is the European Union and the United Kingdom. A specific Dutch case is used as a national illustration of equal treatment legislation, rather than as a universal rule for European banks.

The legal and information cut-off is 24 September 2026. The report draws on legislation, financial regulators' guidance, a published monetary penalty decision, judgments on data protection and an opinion of a national equality body. It distinguishes a binding rule, a supervisory expectation, a fact established in particular proceedings and the author's analytical conclusion. This is especially significant for the EBA Guidelines: they cannot be described as a separate regulation establishing every prohibition that a financial institution must apply.

The report is not based on access to banks' internal logs, the source code of commercial products, confidential customer complaints or providers' contracts. It therefore does not establish the comparative quality of particular information brands. The absence of published statistics does not mean that internal controls are absent. Equally, an organisation's alert-review procedure does not establish that a particular customer received a timely and substantive review.

The selection of enforcement and adjudicative materials is purposive: sources were chosen to reveal different mechanisms of error and control. Such a selection is suitable for identifying legally significant distinctions, but not for statistical extrapolation. A decision concerning a missed sanctions target demonstrates the limits of excessive reductions in sensitivity; it does not establish the prevalence of false positives. An opinion on an individual complaint shows that proportionality analysis can apply, but does not, by itself, characterise every product offered by the bank concerned.

The numerical and situational examples below are hypothetical analytical models. They do not represent ARGA statistics, test results for a particular system or information about client cases. Effects on access to services are analysed separately from the basis for recovering damages: damage, infringement and causation require separate establishment. This distinction makes it possible to discuss the seriousness of the problem without replacing research with a predetermined finding of liability.

3. What counts as a false positive

The term false positive is meaningful only in relation to the proposition being tested. If a system searches for similar names, the similarity it finds may be technically correct. If the same result is presented as confirmation of the customer's sanctions status, the conclusion may be false. Assessing quality requires identifying what the tool promises to do: generate candidates for review, establish identity, identify a particular prohibition or assess the likelihood of suspicious behaviour. Different tasks entail different criteria of correctness.

The first type of error concerns identity: an entry about another person is attributed to the customer. The second is temporal: a historical listing is displayed as current. The third is jurisdictional: one state's restriction is presented as another's prohibition. The fourth concerns legal characterisation: PEP status, participation in litigation or a media mention is converted into an assertion of sanctions. The fifth is operational: a preliminary alert has already been disproved, but the restriction remains. This typology is analytical, rather than an official classification adopted by a regulator.

An inconclusive result should not automatically be counted as a false positive. If additional information is insufficient for a conclusion, the appropriate category is an unresolved match. EBA/GL/2024/15 separately addresses situations in which further due diligence does not establish the nature of a match unambiguously. The Guidelines envisage internal procedures and refraining from providing financial services to the relevant party to a transfer until an informed decision has been reached. This is a significant limit on the proposition that every unconfirmed alert must immediately be cleared. [1, paragraph 35]

For AML monitoring, the concept of error is more complex still. An unusual transaction may legitimately trigger a review without leading to a finding of criminal conduct. The absence of a criminal investigation, charge or conviction does not establish that the initial alert was unfounded. Duties to analyse transactions and report suspicions rest on different grounds from criminal liability. That distinction does not, however, permit a customer profile to retain an assertion of proven criminality where there was only a preliminary indicator. [12, paragraph 11; 15, Articles 13 and 33]

Assessment must therefore take account of the point in time and the level of decision. An alert may have been justified when incomplete data arrived, but lose its basis after a passport is obtained or a list corrected. The reverse is also possible: an initially discounted match may become relevant following a new sanctions measure. A decision's correctness is a relationship between available information, the applicable rule and a particular action, rather than a permanent characteristic of a surname or customer profile.

4. The legal architecture of sanctions and AML controls

Sanctions controls begin with determining the applicable prohibition. A list of names is a tool for implementing it, but does not replace the legislation. Regimes differ in territorial scope, the persons bound, the assets concerned, prohibited services, exceptions and authorisations. A customer's absence from a named list does not exclude restrictions connected with ownership, control, the recipient of funds or the nature of a transaction. Accordingly, disproving a name match resolves a specific identification issue, rather than every possible sanctions issue. [2, Sections 1-3]

In the EU, EBA/GL/2024/14 addresses the general framework for managing the relevant risks, while EBA/GL/2024/15 contains more specific provisions for payment service providers and crypto-asset service providers. Both documents are dated 14 November 2024 and apply from 30 December 2025. Their addressees and scope differ; the detailed requirements of the second document cannot be attributed without explanation to every economic operator. They establish a supervisory framework for organising the implementation of restrictive measures, while the content of a prohibition is determined by the applicable law. [1]

UK OFSI guidance distinguishes a name match from a target match and envisages comparison of additional characteristics. If an organisation is satisfied that it is dealing with a different person, no further action is required in respect of that match. Where uncertainty remains, OFSI may be contacted for assistance. This does not mean that the authority issues mandatory advance clearance for every automated alert or makes all customer-service decisions on the bank's behalf. [2, Section 2.2]

AML due diligence follows a different logic. In the United Kingdom, regulation 28 of the MLR 2017 provides for customer and beneficial-owner identification, understanding the business relationship, ongoing scrutiny of transactions and updating information. The extent of due diligence reflects risk. In the EU, similar basic obligations are laid down in Directive 2015/849 and implemented through national law. These duties are not confined to searching sanctions lists. A match with a commercial profile may be one source of information, but does not replace analysis of the relationship and the transaction. [12; 15, Article 13]

The distinction between legal regimes affects the evidence. For a sanctions restriction, the central issues are identity, an operative prohibition and the transaction's connection to it. For AML due diligence, they are customer information, economic purpose, the pattern of funds movement and the grounds for suspicion. Termination of a contract also raises the rules governing the product and the applicable contract law. Labelling all these decisions simply as compliance obscures different powers and makes it harder to identify which particular basis requires correction.

