**Observatoire ARGA**

# INTERNATIONAL ANALYTICAL REPORT

## D-04. Deleted INTERPOL Notices

## and Commercial Screening Databases

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

23 September 2026

# Contents



Source cut-off: 23 September 2026. Keywords: INTERPOL; CCF; commercial databases; World-Check; WorldCompliance; GDPR; rectification; erasure; data recipients; bank screening.

# 1. Executive summary and principal findings

Deletion of data from INTERPOL's information system and correction of a commercial profile are separate legal processes. A decision of the Commission for the Control of INTERPOL's Files (CCF) concerns data processing within the Organization's system. A commercial screening provider and a bank using its information must assess their own processing separately. A favourable INTERPOL outcome should therefore be treated as important evidence that the information landscape has changed, rather than as a universal instruction requiring every market participant to erase all information about an individual. [1-3]

The central problem arises when past and present are conflated. The statement that a notice was published may remain historically accurate after deletion. A statement that a person is currently wanted through an INTERPOL notice requires independent substantiation as at the date of use. Even an accurate historical entry may be incomplete for the purpose of current screening if the profile does not make clear that the notice has been deleted. The legal assessment must consider not only the literal accuracy of an individual sentence, but also the purpose of processing, the category applied and the context in which the information is presented.

Articles 16 and 17 of the EU General Data Protection Regulation (GDPR) are central to the data subject's position. The former allows rectification of inaccuracies and completion of incomplete data, taking account of the purposes of processing. The latter provides for erasure on specified grounds, subject to exceptions. Additional tools include access, restriction of processing while accuracy is verified, objection to certain processing and notification of recipients of corrections. A demand to erase everything is often less persuasive than a structured explanation of which field is wrong, why it is no longer necessary and what remedy is required. [3]

Two commercial systems are examined through their own public documents: World-Check and WorldCompliance. These documents establish stated contact channels and some principles governing the handling of information. They do not demonstrate actual correction times, the completeness of updates to customer copies or the quality of individual profiles. This report contains no information from closed databases or statistics on successful complaints. Conclusions about the unlawfulness of a particular entry require examination of the entry itself and the circumstances of its use. [4-6]

The proposed approach comprises three connected tasks: establish the precise status of the underlying data; secure a proportionate change to the commercial entry; and determine which recipients received the update and whether separate correction is needed at their level. Completing the first task does not establish that the other two have been completed. Likewise, correcting a database does not equate to restoring banking services: the provider's customer may base its decision on other information and legal grounds. Practical outcomes should be described separately at each level, without substituting a promise of full reputational restoration for a legally verifiable change.

## 2. Subject matter, method and scope

Report D-04 is the third in the agreed ARGA Observatory sequence. It develops the subject of the consequences of INTERPOL data deletion, but focuses on the commercial dissemination of information and data subjects' rights vis-à-vis private organisations. National police files, SIS and independent grounds for arrest are not revisited. The analysis concerns a natural person's personal data in a commercial profile, their use in customer screening and correction mechanisms following a documented change in INTERPOL status.

Here, a screening database means a commercial information system that allows names and related information to be checked against risk categories. This is a working description, not a separate statutory category. A product's name alone cannot determine its legal regime: a single service may provide sanctions information, reports of investigations, information about public functions and other data with different sources, purposes and processing conditions. Inclusion in a commercial database must also be distinguished from inclusion on an official sanctions list.

The method is legal analysis of primary sources: the GDPR's legislative text, official INTERPOL documents, judicial decisions within the stated scope and guidance from the UK supervisory authority. Providers' public policies are examined as statements by the respective organisations. The cut-off date is 23 September 2026. Judicial findings, legal rules, provider positions and the author's proposals are distinguished; hypothetical scenarios are not presented as actual client cases.

The GDPR's applicability is not presumed merely because an individual is a European citizen, holds a European bank account or can access a website from the EU. The territorial connection required by Article 3 must be established: for example, processing in the context of the activities of a controller's establishment in the Union, or the relevant offering of goods or services to individuals in the Union or monitoring of their behaviour under the specified conditions. The subsequent discussion of GDPR rights assumes that this connection is established. The United Kingdom is addressed separately; EU provisions are not presented as a complete statement of UK law. [3]

The research limitations materially affect the assessment of its findings. Subscription interfaces, banks' internal instructions, data supply agreements and update distribution logs have not been examined. There is no representative sample of refusals or complaint decisions. The report therefore identifies legally supported lines of inquiry, but does not measure the prevalence of the problem or evaluate the performance of any particular commercial product. Stronger empirical claims would require a different evidence base and a separate data collection methodology.

