Asylum Research&Global Assistance

ARGA POSITION

on the issue of coordinating confidentiality requirements and the reasons for decisions of the Commission for the Control of INTERPOL Files

Contribution to the Fourth Call for Contributions from Civil Society to the CPD Articles 35(3) and 38(3) of the CCF Statute

ARGA is a non-governmental organization with practical expertise in the implementation of CCF mechanisms, personal data protection, and international police cooperation. This material is presented solely as a neutral expert contribution to the ongoing review of the CCF Statute.

Table of contents

1. Summary

Article 35 of the CCF Statute presumes that information must be accessible to the applicant and the data source, but allows the Requests Chamber to restrict its disclosure to protect specific legitimate interests. Article 38 simultaneously requires that the decision be reasoned and communicated to both parties, taking into account confidentiality requirements. These provisions should not be considered mutually exclusive. Confidentiality may limit the disclosure of certain information, sources, or methods, but it must not preclude a clear presentation of the factual and legal reasoning underlying the outcome.

ARGA proposes the principle of maximum substantive disclosure consistent with legitimate confidentiality. This is implemented through a presumption of disclosure, individual justification of each restriction, a necessity and proportionality check, the priority of redaction over complete non-disclosure, mandatory substantive disclosure of the essence of the withheld material, and the preparation of versions of the decision tailored to each party.

The proposed model does not require absolute transparency, does not compromise ongoing investigations, or limit the CCF's independence. On the contrary, it provides the Requests Chamber with a consistent set of tools that simultaneously protect sensitive information, maintain the trust of data sources, and provide parties with sufficient understanding of the decision, including for the practical use of the Article 42 review mechanism.

2. Institutional context

The formal consultation question concerns the alignment of two elements of the current Statute. According to Article 35(1), information related to a request is available to the applicant and the data source, subject to the restrictions provided. Article 35(3) allows the Requests Chamber to restrict the disclosure of information on its own initiative or at the request of the applicant, the data source, or the General Secretariat in order to protect public security or national security or the prevention of crime;

the confidentiality of an investigation or prosecution; the rights and freedoms of the applicant or third parties; or the ability of the Commission and the Organization to properly perform their functions.

Article 35(4) already contains an important procedural basis: the restriction must be justified, and the party requesting it must indicate whether it is possible to provide some of the information, in particular in summary form. Article 38(2), in turn, requires a written and reasoned decision containing, among other things, a summary of the proceedings and the parties' positions, the established facts, the application of INTERPOL rules, an analysis of the legal arguments, and an operative part. Under Article 38(3), the decision is provided to the applicant and the data source, taking into account confidentiality requirements and restrictions.

Therefore, the issue is not one of choosing between confidentiality and justification. It is necessary to determine the minimum amount of disclosure that preserves the meaningfulness of the decision when specific elements of the case cannot be communicated to one or both parties.

2.1 Contents of each ground of Article 35(3)

The grounds related to public or national security and crime prevention potentially encompass the broadest range of information: operational methods, areas of international cooperation, threat assessments, information on suspected accomplices, arrest plans, surveillance data, and other elements whose disclosure could undermine the effectiveness of crime prevention. It is precisely the breadth of this ground that requires individualization. It is not sufficient to establish that the material relates to security or crime prevention; it is necessary to determine which element of the information creates the risk and whether the protected interest can be preserved by redacting specific details.

The principle of confidentiality of an investigation or prosecution protects not the abstract status of an ongoing investigation, but its actual effectiveness and integrity. Potential risks include the disclosure of investigative leads, warning individuals of planned actions, influencing witnesses, destruction of evidence, coordination of testimony, or the premature disclosure of materials protected by national law. However, the mere existence of an investigation should not automatically conceal information already officially known to a party, the general classification of the alleged act, or a neutral description of a factual allegation, unless disclosing them would create additional risk.

The rights and freedoms of the applicant or third parties require a separate analysis of the recipient of the disclosure. Information that is safe to communicate to the applicant may be dangerous when transmitted to the data source; conversely, a data source's document may contain personal information of a witness that the applicant does not need to understand the rationale behind the decision. The protection of privacy, physical safety, confidential contacts, and international protection status must be balanced with the disclosure of the actual substance of the material in anonymized or aggregated form.

The ground of proper discharge of duties of the Commission or the Organization must be interpreted in a way that protects the institutional capacity of the CCF and INTERPOL to perform their functions, but does not become a general basis for withholding inconvenient or complex information. It may be relevant, for example, to protect internal working methods, confidential consultations, the security of information systems, or trusted channels of cooperation. When applying this ground, it is particularly important to explain why the disclosure of specific information, rather than simply an additional administrative burden, could actually impede the performance of functions.