5. Name matches, transliteration and identification

A name is an important but non-unique identifier. A common surname, an omitted patronymic, a change in the order of name components or reduction to initials expands the range of possible matches. Transliteration adds another layer of ambiguity: different writing systems may render the same sound using different letters. At the same time, two similar spellings may refer either to one person or to different people. Technical string similarity therefore does not, by itself, measure the legally relevant likelihood of identity.

Fuzzy matching is used precisely to detect spelling variations. EBA/GL/2024/15 provides for calibrating such techniques and testing sensitivity. A system that responds only to an exact literal match may miss a known name variant; an excessively broad system generates a stream of weak candidates. Between these extremes lies not a single correct similarity percentage, but a justified configuration for particular data and applicable restrictions. [1, paragraphs 24-25]

Date and place of birth, documents, nationality and known addresses can reduce uncertainty, but carry different evidential weight. A matching document number where authenticity has been checked differs from a match in country of residence. A changed address will generally not rule out identity. Incompatible biographical characteristics may strongly rebut a match, although the significance of a discrepancy also depends on the completeness of the official entry. An empty field cannot be treated as evidence of a match, nor can every populated field be treated as unquestionably reliable.

For organisations, a name is supplemented by a registration number, jurisdiction of incorporation, previous names, legal succession and ownership structure. An identical trading name does not establish that legal entities are the same. Conversely, a change of name does not necessarily create a new entity. A separate error arises when information about a director, shareholder or subsidiary is attributed to the company without identifying the nature of the relationship. Such an entry may be textually based on a real source, yet misdescribe the subject being screened.

Analytically, it is useful to distinguish data that generate a candidate for review from data that resolve a match. The first group permits greater sensitivity. The second must make it possible to explain why this particular subject was identified and why alternatives were rejected. If a system retains only a final score without the source entry and identifiers used, reassessment becomes dependent on unavailable context. In a dispute, this makes it harder both to protect the customer and to substantiate the organisation's good-faith decision.

6. Outdated lists and errors in legal status

Sanctions information changes over time. Listing, correction of an identifier, amendment of a measure's scope and delisting are different events. A commercial database may legitimately retain a historical listing, but must distinguish it from current status where personal-data accuracy requirements apply. If a user sees only a red indicator whose meaning is not explained, even an accurate history can prompt a wrong decision about the present. [7, Article 5(1)(d)]

In the United Kingdom, from 28 January 2026 the UK Sanctions List became the sole source for all UK sanctions designations; the former OFSI Consolidated List ceased to be updated. For a study as at September 2026, this is not a minor technical detail: functioning access to an old list does not establish that current information is being received. Moving a system to the new source requires preservation of record identity and correct handling of changes in status. The migration itself does not, however, establish that a particular organisation made an error. [11]

The European Guidelines cover list management for new measures, amendments and measures that are lifted. For PSPs and CASPs, updating the internal dataset is linked to the entry into force of the relevant change. Data-feed quality therefore cannot be assessed solely by how quickly new subjects are added: delayed processing of a revocation or an amended identifier also changes screening outcomes. Completeness of coverage and correct representation of the entry's status over time are equally significant. [1, paragraph 9]

Jurisdictional errors are possible even with an up-to-date database. Removal from an EU list does not mean removal from the UK list, while US restrictions do not automatically oblige every European operator to freeze assets under EU law. A particular transaction may have several legal connections, so the analysis is not reduced to choosing one list. Each connection must nevertheless be identified: an applicable obligation, a restriction imposed by an intermediary and the organisation's own commercial decision have different legal character.

Historical status requires careful wording. The statements listed, previously listed, removed from a particular regime and all sanctions lifted are not interchangeable. The last formulation is especially risky where only one measure has been checked. Rectification must preserve the necessary distinctions between a past event and the current legal position. This avoids two opposite errors: indefinitely continuing a revoked measure and prematurely lifting a restriction that remains applicable on another basis.

7. Errors of context in payment messages

Transaction screening works with more than the names of the sender and recipient. Additional fields may contain the payment purpose or information about an intermediary, goods, a vessel or an end user. Such data help detect restrictions not apparent from the customer profile. Free text simultaneously creates ambiguity: a name in the payment reference may identify a party to a transaction, the author of a work, a relative, a project or another circumstance unrelated to making funds available to a sanctioned person.

A detected string must therefore be related to its role in the transaction. The question is not only whose name it is, but why it appears in the message. A transfer between the customer's own accounts provides relevant context, although it does not, by itself, exclude sanctions evasion or subsequent provision of funds to another person. Analysis that ignores purpose and the direction of funds movement loses the distinction between mentioning a subject and that subject's participation in the economic outcome.

EBA/GL/2024/15 envisages screening information about transfer participants and, subject to the specified conditions, free-text fields. Intermediaries and available crypto-wallet addresses are also considered. The document does not reduce screening to mechanical comparison of a single string. Where document recognition is automated, the accuracy of information extraction also matters: a misread character may create or conceal a match before the matching algorithm is even applied. [1, paragraphs 19-23 and 43]

Technical transmission may change a message: a field is shortened, a compound name divided, characters normalised or information distributed between structured and free-text components. This is analytically distinct from the quality of the underlying reference database. A provider may supply a correct entry while the bank compares it against an incorrectly transformed message. The reverse is also possible. Establishing the cause requires a record of transformations, rather than only a screenshot of the final result.

A separate difficulty arises where a bank requests information about a third party mentioned in a payment. The customer may not possess that person's passport or full biographical details. Inability to supply unavailable information is not equivalent to an intention to conceal a sanctions connection, but does not remove the organisation's duty to resolve material uncertainty. Legal assessment depends on the request's relevance, available alternatives and the grounds that remain after the transaction's economic purpose has been explained.

8. AML alerts, adverse media and criminal information

Automated AML controls include both matching names against external datasets and detecting unusual transactions. These processes cannot be assessed using a single test. An error in attributing a newspaper report to a particular person differs from a real transaction having an unusual size or structure. In the latter case, the issue concerns the justification for the risk assessment and the depth of review, rather than necessarily the accuracy of personal data. A risk assessment may be disputed even where all factual input fields are correct.