## 3. What INTERPOL data deletion establishes

The first document needed for a commercial dispute is confirmation of precisely what changed within INTERPOL. A CCF decision, notification of its implementation and the disappearance of a public webpage must be distinguished. The absence of a page from a public search does not, by itself, establish the contents of the closed information system, the grounds for deletion or the date processing ceased. A persuasive position requires a document connecting the change to the particular person and data. INTERPOL's official account states that, following deletion, countries are notified so that national information can be updated; a confirming certificate may be issued in appropriate cases. This account does not establish automatic implementation by commercial providers. [1-2]

Accurately describing the subject matter of the decision is equally important. Deletion may reflect non-compliance with INTERPOL's rules, rather than a determination of the merits of criminal allegations. Without further grounds, it does not establish an acquittal, the termination of national proceedings or the falsity of every report about an investigation. Where the available reasoning is limited, missing details must not be filled with favourable assumptions. A submission may state the established outcome while separately noting that the document does not substantiate broader propositions.

Correcting a current status may not require a complete public reconstruction of the criminal case. If a commercial profile continues expressly to describe the notice as active, the central questions are proof of deletion and identity matching. A request to correct that particular assertion is not equivalent to a request to declare the individual innocent. Framing the issue in this way avoids an unnecessary dispute about events that the CCF did not adjudicate and that the provider is not authorised to determine as a criminal court.

At the same time, deletion of one entry does not exclude the existence of another. Numbers, dates, categories and jurisdictions must be compared, not merely the surname. In a hypothetical case, an old notice may have been deleted while the profile also cites an independent judicial decision. Correcting the first basis does not automatically remove the second. However, the controller should explain which assertion it retains and why the deletion confirmation does not alter its substance or currency. A generic reference to negative information does not enable the applicant to conduct a meaningful assessment.

In practice, a short chronology is useful: the original event, the date of the CCF document, the date of confirmed implementation, the date of the disputed profile version and the date of subsequent use. A chronology is not evidence in its own right; each material link requires a source. Its purpose is to identify the version that existed when the bank decided and whether the provider could already have had the update. This matters particularly where a profile was later corrected: the database's present state does not answer whether information supplied earlier was accurate.

## 4. The data chain and allocation of responsibility

A single information event can generate several separate records: an official source, a media publication, a commercial profile, a screening result and an internal bank file. Correction at one level does not guarantee technical synchronisation of the others. For legal purposes, identifying each operation and participant is more useful than saying broadly that the data remain online. The purpose, retention period and role in relation to personal data may differ at each link.

Under Article 4 GDPR, a controller determines the purposes and means of processing, while a processor acts on its behalf. Contractual labels matter, but do not replace an assessment of actual functions. A provider that independently selects sources and assigns profile categories and a bank that determines its customer screening arrangements may be separate controllers. Other arrangements are possible, but the parties cannot automatically be treated as joint controllers merely because they exchange data. That classification requires examination of their involvement in determining the particular processing. [3]

This distinction affects the requests to be made. A provider is approached about the profile, its categories, sources, dissemination and updating. A bank is approached about the personal data it holds, their currency and their use in decision-making. A publisher receives a separate request if the inaccuracy appears in its publication. Sending one generic letter to everyone may leave important questions unanswered because each recipient regards the challenge as directed at another party's conduct. It is preferable to describe the shared chronology consistently while adapting the requests to the recipient's role.

Content and transmission must be distinguished. A provider may correct the current profile, but it is also necessary to establish whether the change was communicated to recipients in circumstances covered by Article 19. A bank may receive the update while retaining the earlier report as a record of a past check. Archival retention and the use of an old status for a new assessment are different operations. The possible lawfulness of retaining history does not automatically establish the permissibility of continuing to present it as current information.

The provenance of a copy has a distinct place in the evidence model. A screenshot without a date or product identifier may not establish the controller or version. Available metadata are needed: service name, download date, profile identifier, the organisation using it and the contents of the disputed field. Such information should be obtained lawfully, without breaching access restrictions. A bank's subscription does not entitle the applicant to enter someone else's subscription system, but neither does it remove the right to request their own personal data from the relevant controller.

## 5. Accuracy, completeness and historical context

The accuracy principle in Article 5(1)(d) GDPR requires reasonable steps to rectify or erase inaccurate data, having regard to the purposes of processing. It operates alongside purpose limitation, data minimisation and storage limitation. Assessment of a commercial profile therefore cannot be reduced to whether the cited source once existed. It is necessary to determine what message the database user receives today and whether it corresponds to the individual's established position. [3]

Five elements of an entry should be distinguished: the person's identification; the event description; its procedural status; the commercial category; and the date as at which the information is current. An error in any one can alter the meaning of the others. A correct surname does not compensate for an incorrect date of birth. An accurate report of charges does not establish a conviction. A historically accurate reference to INTERPOL does not justify an active-notice flag. This typology is the author's analytical tool, not a classification binding on all providers.

A formally accurate but incomplete text poses particular difficulties. In a hypothetical entry, the publication of a notice is recorded with the correct date, but the profile is intended for current screening and omits the subsequent deletion known to the provider. A possible request is to complete the data and change the current category. The applicant should show why the omission matters for the purpose of processing, rather than merely invoke reputational harm in general terms. The addition must remain faithful to the document: deletion from the system must not become a finding that the allegation was unfounded unless such a finding exists.