2.2. Who initiates the restriction and who is responsible for assessing it?

Article 35 allows for restrictions to be imposed either at the initiative of the Requests Chamber or at the request of the applicant, the data source, or the General Secretariat. This means that the ultimate responsibility for the scope of disclosure cannot be entirely shifted to the party designating the material as confidential. Such a party provides information on the nature of the risk, but it is the CCF, as an independent body, that determines whether the restriction complies with the Statute and what remedy is sufficient.

A confidentiality request should be considered as input for an independent assessment, not as a mandatory directive. At the same time, the absence or insufficient detail of such a request should not compel the CCF to disclose information if the materials clearly pose an independent risk to the investigation, security, the applicant, or third parties. In this situation, the CCF may act on its own initiative, recording the basis applied and the reason for the restriction in its internal decision.

3. Guiding principle

ARGA believes that the following principle could serve as the starting point for Articles 35 and 38: transparency should be functional rather than absolute. Confidentiality may protect information, sources, and legitimate interests, but should not conceal the substance of the case or the reasoning that determines its outcome.

In this formula, disclosure is functional if a party is able to understand: what issues were decisive; what material facts were taken into account; what legal rules and reasons were applied; why the result was favorable or unfavorable; and whether there is practical reason to seek reconsideration if new facts emerge.

This approach preserves the CCF's authority to independently determine the scope of disclosure. It also eliminates automaticity: neither a reference to an ongoing investigation nor a reference to national security should, in and of itself, imply a complete closure of all related materials. Specific information and the specific risk arising from its disclosure to a specific party are subject to assessment.

3.1 What does meaningful disclosure mean in practice?

Meaningful disclosure should not be measured by the number of pages disclosed or the percentage of clear text. A large volume of secondary information does not compensate for the absence of a single fact that determined the outcome. Conversely, a brief but precise summary of the nature of the decisive material, its evidentiary value, and its impact on the conclusion can be more meaningful than a lengthy document with numerous redactions.

Functional sufficiency must be assessed from the perspective of the addressee of the decision. After reading the reported version, the party must be able to reconstruct the basic chain of reasoning: what issue was considered, what versions of the facts existed, what material circumstances the CCF found established, which INTERPOL rules were applied, and why these elements led to a specific operative part. If one element of the chain is closed, the decision must contain its secure functional equivalent.

However, meaningful disclosure does not imply a right to full access to case materials, the right to know the identity of each source, or the right to obtain operational evidence in its original form. The model is concerned with sufficient understanding of the decision, not a full reproduction of the CCF's internal file.

4. The proposed model

4.1 Presumption of meaningful disclosure

The basic rule should remain the disclosure of information necessary for the party to understand the proceedings and the decision. Limitations are exceptional and require individualized justification. This does not imply a presumption in favor of full disclosure of every document; the presumption relates to sufficient disclosure of the factual and legal grounds.

4.2. Checking necessity and proportionality

Before limiting the disclosure of Requests Chamber, it is advisable to establish consistently:

1. which specific ground of Article 35(3) applies;
2. what specific and reasonably foreseeable risk would be created by disclosure;
3. is a restriction necessary to prevent this risk;
4. whether the scope of the limitation is proportionate to the significance of the protected interest;
5. can the same interest be protected in a less restrictive way.

This test does not require the data source to disclose the sensitive information itself to justify its protection. It is sufficient to specify the risk category and the causal link between the disclosure and the anticipated harm to the extent possible without self-disclosure of the protected information.

4.3. Sequence of disclosure methods

Complete non-disclosure should be used after consideration of less restrictive options. For each category of material, the CCF may evaluate sequentially:

1. full disclosure;
2. partial disclosure of individual fragments;
3. edited version of the document;
4. anonymization of names, identifiers, locations, methods or other sensitive details;
5. a substantive summary or gist;
6. complete non-disclosure unless other means eliminate the specific risk.

Editing should be aimed at preserving meaning. Mechanically removing so much text that the remaining version obscures the meaning of the material is formally considered partial disclosure, but is functionally equivalent to complete non-disclosure.

4.4. Mandatory presentation of the essence of the material

If a document or individual fact cannot be disclosed, the party should disclose its substantive gist to the greatest extent possible. The statement that "the Commission reviewed confidential information" explains neither the nature of the material nor its role in the conclusions and therefore provides no substantive justification.

The Gist, subject to applicable limitations, must allow for a clear understanding of the category of information, the factual assertion it confirms or refutes, the degree of importance assigned to it by the CCF, and its impact on the outcome. However, the presentation may exclude sources, operational methods, third-party data, precise locations, dates, or other details that could create the risk being protected.