A commercial profile often combines heterogeneous information: public office, sanctions status, litigation, investigative reporting and connections with other people. Without identifying the source, date and procedural position, such aggregation creates a false impression of a single verified fact. A party to civil proceedings, a witness, a suspect and a convicted person occupy different legal positions. The presumption of innocence does not prohibit financial checks, but does not permit an allegation to be described as established guilt.

In the EU, data relating to criminal convictions and offences fall within the special regime of Article 10 GDPR. In addition to a basis under Article 6, the conditions prescribed by Article 10 must be met. A publication's public availability does not remove this question. At the same time, not every sanctions entry automatically constitutes information about a criminal offence: its legal characterisation depends on its content, rather than the category in which a commercial database places it. [7, Articles 6 and 10]

The absence of a suspicious transaction report does not establish that every circumstance is unproblematic, and the existence of a report does not establish a crime. A financial institution acts under preventive obligations that differ from a court's powers. It is analytically wrong to treat the proportion of reports not followed by convictions as a ready-made false-positive indicator. Between reporting and a judicial outcome lie an investigation, other evidence, the authorities' powers and a time lag about which a bank or researcher may have no knowledge. [12; 15, Article 33]

Rectification primarily concerns verifiable factual errors: someone else's biography, an incorrect date, a revoked decision, the wrong procedural status or a non-existent connection. Disagreement with an assessment requires different reasoning: what information was considered, what was omitted and why the conclusion does not follow from it or exceeds the purpose of the processing. This distinction preserves the possibility of challenge without turning the right to data accuracy into a right to demand an exclusively favourable financial profile.

9. Why the proportion of closed alerts does not measure system quality

When assessing screening, it is essential to distinguish the proportion of false results among all alerts from the proportion of wrongly flagged subjects among all subjects to which the criterion does not apply. In the first case, the denominator consists of alerts; in the second, of genuinely negative cases. These measures answer different questions. A high proportion of closed alerts may reflect the rarity of real matches, a broad search strategy, poor data quality or cursory closure. Without further information, it is impossible to choose between these explanations.

A hypothetical calculation illustrates the significance of a rare event. Suppose that, among 100,000 records screened, 10 are genuinely relevant, the system detects 9 of them and wrongly flags 100 others. It generates 109 alerts, of which 100 are false: approximately 91.7%. Yet the false-positive rate among the 99,990 genuinely negative records is approximately 0.1%. Sensitivity to positive cases is 90%, while confirmed matches account for approximately 8.3% of alerts. All these figures are hypothetical and do not describe the actual market.

This example does not imply that a high proportion of false alerts is always acceptable. If each alert automatically stops a payment for several days, a small percentage of a large flow creates a substantial number of restrictions. But simply reducing the number of alerts does not demonstrate improvement either. A system that stops checking part of a list will show a lower workload while becoming worse at detecting prohibited transactions. The result depends on both errors: unjustified restriction and failure to detect a relevant match.

The status of a closed alert also requires scrutiny. Closure may mean a documented finding that two people are different, removal of a duplicate, a change in the applicable regime, technical consolidation of cases or a staff decision based on incomplete data. Combining these reasons into one category makes the statistics less informative. It is particularly risky to train subsequent models on such a dataset as unquestionable ground truth: organisational closure practices begin to reproduce themselves as the standard of correctness.

A substantive assessment therefore considers the screened population, list completeness, reasons for alerts, resolution time, repeated restrictions after correction and sample testing of missed cases. These are analytical dimensions of quality, rather than universally prescribed statutory standards. FCA supervisory observations confirm the significance of calibration and resources, but do not establish a single acceptable false-positive percentage for every organisation. [3; 4]

10. Calibration, testing and the limits of automation

Setting a similarity threshold distributes errors, but does not remove the need for legal analysis. The same threshold may work differently for short and long names, different alphabets and incomplete records. A system receiving only a name and country cannot achieve the degree of differentiation provided by a verified date of birth and identity document. A claim of high model accuracy without a description of the input data therefore has limited value: it may concern conditions absent from the actual payment flow.

Testing against known matches establishes the ability to detect particular variants. It does not demonstrate quality across all languages and circumstances. False candidates, incomplete records and actual message transformations during transmission require separate attention. If a test dataset repeats the data used to calibrate the system, the assessment may reflect memorisation of that dataset rather than robustness in new cases. This is a methodological risk, rather than an established fact about any commercial provider.

In the EBA Guidelines for PSPs and CASPs, calibration is linked to the restrictive measures exposure assessment and regular testing. The rationale for the configuration must be documented. The supervisory purpose is to make it possible to explain the parameters and their limitations, rather than to produce a single certificate of accuracy. Changes in the customer base, the composition of a list or the nature of transactions may require the existing configuration to be reassessed. [1, paragraphs 24-25]

Automating the handling of recurring false matches can reduce unnecessary workload, but creates risks of its own. An internal exception that applied to one customer and one entry must not become a permanent exemption from screening for everyone with the same name. EBA permits an internal list to prevent repeated false alerts, with documented reasons and review following changes in a restrictive measure or customer information. This is a controlled exception to a repeated alert, rather than the removal of applicable sanctions. [1, paragraph 13]

The powers of the people working with the system also matter. An analyst who sees only a score and must follow a preset instruction without authority to assess documents provides a different level of control from a staff member with access to the source information and the ability to change a decision. A person's formal involvement does not guarantee substantive review. Equally, assigning a decision to a person does not, by itself, guarantee correctness: that person may confuse jurisdictions, misread an update or close an alert without sufficient grounds.

11. Instant credit transfers in the EU: a specific screening model

The European legislature has established a specific framework for instant credit transfers in euro. Regulation 2024/886 inserted Article 5d into Regulation 260/2012. Providers offering such transfers must check their users against targeted financial restrictive measures when new measures or amendments enter into force and at least once every calendar day. The compliance deadline for that Article was 9 January 2025. At the date of this study, it is an operative requirement, rather than a planned reform. [10]

During execution of the relevant instant credit transfer, the payer's and payee's providers must not additionally perform the Article 5d screening of those participants against the same targeted measures beyond screening the user base. This model moves a particular control from each transaction to the user's regularly updated status. Legally, it represents not an absence of sanctions controls, but a different method of organising them expressly provided for by legislation. [10, Article 1(2), new Article 5d(1)-(2)]

The exceptions define the rule's limits. The Article preserves action to comply with other restrictive measures, measures not adopted under Article 215 TFEU and requirements to prevent money laundering and terrorist financing. It cannot therefore be paraphrased as a prohibition on any checks of an instant payment or as an exemption of the recipient from AML controls. Nor can it automatically be extended to ordinary international transfers or all crypto-asset transactions.