A different situation is an accurate historical archive in which the date and subsequent change are clearly identified and the information is not presented as evidence of a current wanted status. Erasure of such an entry requires a separate Article 17 justification, such as loss of necessity, unlawful processing or the outcome of an objection. Disagreement with an adverse historical fact is not enough. Equally, describing a record as an archive does not create a universal GDPR exemption: questions of purpose, scope, duration and access remain.

Finally, facts and assessments must be distinguished. A risk category may reflect a provider's analytical judgment, but that does not place the underlying personal data beyond scrutiny. The applicant may challenge an incorrect factual premise, conflated statuses or the absence of a material update. Seeking disclosure and verification of that premise is more precise than demanding a zero-risk classification: data protection law does not guarantee the desired commercial assessment in every circumstance.

## 6. Rectification under Article 16 GDPR

Article 16 provides a right to rectification of inaccurate personal data without undue delay and to completion of incomplete data, including by a supplementary statement, taking account of the purposes of processing. For this subject, it is often the most direct tool: it allows an incorrect current status to be replaced, an event to be clarified or a confirmed CCF outcome to be added without denying the entire historical record. Rectification should not be portrayed as an inferior alternative to erasure; it may address the infringement more precisely. [3]

The subject of the request should be identifiable and reproducible. It is useful to quote the disputed wording, identify its location or field, state the version date and propose the correct content. The document substantiating the change should then be explained. Where the profile is unavailable, the applicant should identify the source of information about the suspected error and request access at the same time. A specific entry must not be attributed to a database solely on the basis of a bank refusal or an intermediary's assumption: processing must first be established, or expressly identified as unconfirmed.

The proposed correction should distinguish at least two questions: what should be removed as incorrect and what should be added as necessary context. Documented cessation of the processing of a notice may, for example, require removal of an active flag and recording of the deletion date. If the applicant also seeks removal of related reports of a national investigation, that is a separate part of the request requiring its own grounds. Separating the requests makes partial compliance assessable and permits a refusal on one point to be challenged without losing what has already been achieved.

A supplementary statement by the data subject has practical value, but should not be used as a universal substitute for correcting an established error. Where a current status is objectively wrong, adding that the applicant disagrees may leave the main inaccuracy unchanged. Conversely, where information is incomplete or a matter is genuinely disputed, an agreed explanation can clarify the meaning. The legal assessment depends on whether the problem has been resolved for the purpose of processing, rather than on the mere addition of text.

The controller's response should be assessed substantively. A statement that the profile has been updated does not establish which fields changed, when this happened or whether the previous category remains. It is reasonable to seek confirmation of the outcome concerning the applicant's own data and information about recipient notification. This does not imply an unconditional right to internal source code or a complete commercial log: information needed to exercise rights should be distinguished from an indeterminate demand to disclose the provider's entire infrastructure.

## 7. Erasure under Article 17: grounds and limits

Article 17 GDPR provides several distinct grounds for erasure. The most relevant to a commercial profile are the data no longer being necessary for the processing purpose, unlawful processing and a successful objection where no overriding legitimate grounds remain. Withdrawal of consent may also matter where consent is the basis and no other basis exists, but a professional screening database cannot be assumed always to rely on consent. The request must address the actual stated basis for processing. [3]

Loss of necessity requires analysis of the particular purpose. If the entry's sole content was an active notice and that status has ended, the question is why the profile or category is retained. However, the age of information does not alone establish that it is unnecessary, and a commercial interest in historical information does not establish necessity. The controller should explain why these particular data are required, to this extent and for this duration. The applicant may, in turn, show that a less burdensome presentation would achieve the stated purpose.

Unlawfulness cannot be inferred solely from a CCF decision. Separate issues may include the absence of an applicable Article 6 basis, non-compliance with Article 10's additional conditions or a breach of accuracy or minimisation principles. Each requires factual and legal substantiation. If particular information falls within the regime for data relating to criminal convictions and offences, invoking legitimate interests under Article 6 is not enough to complete the analysis: Article 10 imposes additional conditions. Their national implementation is not examined here for every EU Member State. [3]

The exceptions in Article 17(3) likewise require a specific assessment. They include freedom of expression and information, a relevant legal obligation, performance of a public task, specified public-interest and research purposes, and the establishment, exercise or defence of legal claims. An exception applicable to one operation cannot automatically extend to the entire profile and all recipients. Reference to a potential dispute does not explain indefinite dissemination of any and all information to an undefined range of customers.

A properly framed request may proceed in stages: erase identified data on the stated ground; if the controller considers erasure inapplicable, explain the exception and its scope; and, independently, correct the inaccurate current status and consider restriction while verification takes place. This structure preserves legal precision. It does not assume that every alternative must succeed, but prevents refusal of complete erasure from obscuring the separate question of accuracy.