4.5. Inadmissibility of a completely hidden decisive reason

If confidential material has a decisive or materially significant impact on the outcome, the party against whom it is used must receive a sufficient explanation of its substance to enable them to understand the ground and, where practicable, respond to it. This does not prohibit the CCF from considering confidential material. The restriction applies to situations where an adverse inference depends entirely on a ground whose existence and content the party cannot even generally determine.

4.6. Architecture of a motivated decision

A practical solution is to separate the internal full text and the versions communicated to the parties. This model does not require the CCF to prepare separate substantive decisions; it is a single decision with controlled disclosure versions.

1. Full Confidential Decision - a complete internal version reflecting all materials reviewed, analysis and reasons.
2. Applicant-Specific Reasoned Decision - a version for the applicant in which only information whose disclosure creates an identified risk has been removed.
3. Source-of-Data-Specific Reasoned Decision - a version for a data source with a separate assessment of information that requires protection from disclosure to the source state.

Versions for the parties may be accompanied by a brief Disclosure Schedule. It may indicate the category of the material, the disclosure status, the applicable Article 35(3) basis, a brief explanation of the restriction, and the alternative used—redaction, anonymization, or summary. The Schedule must not describe the suppressed material in such detail as to indirectly disclose protected information.

This approach improves the consistency of application of Article 35, helps the General Secretariat and the parties understand the structure of the decision, and at the same time creates an internal trail that allows the CCF to verify whether less restrictive measures were actually considered.

4.7. Step-by-step procedure for making a decision on disclosure

In the first stage, the Requests Chamber identifies the materials and factual statements that are actually relevant to the subject of the request. Not all information received will necessarily be included in the reasoning: information irrelevant to the outcome may be excluded without applying Article 35, as it does not form the basis of the decision.

In the second stage, the CCF identifies materials for which a restriction has been declared or for which a distinct risk is identified. For each category, the basis under Article 35(3), the potential recipient of disclosure, and the nature of the potential harm are determined. If a single material poses different risks to different parties, the assessments are separated.

In the third stage, less restrictive methods are explored. First, the feasibility of removing specific identifiers or operational details is assessed. Then, partial disclosure, anonymization, and the preparation of a meaningful summary are considered. Complete non-disclosure is chosen only when every realistic alternative poses a significant risk.

In the fourth stage, the full internal draft of the decision is checked for decisive or materially significant undisclosed reasoning. If the undisclosed material affects the outcome, a non-disclosed summary of its substance is prepared. Even if such a summary is impossible, the internal version should explain why further generalization creates an unacceptable risk and what compensating elements can still be communicated.

At the fifth stage, versions for the parties are prepared and a consistency check is conducted. Revisions must not alter the meaning of the conclusions, create the impression of a different evidentiary base, or conceal the fact that a specific category of material was taken into account. The operative part and the underlying legal logic must remain consistent.

4.8. Substantive summary requirements

A quality summary should answer at least four questions. First, what type of information is it: an official document, a source report, investigative data, personal information, or an internal assessment? Second, what factual assertion does the material support or refute? Third, how significant did the CCF consider the material: supporting, corroborating, materially significant, or decisive? Fourth, how did the material influence the application of INTERPOL rules and the final conclusion?

A summary need not indicate the origin of the information if this allows the source to be identified. It may also exclude exact dates, geographic locations, technical methods, document numbers, and personal information. However, eliminating details should not turn the presentation into an empty formula. The phrase "reliable confidential information" alone does not provide insight into the content of the statement or its place in the argument.

4.9. Quality control of adapted versions

Before communicating the decision, it's useful to conduct a separate review of each version. The first review concerns the completeness of the logic: is the connection between the question, the established facts, the applied rules, and the outcome clear? The second review concerns information security: does the combination of the details provided allow for the indirect identification of the source or person? The third review concerns the symmetry of the outcome: do different versions create incompatible explanations for the same decision? The fourth review concerns Article 42: can the addressee determine which facts have already been assessed and what new fact could potentially be relevant?

5. Reasoned decisions and Article 42

Article 42 allows for review of a decision upon the discovery of a fact that could have led the Requests Chamber to a different conclusion had it been known during the initial review. The request must be filed within six months of the discovery of such a fact. To effectively utilize this mechanism, the party must understand the facts and issues that determined the initial decision.

The CCF is not obligated to advise the party on the review strategy and is not required to list potential new evidence. However, the decision must distinguish between a fact already considered and rejected and a potentially new fact that could impact the outcome. Otherwise, the right to review remains formally preserved, but the party cannot meaningfully determine its applicability.

Therefore, it is advisable to clearly identify the determinative issues, the material facts, the rules applied, and a brief legal rationale for the outcome in the communicated version of the decision. If one of these elements is confidential, the most substantive equivalent compatible with protecting the relevant interest should be used.