Its significance for false matches is that the legislature distinguishes screening a person from repeatedly screening every transaction. A technically possible check is not always legally prescribed at the particular stage selected. Repeated comparison of identical data may reproduce uncertainty that has already been resolved without adding new information. The justification for a particular restriction nevertheless depends on which of the remaining legal bases it falls under and what data were actually checked.

This framework demonstrates the limits of universal assertions about the strictest possible screening. The intensity of a control cannot be assessed separately from its legal structure. User-base screening, current status, other sanctions prohibitions and AML analysis must remain distinguishable. In a dispute, establishing that a transaction was instant is insufficient: the type of transfer, participating providers, measure being checked and actual cause of delay must be identified.

12. Consequences of error: from delay to lasting exclusion

An alert's immediate consequence may be confined to a short delay, but does not always remain so. Repeated restrictions affect payments for housing, wages, medical care, taxes and contractual performance. For a business, a delayed payment may disrupt a supply chain or payments to employees. These categories describe possible mechanisms of harm; the report does not assert their frequency or attribute them to a particular provider without evidence.

The accumulation of consequences is particularly significant. An initial match may remain in an internal profile as an elevated risk and later affect a limit, the need for additional approvals or a subsequent refusal. In that situation, releasing one transfer does not necessarily restore the customer's position. Analytically, lifting a current operational hold must be distinguished from removing the informational basis capable of triggering another. This distinction explains why a favourable outcome on one occasion does not always resolve the dispute.

Another problem is a mismatch between the scope of a restriction and the extent of the uncertainty. Uncertainty about one participant in a particular payment may lead to the suspension of all of the customer's transactions. Sometimes there is an independent legal basis for this; sometimes the wider restriction results from system configuration or an internal process. It cannot be considered justified or unlawful solely because of the original alert. Each restricted service requires its own connection to the uncertainty identified.

A temporary payment block and an asset freeze are also not equivalent. A sanctions freeze follows from an applicable prohibition and has defined legal consequences. A technical hold pending review is a different situation, even if the customer is practically unable to use the funds in either case. Clarifying the legal characterisation affects the competent authority, any possible authorisation and the available remedy. A licence for an act prohibited by sanctions is not designed to correct a simple error concerning the identity of a non-sanctioned customer. [2, Section 3]

Finally, the organisation itself bears consequences. A large flow of unresolved alerts consumes resources, complicates prioritisation and may delay handling of genuinely relevant cases. FCA materials from 2023 noted this relationship. Reducing unjustified restrictions and maintaining robust sanctions controls can therefore be compatible objectives: accurate identification frees capacity for cases where risk remains. This is not a reason to lower requirements, but a reason to assess the quality of the process as a whole. [3]

13. The ING opinion: proportionality and indirect discrimination

In Opinion No 2024-63 of 25 July 2024, the Dutch College voor de Rechten van de Mens considered a complaint about a blocked transfer and additional checks by ING Bank N.V. The trigger was a partial match between a name in the payment reference and sanctions entries. The body did not establish direct selection on grounds of race, but found indirect differential treatment and insufficient objective justification for the particular practice. This was an opinion of a national equality body, rather than a court judgment or a penalty decision. [6, paragraphs 6.8-6.24]

The College accepted the legitimacy of the sanctions objective and the suitability of screening to achieve it. That was nevertheless insufficient to establish proportionality. The assessment took account of the effects of erroneous restrictions, the lack of a timely explanation and the prolonged block. The source thus demonstrates the need to assess not only the search mechanism but also the treatment of the person after an alert appears. It does not establish a general prohibition on automated name screening. [6, paragraphs 6.14-6.23]

The case's analytical significance lies in the distinction between intention and effect. A neutral description of an algorithm does not rule out uneven effects on different groups. At the same time, uneven effects alone do not establish unlawfulness: legal assessment includes the applicable criterion, comparable circumstances, the objective and justification of the means. This differs from investigating a staff member's subjective intention to discriminate against a customer and requires different evidence.

It is also important not to extend the body's conclusions to unknown circumstances at other banks. The case does not provide a quantitative assessment of all sanctions errors in the Netherlands or the EU. Nor does it establish that every request about a third party mentioned in a payment reference is excessive. Its significance is narrower and more verifiable: reliance on mandatory sanctions controls can be assessed against the actual arrangements for resolving erroneous alerts and their consequences for the customer affected.

In this report's context, this means that accuracy and equal treatment intersect but are not identical. Correcting a particular name may resolve an individual error while leaving a systemic practice of prolonged, repeated blocks intact. Conversely, clearer communication does not correct the mistaken identification of two people as one. A complete analysis addresses data quality, the decision-making process and the distribution of adverse consequences without combining those grounds into a single allegation.

14. Bank of Scotland: the case against excessive weakening of controls

An official OFSI notice published on 26 January 2026 describes a £160,000 penalty imposed on Bank of Scotland PLC on 10 November 2025. In February 2023, the bank processed 24 payments totalling £77,383.39 through a designated person's account. Automated screening failed to detect a variant spelling of the name. Later, during manual review, the person's removal from the EU list was wrongly interpreted as removal from the UK list as well. [5, paragraphs 1-7 and 15-20]

This is an example of a missed match and subsequent human error, rather than a false positive. It is included to examine the opposing risk. A reduction in the number of alerts is not, by itself, evidence of effective controls. A system may generate fewer alerts precisely because it fails to recognise legally significant variants. Particularly important here is the combination of a technical problem and an incorrect legal interpretation after further information had been obtained.