## 8. Restriction of processing and objection

An accuracy dispute may continue while an entry is used for new checks. Article 18(1)(a) GDPR provides for restriction during the period needed for the controller to verify the accuracy of contested data. It is therefore useful to accompany the request with a distinct request to consider restriction, identifying the particular inaccuracy and supporting evidence. Restriction is neither automatic erasure nor a universal ban on every operation: restricted processing has its own conditions. [3]

Under Article 18(2), processing beyond storage is permitted in specified circumstances, including with the data subject's consent, for legal claims, to protect another person's rights or for reasons of important public interest. The subject must be informed before restriction is lifted. In a commercial dispute, it is useful to establish how restriction affects the disputed entry and its transmission. Without access to the product, however, one cannot assert in advance that a particular interface flag ensures compliance or that the absence of a known flag establishes a breach.

Article 21(1) concerns processing based on Article 6(1)(e) or (f) and requires consideration of the subject's particular situation. Arguments may include confirmed notice deletion, the absence of a current basis for the previous category, disproportionate consequences and a less burdensome way to present the history. The controller must assess whether there are compelling legitimate grounds overriding the individual's interests, rights and freedoms, or grounds relating to legal claims. The absolute objection regime for direct marketing cannot be transposed to AML screening. [3]

Restriction and objection serve different purposes. The former may preserve the position while verification occurs; the latter seeks to stop particular processing in light of its basis and the individual's situation. Conflating the terms may produce a response to the wrong question. A letter should distinguish the subject of each request and identify the data it covers. If the issue concerns only a deleted notice, the request should not extend without explanation to unrelated information.

Preserving evidence before a profile changes is practically important. An applicant may need the earlier version to substantiate a complaint or losses; a controller may need limited retention to defend legal claims. A demand to destroy every trace of processing immediately can therefore conflict with the applicant's own interest in establishing an earlier infringement. One possible approach is to distinguish cessation of ordinary dissemination from justified retention of evidential material for a limited purpose. The permissibility of that solution depends on the particular basis and is not presumed.

## 9. Access and identification of recipients

Access under Article 15 GDPR helps move from assumptions to a verifiable record. A request may cover confirmation of processing, the person's own personal data, purposes, categories, recipients, the anticipated retention period or criteria for determining it, and available source information where data were not obtained from the subject. This can establish whether the challenge concerns an outdated official status, a summary of a publication or an independent category. The right to a copy of personal data should not be described without qualification as a right to the entire commercial product. [3]

In C-154/21, the Court of Justice clarified the significance of recipient information. Where data have been or will be disclosed, the subject is in principle entitled to know the actual recipients. Providing only categories is permissible where recipients cannot be identified or the controller demonstrates that the request is manifestly unfounded or excessive. This finding helps direct subsequent requests to organisations that actually received the data, but does not guarantee that a particular technical log exists or that a specified export format is available. The case did not concern correction of a World-Check profile. [7]

Article 19 links rectification, erasure and restriction to notification of recipients to whom data were disclosed, unless this proves impossible or involves disproportionate effort. On request, the subject is informed about those recipients. An actual recipient of the disputed data must be distinguished from any organisation subscribing to the product. The provision should not be paraphrased as an obligation to circulate the individual's history to every customer, irrespective of whether that customer received the information. [3]

A request usefully separates three questions: to whom the data were disclosed; who was notified of the change; and what exceptions were relied upon and why. This is the author's suggested structure, not a prescribed form. It helps identify incomplete answers: for example, a list of customer categories without explaining why actual recipients cannot be identified, or confirmation of correction without addressing notification. Assessment of the response must take account of others' rights and applicable restrictions; commercial sensitivity and system size do not by themselves replace legal justification.

Notification does not amount to proven amendment of all the recipient's systems. A bank receiving the message may hold several related records and have its own retention obligations. If there are grounds to believe it continues using the previous status, a separate request is necessary. The notification date is particularly useful at that stage: it allows a specific question about which data were used after the update arrived, without assuming that the bank's error has already been established.

## 10. World-Check: public procedure and matters to verify

World-Check's public notice identifies Refinitiv Limited as controller in the stated context and provides for requests for access, correction and consideration of deletion through contact@world-check.com, subject to identity verification. It recognises the possibility of errors and outdated information, while linking outcomes to accuracy, relevance and grounds for continued processing. Inclusion is not presented as sufficient in itself for an adverse inference; users are directed to undertake their own verification. This describes the provider's position, not a finding of compliance in every case. [4]

For the applicant, the response concerning the disputed field matters more than the product's general description. If a CCF document concerns the same person and entry, it is necessary to establish which category will remain after updating, what assertion it conveys and which source supports it. Outcomes may differ: changing a current status, clarifying the historical account, removing one basis or deleting the profile. The report does not claim that the policy requires the same result whenever INTERPOL data are deleted.

Identity verification has an understandable purpose: preventing disclosure to outsiders and changes prompted by a false request. However, the amount of additional information requested also requires justification. It is sensible to confirm a secure transmission channel and send only what is necessary to establish identity and a representative's authority. The entire criminal case file should not automatically be the first attachment when the dispute concerns a single verifiable status. Excessive disclosure creates new risks and makes the evidence actually relevant to the request harder to isolate.