5.1. The boundary between motivation and consultation about revision

Sufficient reasoning does not require the CCF to anticipate all possible grounds for review. The Commission should not advise a party which documents it needs to obtain, what arguments to formulate, or how to modify its evidentiary strategy. Such a function would be incompatible with neutrality and could create inequality between the parties.

The minimum requirement is different: the decision must clearly indicate what circumstances were the subject of the assessment and what conclusions are based on them. If, for example, the CCF rejects a factual account as unconfirmed, the party must understand what exactly was considered unconfirmed. Then, the subsequent discovery of objectively new material can be compared with the original logic. Without this comparison, the six-month mechanism of Article 42 is difficult to use meaningfully.

The reported version must also distinguish between grounds that independently support the result and those that are valid only in combination. This is important for assessing the materiality of a new fact: refuting a single supporting element might not necessarily change the decision, whereas a new fact affecting a single determinative ground may be of fundamental significance.

6. Protection of sensitive information of the applicant and third parties

Formal equality between the applicant and the data source does not imply identical risks of disclosure. Sharing information with the data source may reveal the applicant's location, family and witness details, international protection information, contacts with third-country authorities, confidential communication channels, or elements of a protection strategy. In certain circumstances, this may create a risk of pressure, intimidation, or persecution.

Therefore, the assessment must be risk-sensitive and party-specific. The same material may be disclosed to the applicant but restricted to the data source, or vice versa. The CCF should consider not only the formal category of information but also the reasonably foreseeable consequences of its disclosure to a specific recipient.

At the same time, protecting the complainant should not automatically exclude information from the source's version of the data. If the withheld information significantly influenced a conclusion unfavorable to the source, anonymization, aggregation, or disclosure of the actual substance without identifying and protective details should be considered.

6.1 Categories of particularly sensitive information

Particularly sensitive information may include addresses and travel details of the applicant, details of family members and close associates, witness contacts, international protection documents, medical information, communications with lawyers and aid organizations, and information received from third-country authorities under confidentiality. The list itself should not be closed: the determining factor is not the category designation, but the reasonably foreseeable consequences of disclosure.

Particular attention should be paid to the mosaic effect—a situation where each individual fragment appears innocuous, but the combination of dates, locations, positions, and circumstances allows one to establish the source's identity or location. Therefore, a risk-sensitive review should evaluate not only individual edits but also the final version of the decision as a whole, in conjunction with information already known to the recipient.

The risk must be sufficiently real and concrete, but not necessarily confirmed by harm already occurring. The protective function of Article 35 is preventive in nature. However, citing the hypothetical possibility of pressure or reprisals without reference to specific information should not automatically preclude disclosure of the actual nature of the material.

6.2. Information provided by the applicant

A requester providing information to the CCF may reasonably expect it to be used to consider the request, but not all information should be automatically disclosed to the data source. The CCF should distinguish between facts necessary for a fair assessment of the source's position and protective or identifying details that do not require disclosure. In some cases, a data source may receive a neutral statement of an allegation without information about who made it or the location of the individual.

If the data source's position is necessary to verify a disputed fact, the CCF can formulate the question at the substantive level without revealing the originator of the information or the application from which it was obtained. This approach preserves the quality of fact-finding while reducing the risk to the applicant and third parties.

6.3. Comparative benchmarks

ARGA does not propose to directly impose binding standards on the CCF, such as national judicial procedures, the ECHR, or European Union law. The CCF is a sui generis independent body of INTERPOL, operates in the area of international police cooperation, and must take into account specific requirements for security, confidentiality, and protection of sources. However, comparative practice confirms the usefulness of several procedural tools.

In ZZ v. Secretary of State for the Home Department, the Court of Justice of the European Union held that full disclosure may be limited by national security interests, but the interested party must in any event be informed of the substance of the reasons in a manner that takes into account the necessary confidentiality. In Regner v. the Czech Republic and Muhammad and Muhammad v. Romania, the European Court of Human Rights assessed not confidentiality in isolation, but rather a combination of compensating safeguards, including independent verification of the need for secrecy and the sufficiency of the information communicated to the affected party.

These approaches are useful not as a source of external obligations for INTERPOL, but as confirmation of a practical idea: the more significant the disclosure limitation, the more important is the specific justification, independent risk assessment and compensatory presentation of the substance of the material.

6.4. Limits of comparative legal analogy

The CCF is not a court, does not adjudicate criminal charges, and is not obligated to replicate national models of closed-material procedures. Therefore, the concepts of equality of arms and adversarial proceedings should not be used as direct legal requirements for INTERPOL. Their usefulness is limited by the functional question: what minimum procedural tools allow the body to make a decision based on classified information while maintaining its clarity and institutional legitimacy.