OFSI does not establish a universal obligation to purchase a commercial sanctions list in the notice. It considers sufficient enhancement of screening with relevant available information in light of risk. This distinction prevents another unsupported conclusion: a contract with a well-known provider does not, by itself, guarantee adequate controls, while the absence of such a contract does not establish an infringement. The available information, the system's design and its use are what matter. [5, paragraphs 18 and 28]

The case also demonstrates the limits of transferring decisions between legal regimes. Even a correct report of removal from one list requires its scope to be established. If a bank's instruction turns that record into general permission for all transactions, the error occurs at the legal-characterisation stage. The source provider may have communicated the fact correctly while the subsequent decision was wrong. Responsibility therefore cannot be allocated without reconstructing who created the record, who interpreted it and who authorised the action.

Human involvement did not eliminate the risk. This does not mean that manual review is useless; it means that its quality depends on competence, access to sources, escalation procedures and a correct understanding of authority. An analytical model concerned exclusively with releasing wrongly affected customers would be incomplete without this counterargument. Accuracy requires a justified distinction between a false alert and an actual restriction, even where both involve similar name spellings.

15. The commercial database and the bank: allocation of roles

A screening information provider may perform several functions: collecting source information, combining entries, assigning categories, calculating matches, supplying an interface or conducting checks on a client's instructions. Its legal role is determined by its actual involvement in choosing the purposes and means of processing, rather than solely by the contract's label. In the EU, Article 4 GDPR defines controllers and processors. One company may occupy different roles for different processing operations. [7]

Where a provider independently determines a commercial database's composition, sources and profile-inclusion rules, its independent obligations as a controller must be considered. Where it merely carries out bank-defined operations on a supplied dataset, it may act as a processor. Joint determination of purposes and means may require an assessment of joint controllership. Merely exchanging information or purchasing database access does not, however, automatically establish joint controllership. Each stage requires separate characterisation. [7, Articles 4, 26 and 28]

A bank using information to serve a customer will usually determine its own purpose for the check and make its own decision about a product or transaction. A provider's notification of a possible match and a bank's restriction are therefore not the same action. An error may arise in the source profile, matching configuration or interpretation of the result. Each scenario involves different evidence, available corrections and potential grounds of liability.

The European Guidelines on restrictive measures preserve the ultimate responsibility of PSPs and CASPs for compliance with the relevant obligations when functions are outsourced. They also provide for written allocation of rights and obligations and oversight of the external service's quality. These provisions do not automatically resolve a civil dispute between a provider and a bank's customer, but prevent outsourcing from being presented as a complete release of the financial institution from control obligations. [1, paragraphs 26-30]

For the affected person, this allocation means that claims may be directed at several parties, each with a different subject matter. A challenge to the provider concerns the entry and its dissemination; a challenge to the bank concerns its own data, the link to the profile and the consequences of its decision. One addressee may lack authority to change another's actions. This is not a reason to abandon rectification, but an important limit on the expected result: a deleted profile is not an instruction to every bank to resume services, and a released payment does not necessarily correct the external database.

16. Accuracy, minimisation and a lawful basis for processing

In the EU, the accuracy principle requires personal data to be accurate and, where necessary, kept up to date, with reasonable steps to rectify or erase inaccuracies without delay in light of the purposes of processing. For screening, purpose has practical significance. A historical entry about a previous listing may accurately describe the past yet be misleading when used to indicate a current prohibition. The assessment therefore concerns not only a passage's literal truth but also how it is presented and used. [7, Article 5(1)(d)]

Completeness is also relative to purpose. A profile that reports an allegation but omits a known acquittal may distort a person's position. The right to accuracy does not, however, entail a duty to include every favourable characteristic or rewrite an entire historical archive. The question is whether the omitted circumstance is material to the meaning of the entry being disseminated. This is why the event date, procedural status and update date matter when assessing a profile's lawfulness.

Data minimisation is not equivalent to using only a name. In some situations, an additional identifier makes it possible to exclude a false match and reduce interference. Yet collecting a complete family and professional dossier to resolve a straightforward mismatch may exceed what is necessary. The balance is determined by the specific purpose and relevance of the information, rather than an abstract rule that more information means greater safety. Additional data themselves create duties of accuracy, security and limited retention. [7, Article 5]

The bank's legal basis does not automatically extend to every provider. A financial institution's obligation to comply with AML legislation does not answer why an independent commercial database may collect particular information, retain it for a particular period and disclose it to a particular range of clients. Each processing activity requires an applicable basis, with additional conditions for special categories and criminal information. Public availability of the source and paid access to the product do not replace this analysis. [7, Articles 6, 9-10]

Personal data concern an identified or identifiable natural person. Information solely about a legal entity does not acquire the full set of GDPR rights merely because it is used in screening. A corporate profile may, however, also contain personal data about a director, beneficial owner or sole trader. It is then necessary to distinguish whose information is being processed and who is asserting the relevant right. An error in that characterisation may result in a substantively valid request being advanced on an inappropriate legal basis.

17. Rectification, erasure and restriction of processing

Article 16 GDPR gives the data subject the right to have inaccurate data rectified without undue delay and, in light of the purposes of processing, to have incomplete data completed. For a false match, the object of rectification may be not the sanctions entry itself, but its link to the person. If an official list correctly describes someone else, the entry need not be removed from the entire database. The erroneous attribution and its consequences must be addressed in the systems where that link was established. [7]

The right to erasure has different conditions and exceptions. It may arise, for example, where processing is no longer necessary or is unlawful, but does not override a legal retention obligation. A bank may need to retain the history of its transaction review and evidence explaining why an alert was discounted. Proper retention of a historical record is not equivalent to retaining a current adverse status. Confusing these functions creates a false choice between destroying all documentation and continuing a restriction indefinitely. [7, Article 17; 15, Article 40]

Where accuracy is contested, Article 18 GDPR provides for restriction of processing for a period enabling the controller to verify the data. This is a distinct mechanism: an entry may remain stored, but its use is restricted to the prescribed extent and subject to the applicable exceptions. Restriction of personal-data processing is not equivalent to a bank freezing funds. Nor does it automatically authorise a disputed transaction: a sanctions measure or another mandatory restriction may have an independent basis. [7, Article 18]

The general GDPR response period is governed by Article 12: without undue delay and, generally, within one month, with an extension possible under specified conditions and subject to notification. That period cannot be described as permission to continue an adverse classification already known to be wrong for an entire month. The procedural response period must be distinguished from the duty to correct an identified inaccuracy promptly and from banking-complaint deadlines under a different legal framework. [7, Articles 12 and 16]

A request's content depends on the nature of the error. Identifiers are relevant to mistaken identity; a subsequent official act to an outdated status; the precise scope of delisting to confused jurisdictions; and a procedural document to an incorrect role in proceedings. A statement that the person is not sanctioned, without identifying the disputed entry, may be insufficient, but demanding proof of the absence of every possible risk does not correspond to the specific object of rectification either. Analytically, a robust procedure connects the disputed assertion to a verifiable fact and a defined result.