Where the provider invokes an independent source, it is necessary to check whether that source supports the assertion being retained. A report of an earlier arrest does not necessarily establish an active notice; reporting of an investigation is not equivalent to a conviction. The question should address substance: which element of the profile relies on that source, and why does the update not affect its accuracy or necessity? This approach allows lawful historical information to remain while preventing one event from being substituted for another.

After a response arrives, the outcome should be compared with the original request point by point. Have the new data been confirmed, has restriction been considered and has recipient notification been addressed? An official contact channel facilitates the start of the procedure but does not establish its completion. Without an individual response, neither refusal by the provider to comply with the law nor actual correction across all customer copies can be asserted.

## 11. WorldCompliance: source, profile and independent obligation

The LexisNexis Financial Crime Compliance Solutions notice, updated in December 2025, describes the processing of information for screening and potential rights of access, correction, deletion and restriction under applicable law. It provides separate request routes for the United States and other jurisdictions. The provider states that it does not make customers' decisions and that its data should not be their sole basis. These provisions describe the service's stated arrangements; customers' actual compliance with contractual requirements was not examined. [5]

The WorldCompliance section of the Consumer and Data Access Policies page addresses access and challenges to errors; it also notes that the third-party origin of information may require an approach to the original source. Such a response must be assessed separately from the controller's obligation under applicable legislation. A public policy creates no independent exception to Article 16 GDPR. Equally, its existence does not establish that the provider will refuse to correct a substantiated inaccuracy in a particular case. [6]

Two separate issues arise. The first is the original publication's content: for example, misidentification or a report of an event that never occurred. The second is the provider's own processing: an incorrect category, missing update or presentation of an old report as current status. Correcting the publication may help in both situations, but waiting for the publisher's decision does not always answer the independent question of the commercial entry's accuracy. A request should expressly identify which part concerns each level.

Where a source is historically accurate, demanding that it be rewritten as though the material had never existed may be unjustified. Nevertheless, the commercial profile may require completion with information about the notice's subsequent deletion. The absence of an error by the publisher does not exclude incompleteness by an aggregator using the information for a different purpose. This is an analytical conclusion drawn from the distinction between operations and accuracy requirements, not a judicial finding that the product concerned is unlawful.

Comparison of the two providers has a limited purpose: to demonstrate the need to read the particular controller's current policy and avoid transferring one service's procedure to another. It is not a quality ranking. Evaluating actual performance would require comparable individual requests, documented responses and checks of subsequent profile versions. ARGA claims no such sample in this report; the recommendations are based on legal rules and documented public channels.

## 12. Judicial guidance and the limits of analogy

Case law is useful when its legal finding is matched to the subject of the particular dispute. A decision about search results does not become a decision about a subscription database, and an interpretation of the right to recipient information does not establish causation between an entry and a banking refusal. This study identifies three narrow points of guidance: access to recipients, assessment of a request alleging inaccuracy and the conditions for compensation. Each is used within the verified text's limits. [7-9]

C-154/21 directly interprets the general right of access and assists in identifying the addressees of further requests. Its application here to commercial screening is the author's analysis: a subject may seek actual recipient identities to exercise rights to rectification and legal protection. The judgment does not require a provider to guess all indirect users or name organisations that never received the data. The request must remain linked to actual processing, and exceptions must be assessed against the Court's standard. [7]

C-460/20 concerned search-engine de-referencing. The verified paragraphs 72-73 link the outcome to relevant and sufficient evidence of manifest inaccuracy in all the content or a non-minor part of it; where inaccuracy is not apparent from the evidence and there is no corresponding judicial decision, an obligation to grant the request does not arise on that basis. The full judgment could not be accessed directly during this verification exercise; use is limited to the identified official excerpts. The particular approach to a search engine is not transposed into Article 16 as an additional universal condition for profile correction. [8]

In C-300/21, the Court held that a GDPR infringement alone is insufficient for compensation and that compensation for non-material damage cannot depend on reaching a minimum threshold of seriousness. Damage and a causal link remain material to an Article 82 claim. This report uses the officially published operative part; it does not report an award of a particular amount to the applicant or present the case as an INTERPOL dispute. [3, 9]

The practical conclusion is that remedies must be separated. Correction of an inaccurate field does not require prior proof of a monetary loss equal to a cancelled contract. For compensation, conversely, correction following a complaint is not enough by itself: infringement, damage and causation must be established. To seek reconsideration of a banking decision, it is necessary to understand which data were actually used. Combining these tasks into one undifferentiated demand weakens the evidential position and creates expectations that the relevant procedure does not guarantee.