The proposal also does not propose introducing special advocates, closed hearings, or independent judicial review of confidential materials. Such mechanisms would be disproportionate to the CCF's mandate and resources. The ARGA proposal is deliberately limited to tools that can be integrated into existing written proceedings: individualized justification, redaction, anonymization, gist, party-specific versions, and an internal Disclosure Schedule.

7. Proposed clarifications to Articles 35 and 38

Implementing the proposed model does not require rewriting the Statute. Limited amendments or formal procedural guidance may suffice, providing for the following:

Position	Current norm	Proposed wording	Justification
Article 35(3)	Communication may be restricted for one or more of the listed legitimate grounds.	Any restriction shall be limited to what is necessary and proportionate to address a concrete risk falling within one or more of the listed grounds in this paragraph.	It consolidates individual risk assessment and eliminates automatic complete closure of materials.
Article 35(4)	Restrictions must be justified and must specify whether some information, such as summaries, may be provided.	Before withholding information in full, the Requests Chamber shall consider partial disclosure, redaction, anonymization or a substantive summary. Where undisclosed material is decisive or materially significant, its substance shall be communicated to the party concerned to the maximum extent compatible with the protected interest.	Makes partial disclosure and substantive gist a routine step in the assessment, while maintaining the option of full non-disclosure when there is real risk.

Article 38(2)	Decisions shall be reasoned and contain a summary of proceedings, submissions, facts, application of INTERPOL's rules, legal analysis and operative parts.	A reasoned decision shall identify the determinative issues, material facts, applicable rules and legal reasoning in sufficient detail for each party to understand the basis and effect of the decision.	Specifies the minimum content of the justification without the obligation to disclose the protected details.
Article 38(3)	Decisions are provided to the applicant and the source of data subject to confidentiality requirements and restrictions.	The Commission may provide party-specific versions of the same decision. Any restriction shall be assessed separately for the applicant and the source of data, taking account of risks to either party and to third parties.	Allows for consideration of risk differences and protection of the applicant, the data source, and third parties without losing the logic of the decision.

A preferred first step might be to adopt a practical guide or standard internal template. This will allow the model to be tested without excessive regulatory detail and to assess its impact on Requests Chamber's workload.

7.1 Feasibility and Limitations

The proposed model should remain proportionate to CCF resources. Separate line-by-line evaluation of each document is not required if the materials form a homogeneous category and the same criteria apply to them. The Disclosure Schedule can be short, and adapted versions of the decision can be created from a single full text using standardized redaction categories.

The model also should not create indirect disclosures. In cases where even a description of the material category can identify the source, method, or person, the CCF may use a more general level of formulation. However, the degree of generality should be determined by the specific risk and not applied automatically.

Finally, the lack of sufficient justification for a request for confidentiality should not automatically lead to disclosure if the CCF independently determines a real risk. In such cases, the Commission retains the ability to restrict disclosure on its own initiative, but must record its own assessment of the justification, necessity, and available alternatives.

8. Conclusions and recommendations

1. To establish the principle of maximum meaningful disclosure compatible with legitimate confidentiality as the basis for the joint application of Articles 35 and 38.
2. Require an individualized determination of the basis, specific risk, necessity and proportionality of each significant restriction.
3. Consider redaction, anonymization and substantive gist until complete disclosure.
4. Provide a party with a reasonable understanding of any underlying cause that has a decisive or materially significant effect on the outcome.
5. Use the full internal version and adapted party-specific versions of the reasoned decision.
6. Consider separately the risks of disclosure to the applicant, the data source and third parties.
7. Provide a degree of reasoning that allows for a practical assessment of the applicability of Article 42 without turning the CCF into an advisor to the parties.

Conclusion

Confidentiality is a prerequisite for the effective operation of the CCF and international police cooperation. However, its protective function does not require a complete renunciation of substantive justification. Articles 35 and 38 can be harmonized through a consistent model that limits specific information, rather than the ability to understand the decision itself.

The proposed approach preserves the independence of the CCF, protects the legitimate interests of applicants, data sources, and third parties, and simultaneously enhances the predictability and practical value of Requests Chamber decisions. Its key outcome is not the maximum volume of disclosed data, but the maximum amount of clear and useful justification that can be provided without creating the identified defensible risk.

Appendix 1. Detailed versions of point corrections

Below are draft amendments intended for internal consultation. They do not involve revising the architecture of the Statute and could be implemented either directly in Articles 35 and 38, or, more cautiously, through the Operating Rules or a practical guide for the Requests Chamber.

1.1 Article 35(3): specific risk, necessity and proportionality

Working wording: Any restriction on the communication of information shall be limited to what is necessary and proportionate to address a concrete and reasonably foreseeable risk falling within one or more of the grounds listed in this paragraph.