18. Propagating corrections and residual records

Correction at one point in the information chain does not guarantee changes to every copy. Data may be held by the provider, bank or intermediary, in a local archive or export, or in a separate matching service. Technically, updating the source and recalculating the customer's result are different operations. If a system stores the previous decision independently of the profile, a new database version may have no effect on the current restriction. This is a possible mechanism through which an error persists and must be checked against the specific logs.

Article 19 GDPR requires communication of rectification, erasure or restriction of processing to each recipient to whom the data were disclosed, unless this proves impossible or involves disproportionate effort. The data subject is informed about those recipients on request. This rule matters for commercial databases because correction is intended to do more than update their own interface. It does not, however, create an unlimited duty to locate every unknown copy worldwide or override statutory restrictions on rights. [7]

A recipient remains a participant in a separate processing activity. Following notification, its own purpose and basis matter, as do the decisions that relied on the incorrect entry. A bank may retain archival evidence of an earlier check, but must distinguish it from its current assessment of the customer. If it continues a restriction for another reason, the issue is whether that reason is independent, rather than whether it can again rely on a fact that has already been disproved.

Assessing whether an error has been remedied requires a sequence of events: when the original source changed, when the provider received the change, when it updated the profile, when it notified recipients and when the bank reviewed its own decision. A delay between stages may explain a repeated block without assuming deliberate misconduct. Once the causes have been established, however, that same sequence identifies the stage at which the problem arose and whose duties may not have been performed.

A provider cannot be required to promise that no financial institution will ever generate another alert. A new match may result from different data, a new measure or an independent check. The object of scrutiny is narrower: whether the correction was properly communicated, the erroneous link removed and the old conclusion prevented from being reproduced as if it were new. This distinction makes the outcome verifiable without replacing the right to accurate data with a guarantee of unrestricted service at every institution.

19. Explaining automated decisions and human review

In the EU, Article 22 GDPR concerns decisions based solely on automated processing that produce legal effects or similarly significantly affect a person. Not every name search or similarity calculation meets these conditions in itself. But where the result determines a significant refusal or restriction without substantive assessment, the question of the Article's applicability arises. The actual process must be examined, rather than merely the formal presence of an employee in an organisational chart. [7]

The content of the right to information was explained by the Court of Justice in Dun & Bradstreet Austria, C-203/22, on 27 February 2025. The case concerned credit profiling, rather than sanctions screening. The Court interpreted Article 15(1)(h) in the context of automated decisions: the information must make it possible to understand the procedure and principles actually applied to obtain the result. Merely presenting a complex formula does not necessarily provide that understanding. [8, paragraphs 38-61]

For screening, this offers a legal reference point where the conditions of the relevant provisions are met. An explanation may concern the personal data used, their significance for the result and the role of an external profile. The judgment does not give every customer an unconditional right to obtain source code, all security parameters or an entire commercial database. The Court also addresses balancing trade secrets and third-party rights through the competent authority or court, rather than treating them as grounds for a blanket refusal of access. [8]

An intelligible description of an algorithm does not, however, replace review of a factual error. A person may learn that the system compares names and dates of birth while disputing whether the profile used belongs to them. Alternatively, the input data may be correct and the dispute may concern a disproportionate outcome. In the first case, rectification and reassessment are central; in the second, the decision's legal basis and applicable safeguards. Explainability is useful insofar as it makes the specific subject of disagreement identifiable and testable.

The conclusions in this section concerning Article 22 GDPR and the cited Court of Justice judgment relate to EU law. They cannot automatically be extended to the UK regime for automated decisions. The UK part of the report is confined to separately verified rules on financial controls, accuracy, rectification and exemptions from data rights. This separation avoids the mistaken assumption that shared GDPR terminology means complete identity between the two jurisdictions' operative rules.

20. Confidentiality, AML and limits on disclosure

A financial institution is not always entitled to disclose every aspect of a review to its customer. Prohibitions on disclosing information about reports to financial intelligence units and investigations protect distinct public interests. In the EU, the relevant framework includes Article 39 of Directive 2015/849 and national legislation. In the United Kingdom, regulation 28 of the MLR expressly addresses situations in which continuing ordinary customer due diligence may result in prohibited disclosure. [12, paragraphs 14-15; 15]

Confidentiality of particular material does not, however, mean that all data in a compliance profile are automatically excluded from accuracy requirements. Internally, the organisation must still distinguish the customer from a namesake, past from current status, and a report of suspicion from an established fact. The ability to communicate a result to the subject and the duty to process information correctly are related but separate questions. A justified restriction on access does not make an inaccurate entry accurate.

In the EU, restrictions on rights under Article 23 GDPR require a legislative basis and compliance with the prescribed conditions. In the United Kingdom, Schedule 2 to the Data Protection Act 2018 contains exemptions concerning, among other matters, the prevention and detection of crime. Their application depends on the specific provisions and the extent to which giving effect to a right would prejudice the protected purpose. Referring to crime or AML as the general subject of processing is insufficient to conclude that all of the data subject's rights are displaced. [7; 14]

The explanation given externally may be more limited than the internal reasoning. This does not mean that the decision lacks a verifiable basis. In a dispute, a competent authority or court may assess documents within its powers and procedural rules. The report does not assume a single confidential-access mechanism for every type of complaint; the particular possibilities depend on the jurisdiction and procedure. The absence of a full explanation to the customer does not, by itself, establish either the lawfulness or the unlawfulness of a restriction.