## 13. The United Kingdom: a separate legal route

The UK dimension cannot be addressed simply by replacing the name of a European supervisory authority with the ICO. Following the 2025-2026 reforms, the applicable UK GDPR, Data Protection Act 2018 and commenced amendments must be checked. This section is limited to two verified issues: processing of criminal offence data and complaints to controllers. It is not a comprehensive review of the UK regime or all its exceptions. [10-12]

The ICO explains that processing criminal data requires not only a general lawful basis, but also official authority or the relevant legal authorisation with appropriate safeguards. Where there is no official authority, the DPA 2018 conditions matter. The ICO page is marked as under review following the Data (Use and Access) Act 2025; it is therefore used for this limited distinction, rather than as confirmation that every aspect of the guidance is fully current. In an individual case, the particular condition must be checked against the legislation in force. [10]

According to the ICO's official announcement, new complaint-handling requirements took effect on 19 June 2026. An organisation must provide a way to make a data protection complaint, acknowledge receipt within 30 days, take appropriate investigative steps without undue delay, keep the complainant informed and communicate the outcome. The 30-day period concerns acknowledgement, not a promise that the dispute will be finally resolved or the profile deleted within that time. [11-12]

This distinction should be reflected in the timetable for correspondence. A request to exercise a right and a complaint about its infringement may serve different procedural functions. An automated acknowledgement does not mean that the merits have been addressed; equally, the absence of a final decision on day 30 does not, without further analysis, establish breach of a final-response deadline. For a UK request, time limits and any particular features must be checked separately; the EU GDPR Article 12 rules discussed below are not presented as a complete account of the post-reform UK GDPR.

For a cross-border profile, the legal entity, processing role and applicable regime must be established, rather than selecting a jurisdiction solely because its online form is convenient. A single factual episode may involve several organisations, but that does not justify promising the same procedure and outcome in every country. The UK route in this report illustrates the need for separate legal classification while preserving the common practical principle: identify the record and controller first, then select the applicable law and remedy.

## 14. Preparing evidence and sequencing requests

The first stage is to preserve available documents in their original form and list what each establishes. A CCF decision establishes its own subject matter; a bank letter establishes the reason communicated by the bank or the fact of refusal; a profile establishes the contents of a particular version. None should be used as a substitute for another. An unclear source is recorded as a gap to be addressed through access, not as an established fact that a particular database was used.

The second stage is to establish identity. Available identifiers for the individual, the INTERPOL entry and the commercial profile are compared. Where a common name matches, date of birth, nationality, related organisations and the event's circumstances become particularly relevant. Only necessary data should be used; information about relatives or third parties is not included automatically. If the dispute arises from a false match, the request concerns the incorrect association with the person, not only the notice's status. Deletion of an accurate entry about someone else is not a necessary outcome of such a dispute.

The third stage is to formulate requests on separate grounds. Under EU GDPR these may comprise access under Article 15, rectification under Article 16, erasure of specified data under Article 17, restriction under Article 18, recipient notification under Article 19 and objection under Article 21 where the relevant basis applies. There is no need to recite every provision mechanically: each request should have its own subject and explanation. An excessive set of unrelated allegations makes the response harder to assess and may obscure the strongest argument.

The fourth stage is to maintain a procedural chronology. Under Article 12 EU GDPR, information about action taken on a request is provided without undue delay and normally within one month; where necessary, the period may be extended by two further months, with notification and reasons in the first month. This does not guarantee successful deletion or full restoration of services within a month. Where no action is taken, reasons and information about complaints and judicial remedies matter. If there are reasonable doubts about identity, the controller may request additional information to confirm it. [3]

The fifth stage is to verify the result, rather than merely the existence of correspondence. The changes claimed and the response are compared against each disputed element; recipient notification and the position at a known data user are assessed separately. Unresolved issues are carried into a complaint with the chronology, documents and a specific subject. The author's recommendation is to prepare a concise principal explanation and an organised evidence set, avoiding emotive accusations and predictions of a future court outcome.

If the response does not remedy the alleged infringement, Article 77 GDPR provides for a complaint to a supervisory authority, particularly in the Member State of habitual residence, place of work or alleged infringement. Article 79 provides a judicial remedy against a controller or processor without prejudice to administrative and non-judicial remedies. Identifying the competent authority and court requires assessment of the circumstances; making a complaint does not predetermine an obligation to restore banking services. The complaint's subject should distinguish inaccuracy, refusal to facilitate a right and a claim for compensation, for which the Article 82 conditions are assessed separately. [3]

## 15. The customer copy and the bank's decision

A commercial profile is an information input; a bank's decision is a separate act. Even proven correction by a provider does not establish that the bank used that particular entry or that it was the sole basis for refusal. Analysis should begin with the bank's available explanation and the individual's own data obtained lawfully. If details are not disclosed, the gap must not automatically be filled with an assumption about a particular product or motive. Possible lawful disclosure restrictions are assessed separately under the applicable law.

Following confirmed correction, the applicant may send the bank evidence of the new status and ask it to check the currency of its own data, update the relevant field and reconsider its decision within the applicable procedure. These requests differ in legal character. Rectification of personal data does not itself create a general entitlement to any financial product. Possible rights to a particular type of account, contractual obligations and procedures for challenging banking conduct require a separate jurisdiction-specific assessment, which this report does not undertake.