The purpose of the change is not to raise the threshold of protection to the level of proven harm, but to eliminate abstract and categorical restrictions. The data source or other party requesting confidentiality must define the protected interest, the category of information, the nature of the risk, and the causal link between disclosure and potential harm. The CCF retains the ability to restrict disclosure on its own initiative if the risk is evident from the case file.

A possible objection is that specifying the risk itself can reveal sensitive information. The answer is a flexible level of detail: the rationale can be set out at a more general level if further specification creates the very risk that needs to be protected. However, such generalization must also be explained individually.

1.2. Article 35(4): sequence of less restrictive measures

Working wording: Before withholding information in full, the Requests Chamber shall consider whether the protected interest can be adequately safeguarded by partial disclosure, redaction, anonymization or the communication of a substantive summary.

The proposed clarification transforms the existing summary option in Article 35(4) into a sequential decision-making process. It does not create an absolute obligation to disclose part of each document. If no less restrictive method eliminates the risk, complete non-disclosure remains permissible. The CCF must merely demonstrate in its internal decision that alternatives have been considered.

For homogeneous data sets, assessment can be performed by category rather than line by line. This reduces administrative burden and allows for a unified approach to operational data, third-party information, investigation data, or internal organizational materials.

1.3. Article 35(4): substantive gist of the decisive material

Working formulation: Where undisclosed information is decisive or materially significant to the outcome, the substance of that information and its role in the reasoning shall be communicated to the party concerned to the maximum extent compatible with the interest protected under paragraph 3.

The term "materially significant" is broader than "strictly decisive" and encompasses material that is not the sole basis for a decision but significantly influences the assessment of the facts or the applicability of INTERPOL rules. This term refers not to the document itself or the protected detail, but to the greatest possible extent to which the factual assertion is relevant and its role in the CCF's conclusion.

The final part of the formula serves as a safeguard against indirect disclosure. Even if a general gist can identify a source, method, person, or line of investigation, the CCF has the right to increase the level of generalization. In exceptional cases, full disclosure of the substance may be impossible; such a decision must be subject to separate internal justification.

1.4 Article 38(2): minimum structure of reasons

Working formulation: A reasoned decision shall identify, in sufficient detail for the parties to understand its basis and effect, the determinative issues, the material facts accepted by the Requests Chamber, the applicable INTERPOL rules, the principal submissions considered and the legal reasoning supporting the operative part.

The amendment does not require a response to every argument and does not transform the CCF decision into a judicial act of the national court. It clarifies the minimum functional requirements: the party must understand what was decided, what facts were accepted, what rules were applied, why the main arguments were accepted or rejected, and how the analysis relates to the operative part.

1.5. Article 38(3): Versions of the decision for specific parties

Working wording: The Commission may communicate appropriately redacted party-specific versions of the same reasoned decision. Restrictions shall be assessed separately in relation to the applicant and the source of data, taking account of the rights and legitimate interests of either party and of third persons.

We are talking about a single decision, not two different sets of reasons. The full version ensures the internal consistency of the analysis. The versions for the applicant and the data source differ only in the scope of disclosure. Any revision must retain the same operative part and not distort the factual or legal logic of the full decision.

Appendix 2. Disclosure Schedule Model

A Disclosure Schedule may be a brief appendix to the communicated version of the decision or an internal control document. Its purpose is to document the consistent application of Article 35 without disclosing protected information or creating a separate subject of dispute.

Material category	Status	Basis Article 35(3)	Reason for restriction	Alternative disclosure
Operational information on the progress of the investigation	Partially disclosed	35(3)(a)–(b)	Disclosure of specific actions could impact the ongoing investigation.	General factual gist without dates, methods, and identifiers
Data of the applicant and third parties	Limited for source of data	35(3)(c)	Reasonably foreseeable risk to privacy, safety or secure communications	Anonymized description of a fact and its meaning
Source Information	Not disclosed	35(3)(a)–(d)	Even a description can help identify the source.	General indication of category and evidentiary weight
Legal Analysis by Requests Chamber	Revealed	Not applicable	The analysis itself does not create an established risk	A full explanation of the rules and logic used

In the actual document, categories may be combined. The reason for the restriction must be sufficiently specific to allow internal control, but must not reveal the content of the concealed material. The schedule does not replace a reasoned decision: it only explains the disclosure architecture.

2.1. Requests Chamber Security Questions

1. Is a specific category of information defined, rather than the entire document, based on a formal criterion?
2. Is the applicable Article 35(3) ground and reasonably foreseeable risk stated?
3. Have redaction, anonymisation, partial disclosure and substantive summary been checked?
4. Does the communicated version maintain a clear connection between facts, rules, and outcome?
5. Doesn't the very wording of Schedule create an indirect disclosure of source, method or identity?
6. Has a separate assessment been conducted for the applicant, the source of data, and third parties?
7. Does the decision allow us to understand the determinative issues for the purposes of a possible revision under Article 42?