For analytical purposes, the scope of the actual refusal matters. Not disclosing the existence of a suspicious report and refusing to check an incorrect date of birth are different actions. Distinguishing them can often identify which information is genuinely protected and which concerns ordinary identification. At the same time, that distinction does not entitle a customer to circumvent a prohibition through a series of indirect requests. Assessment must preserve both objectives: effective investigation and the avoidance of unjustified use of incorrect personal data.

21. Potential liability of information providers

A provider's liability cannot be inferred solely from its product's involvement in a check. The relevant act or omission must be identified: erroneous combination of profiles, failure to update a status, transmission of an inaccurate category, failure to act on a substantiated rectification request or another specific defect. The applicable duties and the connection to the adverse consequence must then be established. A technical provider, an independent database controller and a consultant preparing an assessment may be liable on different grounds.

Article 82 GDPR distinguishes the liability of controllers and processors. A controller involved in processing is liable for damage caused by processing that infringes the Regulation; a processor is subject to specific conditions connected with its obligations or acting beyond lawful instructions. Exemption is possible where the absence of responsibility for the event causing the damage is proved, as are liability of multiple participants and subsequent allocation between them in the circumstances prescribed by the Article. This is not automatic joint and several liability of every company that has ever encountered an entry. [7, Article 82]

In Österreichische Post, C-300/21, on 4 May 2023, the Court of Justice made compensation dependent on the cumulative existence of an infringement, material or non-material damage and a causal link. An infringement alone is insufficient. At the same time, compensation for non-material damage cannot depend on reaching a separate threshold of seriousness. The judgment interprets the GDPR and does not establish a fixed payment for a false sanctions alert. [9]

Causation requires particular scrutiny in banking. If a bank would have refused service even without the disputed entry on an independent lawful ground, the connection between the provider's error and the entire loss claimed may be disputed. If the profile was decisive, access logs, the data version and the reasoning become significant. Several causes may also combine: inaccurate information, an unchecked decision by the bank and delay in subsequent correction. Distinguishing them cannot be achieved by a general reference to an algorithm.

The provider's contractual liability to the bank differs from a data subject's claims. Quality terms, update frequency, liability limitations and recourse may be governed by the contract and applicable national law. The bank's customer is not necessarily a party to that contract. Similarly, an administrative fine, civil compensation and a rectification order are different consequences. The existence of one does not justify promising another without a separate basis, and correcting the entry does not necessarily end a dispute over damage already caused.

22. The customer's position and distinct avenues of redress

The avenue of redress depends on what is challenged. Where identity is mistaken, the issue is the customer's link to a particular profile. Where the person is themselves currently designated on a sanctions list, the dispute concerns the lawfulness of that designation, a licence or an exception, rather than ordinary correction of another person's entry. Where a bank refuses service after a match has been resolved, the independent ground for refusal must be identified. These procedures may intersect, but are not interchangeable.

In the EU, the GDPR provides for complaints to a supervisory authority, judicial remedies and, where the relevant conditions are satisfied, compensation. The data protection authority assesses processing within its powers; it does not replace the authority empowered to amend a sanctions measure or automatically resolve every contractual dispute with a bank. A financial supervisor, ombudsman or court may address other aspects of the relationship, depending on the national system and the admissibility of the complaint. [7, Articles 77-82]

In the United Kingdom, the right to rectify inaccurate personal data is separately established in the UK GDPR. Its existence does not depend on whether the provider is a bank, although the regime's applicability and the addressee's role must be established. Restrictions on rights are assessed under UK legislation. The European GDPR judgments discussed may explain the origins of legal issues, but do not replace checking the operative UK provision and the rules governing its judicial application. [13; 14]

Reconstructing the decision over time is central to assessing a particular dispute. What data were available when the alert arose? What changed after the customer's explanation? When did the addressee receive confirmation of the error? What outcome remained thereafter? This sequence distinguishes initially justified caution from subsequent inaction and tests whether the restriction was connected specifically with the disputed entry. Without it, a provider can easily be blamed for consequences caused by an intermediary's separate decision or another legal prohibition.

The practical accessibility of a remedy matters alongside the formal existence of a right. If the subject does not know the entry, provider or actual decision-maker, identifying the object of a claim is difficult. This information asymmetry does not, however, automatically establish an infringement by a particular party. It explains the significance of source traceability, a clear distinction between roles and documented corrections for making the procedure genuinely reviewable. The research finding concerns the structure of safeguards, rather than a promise that every complaint will have the same outcome.

23. Counterarguments and alternative explanations

The first substantial counterargument is that sanctions controls must prevent a transaction before funds move beyond the reach of the restriction. Waiting for final judicial confirmation of identity in every case would make such controls ineffective. A preliminary suspension and additional checks may therefore have a lawful basis. Criticism of false alerts must recognise that function and examine the sufficiency of the factual grounds, the speed of analysis and subsequent changes in circumstances, rather than deny the preventive nature of the control.

The second counterargument concerns incomplete official identifiers. A financial institution does not always have the data needed to exclude identity quickly. This may explain a request for additional information and continuing uncertainty. An absence of data is not, however, positive evidence of a match. The missing characteristic, conflicting information and the possibility of reasonable clarification all matter. Not every unresolved case is an error; not every indefinite wait becomes justified because the matter was once unclear.

The third counterargument is the bank's independent risk management. Even after the database has been corrected, other lawful reasons for restricting a particular product may remain. Successfully challenging an entry therefore does not establish a right to every service. A commercial choice and a mandatory prohibition nevertheless rest on different grounds. Where a decision is actually based on risk policy, describing it as an inevitable requirement of sanctions law may distort the dispute. Review must establish the real reason without assuming it in advance.

The fourth counterargument concerns confidentiality and the threat of evasion. Full disclosure of all screening parameters may reduce effectiveness, while particular information is protected by law. This does not mean that internal review, correction of factual errors or oversight by a competent authority is impossible. An approach that makes every safeguard dependent on publication of all protective mechanisms creates a false choice. The possibility of disclosure is assessed separately from the ability to correct and substantiate a decision.