An internal copy of an earlier report may preserve evidence that an organisation screened the customer on a particular date. The question is how it is labelled and used after the update is received. Retention of the earlier version as history, with correction reflected in the current assessment, differs from renewed use of an old active status. A demand to destroy the entire archive may disregard

lawful retention obligations; a request to separate the historical version from the current status may address the dispute more precisely.

If refusal continues, it is useful to establish which issues remain unresolved after updating. This does not necessarily mean a right to the entire internal risk analysis. A response may nevertheless show that the disputed status was corrected while the decision concerns something else. For subsequent protection, it is important not to conflate an established data infringement with an unmet commercial expectation. Both may matter, but they require different legal rules and evidence.

Causation is particularly important in a compensation claim. Available information is needed about the timing of transmission, the profile version, the decision date and the consequences suffered. Temporal sequence alone does not establish cause: a refusal after publication does not prove a refusal because of publication. However, an express reference to the erroneous status, repetition of the same wording or documented receipt of the profile may contribute to the overall assessment. Their legal weight is determined in the particular proceedings, not in advance by an analytical report.

## 16. Counterarguments and testing the position

The first strong counterargument is historical accuracy. A provider may point out that an event actually occurred and does not disappear from history when a notice is deleted. The response should not deny the obvious. It is necessary to establish whether the applicant challenges the event's existence or its present depiction. If the historical entry is accurate and clearly supplemented by the subsequent change, erasure requires other grounds; if the old status is presented as current, historical accuracy does not resolve the problem.

The second counterargument is the need for AML screening and prevention of financial crime. A lawful purpose may justify certain processing, but does not establish the necessity of any quantity of data, any category or indefinite dissemination. The question is specific: how does the disputed field serve the purpose after updating, and is there a less burdensome way to present the relevant history? The report sets no universal retention period and does not assume that every commercial provider has the same duties as a bank.

The third counterargument is the continued existence of independent sources. Where a profile has several bases, removal of one does not eliminate the others. Each assertion should be assessed separately. However, a source substantiating one event cannot be replaced by a reference to any other adverse report. A reasoned response must connect the fact, category and purpose. The applicant's acceptance that one historical element may remain does not waive the right to correct another.

The fourth counterargument is the impossibility of controlling every copy. A provider cannot promise actual destruction of each document already held by a separate controller. This is precisely why Article 19 concerns recipient notification and provides exceptions, while individual follow-up continues with known users. Limited technical control must not be converted into a complete

absence of obligations, but neither can one promise that a single letter will make information disappear universally.

The fifth counterargument is insufficient evidence from the applicant. This requires an honest assessment. An illegible letter, an unverified translation or a document about another notice may prevent the controller from verifying the request. The deficiency should be addressed rather than every additional question being characterised as abuse. At the same time, requests for evidence should remain connected to the matter being checked. If a document unambiguously establishes deletion of a particular entry, a demand to prove innocence in the entire criminal case may concern a different task and requires a separate explanation.

## 17. Hypothetical scenarios and recommendations

All the following situations are the author's models, not accounts of ARGA clients or established provider infringements. In the first scenario, a profile retains an active INTERPOL flag after confirmed deletion. The principal route is correction of the particular status supported by the deletion document, consideration of restriction during verification and an inquiry about recipient notification. A demand to declare the national allegation false is not included without independent evidence. Success is measured by the new status and compliance with related duties, not automatically by resumed services.

In the second scenario, an entry clearly describes the historical notice and its subsequent deletion, but remains available for screening. Current inaccuracy cannot be declared in advance. Analysis shifts to necessity, scope, processing basis, additional conditions for criminal data and applicable erasure exceptions. Continued use may be challenged as disproportionate, but the CCF document does not replace that argument. The outcome may be retention of some information, a category change or erasure, depending on the facts established.

In the third scenario, the provider has corrected the profile, but the bank uses an old export. The copy's contents and date must be confirmed, the update supplied to the bank, correction of its own data requested and the applicable reconsideration procedure identified. Article 19 notification is examined at the same time. Responsibility cannot automatically be assigned exclusively to either provider or bank: roles, actual conduct and when each received information about the change all matter.

In the fourth scenario, the bank's refusal is known, but the profile and source are unidentified. The starting point is clarification and access, rather than a public accusation against a particular database. If a false match is established, the link between person and entry is corrected; if historical data about the same person were used, accuracy and purpose are examined. This scenario shows why early classification without documents can direct effort to the wrong addressee.

For providers, the author's recommendation is to distinguish clearly between current and historical statuses, record the date of a confirmed change and provide a verifiable correction and notification procedure. For data users, it is to verify material information and reflect updates in their own records. For data subjects, it is to preserve evidence, frame requests by particular field and

separately check the outcome with a known recipient. These proposals are not presented as an existing ARGA standard, a mandatory product specification or an empirically validated efficiency programme.