Appendix 3. Adversarial stress test of the proposed model

Perspective	The main objection	Risk	Minimal adjustment
General Secretariat	The model will increase the volume of decision-making and administrative burden	Requests Chamber slowdown	Categorical rather than line-by-line assessment; standard templates; pilot procedural guidance
Data source / NCB	Even a GIST can reveal the operational direction, source, or gaps in an investigation.	Damage to crime prevention and international cooperation	Flexible level of generalization; separate assessment of indirect disclosure; complete non-disclosure in exceptional cases
Data protection specialist	Versions for the parties may be inconsistent and disclose redundant third-party data	Violation of the rights and freedoms of the applicant or third parties	Party-specific assessment; data minimization; anonymization; internal editorial log
Applicant representative	Too general a summary does not allow one to understand and challenge the decisive grounds	Formal but ineffective motivation and revision	Mandatory indication of the nature of the fact, its evidentiary weight and impact on the outcome
CCF institutional independence	A rigid disclosure ladder may be perceived as an external constraint on the CCF's discretion	Excessive normative formalization	Retain the "shall consider" formula and explicitly establish the CCF's authority to determine the required scope of disclosure

The stress test shows that the core idea is preserved only by refusing automaticity in both directions. Neither confidentiality nor disclosure should be applied categorically. The CCF should retain the right to completely seal material if a risk is identified, but simultaneously document why less restrictive methods do not provide sufficient protection.

Appendix 4. Article-by-Article Analysis of Operating Rules 2026 and RPD

This section tests the proposed model not only against the CCF Statute but also against the current Operating Rules and the Rules on the Processing of Data. These documents regulate different levels of confidentiality. The Operating Rules govern the Commission's internal work and the communication of its findings; the RPDs regulate the confidentiality and access to data within the INTERPOL Information System. They cannot be mixed, but they must be applied consistently.

4.1. Operating Rules: Internal Confidentiality of the Commission

Rule 13(1)–(3) establishes that the Commission's work and files are confidential, materials and reports are for internal use only unless the Commission expressly decides otherwise, and that members of the Commission and the Secretariat are required to maintain the confidentiality of all documents and information received. Rule 13(4) links this general obligation to the more specific regime of Rule 29.

Rule 29(1) reiterates the confidential nature of the Commission's information, work, and files and requires appropriate measures to protect the request itself and all materials comprising it. These rules explain why the full internal version of the decision and the internal Disclosure Schedule may remain confidential. At the same time, they do not require that the version communicated to the parties be unsubstantiated: the regime of internal secrecy coexists with the Statute's requirement for a reasoned decision.

4.2. Operating Rules: Reasoned Conclusions and Notification of Parties

Rule 31(3) requires that the applicant be informed of the reason for declaring a request inadmissible. Even at the preliminary stage, the Operating Rules assume that an unfavorable procedural outcome must be accompanied by a clear explanation.

Rule 32(3) provides for notice and an opportunity to respond before measures are taken in connection with alleged misconduct, where appropriate and subject to confidentiality requirements and restrictions. Rule 32(4) additionally requires the reasoning behind the decision to take such measures to be communicated. These provisions confirm that confidentiality in the current system is already viewed as a limitation on the scope of communication, not as a waiver of the obligation to explain the decision.

Rule 33(1) requires the General Secretariat and the applicant to provide reasoned opinions, taking into account confidentiality requirements. A practical gap is that the Operating Rules do not define the minimum substantive content of the stated reasons, do not establish a redaction-before-withholding procedure, and do not provide for a separate assessment of the version of the source data. The proposed model fills this gap without changing the confidentiality principle of Rules 13 and 29.

4.3. Operating Rules: revision

Rule 30(7) requires that a request for revision state the fact discovered, explain why it might have led the Requests Chamber to a different conclusion, and be filed within six months of the discovery. Rule 30(8) requires a clear statement of all relevant elements and specific references to annexes. These requirements cannot be meaningfully met if the original decision does not indicate which facts and issues were determinative. Therefore, the link between Article 38 and Article 42 is confirmed by the procedural structure of the Operating Rules themselves.

4.4. RPD Article 14: Risk-Based Privacy

RPD Article 14(1) directly links the confidentiality of data to the risks of its disclosure for the individuals being cooperated with, sources, and the Organization. This is an important systemic argument in favor of risk-sensitive and party-specific analysis: INTERPOL's current system already defines confidentiality based on the consequences of disclosure, not just the formal category of the document.