Finally, an adverse outcome may have several independent causes. A correspondent's hold, an error in payment details, insufficient documentation or another prohibition may coincide with the appearance of an external profile. Correlation does not establish causation. Without logs and decisions, a definitive finding against a particular participant would be premature. The report therefore formulates verifiable criteria for characterisation and liability, leaving the outcome of an individual dispute open until the facts are established.

24. Overall assessment

False positives represent several legally distinct situations rather than a single technical defect. Mistaken identification, outdated status, confusion between jurisdictions, an incorrect understanding of transaction context and retention of a disproved restriction require different evidence and corrections. The general label false positive is useful for identifying the problem, but insufficient for legal characterisation. Examining a particular case begins with precisely identifying the proposition that proved incorrect and the action based on it.

Primary sources confirm the need to distinguish an alert from a confirmed match, keep data current and investigate results substantively. At the same time, they preserve the duty to prevent an actual infringement. The European instant-transfer model and UK practice demonstrate that control arrangements depend on the particular legal framework. The universal formula that more checks mean better compliance does not reflect these distinctions; the formula that fewer alerts mean fewer errors is equally incomplete.

For personal data in the EU, rectification concerns not only an incorrect source fact but also its use in a particular profile. Notification of recipients and review of dependent decisions connect the informational and operational levels. Those levels do not merge, however: the right to a correct entry is not an unconditional right to a financial product, and lawful retention of historical information does not permit a revoked status to be represented as current. The UK framework requires separate analysis of national rules while preserving the same factual distinction between data and decision.

The potential liability of an information provider is determined by its role and a particular infringement, while a bank's responsibility depends on its own obligations and use of the result. Causation and damage are not presumed from the mere existence of an alert. Supervisory materials and case law support this analytical framework, but do not justify promising automatic compensation or identifying the responsible participant without documentary evidence. Clearly distinguishing powers and responsibilities makes both parties' claims more verifiable.

The public evidence does not establish a single error rate across the market. It supports a narrower but robust conclusion: screening quality is determined by the ability to distinguish an actual restriction from an unfounded match in a timely manner, maintain that assessment's accuracy as information changes and ensure that the consequences are corrected. This relationship between data, the legal rule and the particular decision determines whether automation remains a control tool or turns a preliminary assumption into a lasting obstacle to lawful financial activity.

25. Sources

[1] European Banking Authority. Final Report: Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures. EBA/GL/2024/14 and EBA/GL/2024/15, 14 November 2024. Applicable from 30 December 2025. In particular EBA/GL/2024/15, paragraphs 9, 13, 17-35, 43, 47-49. Official copy hosted by the Financial Market Authority Austria.
EBA / FMA - Guidelines 2024/14 and 2024/15

[2] Office of Financial Sanctions Implementation. UK financial sanctions general guidance. Sections 1-3: applicability, name matches and target matches, freezing, ownership and control.
OFSI - general guidance

[3] Financial Conduct Authority. Sanctions systems and controls: firms' response to increased sanctions due to Russia's invasion of Ukraine. 6 September 2023; updated 20 March 2024. Sections on resources, calibration and customer due diligence.
FCA - 2023 review

[4] Financial Conduct Authority. Sanctions systems and controls in our firms: our findings. 28 May 2026. In particular Sections 6.3 and 6.5-6.10.
FCA - 2026 review

[5] Office of Financial Sanctions Implementation. Imposition of Monetary Penalty - Bank of Scotland PLC. Penalty decision of 10 November 2025; published 26 January 2026. Paragraphs 1-7, 15-20, 28-29.
OFSI - Bank of Scotland

[6] College voor de Rechten van de Mens. ING discrimineert een man op grond van ras, door zijn betaling te blokkeren en controleren. Opinion No 2024-63, 25 July 2024. In particular paragraphs 6.8-6.24; Dutch original.
College - Opinion 2024-63

[7] Regulation (EU) 2016/679 of 27 April 2016 (GDPR). OJ L 119, 4 May 2016. Articles 4-6, 9-10, 12, 15-19, 22-24, 26, 28, 77-82.
EUR-Lex - GDPR

[8] Court of Justice of the European Union. Dun & Bradstreet Austria, C-203/22, judgment of 27 February 2025, ECLI:EU:C:2025:117. Paragraphs 38-76 and operative part.
CURIA - C-203/22

[9] Court of Justice of the European Union. Österreichische Post, C-300/21, judgment of 4 May 2023, ECLI:EU:C:2023:370. Article 82 GDPR: infringement, damage and causation; no threshold of seriousness for non-material damage. Paragraphs 32-42, 45-51 and operative part.
EUR-Lex - C-300/21

[10] Regulation (EU) 2024/886 of 13 March 2024 amending the rules on instant credit transfers in euro. Article 1(2): Article 5d of Regulation 260/2012, including the specific screening regime, its limits and the deadline of 9 January 2025.
EUR-Lex - Regulation 2024/886

[11] HM Treasury / OFSI. Financial sanctions targets: list of all asset freeze targets. Official notice of the cessation of updates to the OFSI Consolidated List and the transition to the UK Sanctions List from 28 January 2026.
GOV.UK - transition to a single list

[12] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692. Regulation 28: identification, monitoring and risk assessment; in particular paragraphs 11-16.
legislation.gov.uk - Regulation 28

[13] UK General Data Protection Regulation. Article 16: Right to rectification. UK version, official text on legislation.gov.uk.
legislation.gov.uk - UK GDPR, Article 16

[14] Data Protection Act 2018, c.12. Schedule 2, Part 1, paragraphs 1-2: crime and taxation exemptions and the limits of their application.
legislation.gov.uk - DPA 2018, Schedule 2

[15] Directive (EU) 2015/849 of 20 May 2015. Articles 13, 33, 39 and 40: customer due diligence, suspicious reporting, disclosure restrictions and retention. Consolidated text of 30 December 2024; implemented through national legislation.
EUR-Lex - Directive 2015/849