## 18. Conclusion: what counts as correcting the information record

Legally meaningful correction begins with an accurate description of the INTERPOL outcome. Deletion must be reflected where the previous status is used as current, but does not automatically rebut every historical fact. This position protects accuracy without requiring a commercial controller to take the place of a criminal court. Its strength lies in the verifiability of a particular assertion and the fit between the chosen remedy and its subject.

For Article 16, the central question is inaccuracy or incompleteness in light of the purpose. For Article 17, it is the existence of an erasure ground and the scope of exceptions. Articles 18, 19 and 21 address interim protection, dissemination of updates and the continued permissibility of processing; Article 15 assists in establishing the record's contents and recipients. These tools form a sequence, but do not guarantee the same outcome across jurisdictions and products. Each provision's applicability must be established rather than assumed from the database's name.

Outcomes should be described at four levels: the underlying status has changed; the commercial profile has been corrected; the relevant recipients have been notified; and the known user's own record has been checked. The last level is not equivalent to the desired commercial decision. Recording each separately permits an honest account of partial success and identifies the next step. An unqualified statement that everything has been deleted can conceal both a continuing error and lawfully retained history that is not erroneous.

The study supports a specific, documented approach, but does not establish the scale of market infringements. Further monitoring requires an anonymised observation methodology, lawful access to profile versions, comparable requests and verification of responses. Until that evidence exists, error rates, average correction times and ARGA achievements in restoring services cannot be claimed. This report provides a legal and evidential basis for individual assessment while keeping those limitations explicit.

# 19. Sources and references

**[1]** INTERPOL. Compliance and review. Official account of the consequences of notice deletion and confirming documents. Accessed 23 September 2026.
https://www.interpol.int/How-we-work/Notices/Compliance-and-review

**[2]** INTERPOL. Statute of the Commission for the Control of INTERPOL's Files. 2025 edition, amendments of 27 November 2025. Articles 33(4), 38–41; limits of competence and implementation.
https://www.interpol.int/en/content/download/5695/file/Statute%20of%20the%20CCF%20(E).pdf?inLanguage=eng-GB&version=17

**[3]** European Parliament and Council. Regulation (EU) 2016/679 of 27 April 2016 (GDPR), OJ L119, 4 May 2016. Articles 3–6, 10, 12, 15–19, 21, 77, 79, 82. The official original EU text reproduced on legislation.gov.uk was read; this is not the consolidated UK GDPR. EUR-Lex identifier: CELEX 32016R0679.
https://www.legislation.gov.uk/eur/2016/679/pdfs/eur_20160679_adopted_en.pdf

**[4]** LSEG. World-Check Privacy Statement. Public controller notice: access, rectification, limits to deletion and users' role. Provider statements, not an independent audit. Accessed 23 September 2026.
lseg.com/.../world-check-kyc-screening/about/privacy-statement

**[5]** LexisNexis Risk Solutions. Financial Crime Compliance Solutions Processing Notice. Last updated December 2025. Public notice on processing and routes for exercising rights.
https://risk.lexisnexis.com/corporate/processing-notices/financial-crime-compliance-services

**[6]** LexisNexis Risk Solutions. Consumer and Data Access Policies. WorldCompliance subsection only: access, disputes about errors and approaching the original source. Accessed 23 September 2026.
https://risk.lexisnexis.com/consumer-and-data-access-policies

**[7]** Court of Justice of the European Union. RW v Österreichische Post AG, C-154/21, 12 January 2023, ECLI:EU:C:2023:3. Full official text; in particular paragraphs 37–51 on actual recipients and exceptions.
https://juris.curia.europa.eu/juris/document/document.jsf?docid=269146&doclang=en

**[8]** Court of Justice of the European Union. TU, RE v Google LLC, C-460/20, 8 December 2022, ECLI:EU:C:2022:962. Officially indexed paragraphs 72–73 were used. The full text was not directly obtained; a narrow comparative finding, not a rule about commercial databases.
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62020CJ0460

**[9]** Court of Justice of the European Union. UI v Österreichische Post AG, C-300/21, 4 May 2023. Official operative part: OJ C216, 19 June 2023, pp. 6–7, 2023/C 216/07. Infringement alone is insufficient for compensation; a minimum seriousness threshold for non-material damage is impermissible.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CA0300

**[10]** Information Commissioner's Office. What are the rules on criminal offence data? Marked as under review following the Data (Use and Access) Act 2025. Used only to distinguish a general lawful basis from an additional processing condition.
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/criminal-offence-data/what-are-the-rules-on-criminal-offence-data/

**[11]** Information Commissioner's Office. How to deal with data protection complaints. Published 12 February 2026, updated 8 May 2026. Official complaints guidance.
https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/

**[12]** Information Commissioner's Office. One month to go: what businesses need to know to meet new data law. 19 May 2026. Confirms commencement of complaints requirements on 19 June 2026 and the acknowledgement deadline.
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/05/one-month-to-go-what-businesses-need-to-know-to-meet-new-data-law/