Under Article 14(2) of the NCB, national and international entities assign confidentiality levels to input data and are obligated to respect them when using it. Article 14(3) obligates the General Secretariat to ensure processing complies with the assigned level. These powers apply to processing in the INTERPOL Information System; they should not automatically prejudge the scope of the CCF's justification. The Requests Chamber nevertheless applies its own Article 35 test after consultation with the owner of the information.

4.5. RPD Articles 7, 58 and 59: Source Control and Access Restrictions

RPD Article 7 establishes sources' control over the processing of the data they input. Article 58 allows NCBs and international entities to impose general and additional access restrictions, with the restrictions themselves being confidential data. Article 59 permits the disclosure of restricted data only in specified, urgent situations.

These standards protect police-to-police access within the information system and the trust of sources. However, access restrictions under RPD are not the same as communication restrictions under CCFs. If these regimes were automatically equated, the data source would effectively determine the content of the independent oversight body's decision. A consistent interpretation should preserve the source's control over the original data, but allow CCFs to communicate secure substantive information that does not reveal the restricted data itself.

4.6. RPD Articles 112–114: Confidentiality Levels and Technical Protection

Articles 112–114 establish a regime of classification and technical measures. Article 112 permits changes to the confidentiality level, including a reduction if the data requires less protection. Article 113 allows the General Secretariat to increase the level with the consent of the source if there is a risk to police cooperation, the Organization, personnel, or Member States. Article 114 requires appropriate administrative and technical procedures.

These provisions support two ideas. First, confidentiality is not an immutable binary status: the level of protection depends on the risk and can be adjusted. Second, the technical classification does not answer the question of what part of the legal logic must be disclosed to the parties. Therefore, the draft amendments to Articles 35 and 38 do not weaken the RPD regime; they create a separate procedural method for preparing reasoned decisions without unauthorized disclosure of the original data.

4.7. RPD Article 42: Particularly sensitive data

Article 42 of the RPD permits the processing of particularly sensitive data only if it is particularly relevant and has significant forensic value, requires an objective description free of evaluative or discriminatory comments, and prohibits discriminatory use. For the CCF, this means the need for increased caution when disclosing biometric, medical, and other sensitive information. However, this enhanced protection of this data category does not preclude the possibility of providing a legally neutral description of its role in the decision.

4.8. Summary of the article-by-article analysis

The Operating Rules and RPD do not refute the ARGA model. On the contrary, they already incorporate its key premises: risk-based confidentiality, the obligation to explain individual decisions, the ability to adapt the level of protection, and the independent role of the CCF. What is needed is a clearer distinction between the protection of original data and the obligation to communicate the secure nature of the rationale.

Appendix 5. Extended International Comparative Analysis

Comparative materials are used solely for persuasive guidance. They do not transform the CCF into a court of law or make the norms of the relevant systems directly applicable to INTERPOL. Their value lies in identifying recurring technical solutions: independent assessment of the need for secrecy, disclosure of the substance of the grounds, redaction, summaries, restriction of access to source materials, and compensatory guarantees.

5.1. CJEU: ZZ and Kadi II

In ZZ v Secretary of State for the Home Department, C-300/11, para. 65, the CJEU stated that the interested party must be informed of the essence of the grounds of the decision, even when full disclosure of evidence is restricted by national security interests. For the CCF, the distinction between protected evidence and the essence of grounds is not an absolute formula, but rather a useful one.

In the joined cases of Kadi II, C-584/10 P, C-593/10 P, and C-595/10 P, paras. 114–129, the CJEU linked the sufficiency of reasons to the ability to verify the factual basis of the restrictive measure and provided for judicial review of confidential materials. For INTERPOL, a more specific approach is relevant: if the full materials are not disclosed, the public version must contain sufficiently specific reasons so that the result does not rely on an incomprehensible assertion.

5.2. ECtHR: Jasper, A. and Others, Regner and Muhammad

In Jasper v United Kingdom [GC], paras. 51–53, the ECtHR recognized that some material may be withheld from disclosure to protect a significant public interest, but that restrictions must be strictly necessary and offset by procedures allowing the body to independently assess the need for non-disclosure. In A. and Others v United Kingdom [GC], paras. 205–220, the Court paid particular attention to whether the information available was sufficient to effectively respond to the underlying allegations.

In Regner v. Czech Republic [GC], paras. 146–149, the Court considered classified materials in the context of a set of safeguards, including access by an independent tribunal to all materials and its power to review the need for secrecy. In Muhammad and Muhammad v. Romania [GC], paras. 125–157, the Court codified the importance of information on the factual basis and compensating safeguards when restricting access to classified materials.

For the CCF, these cases do not create an obligation to institute legal proceedings. They confirm the principle of proportionality: the less information a party receives, the more important an independent risk assessment becomes, and the more substantive the compensatory explanations must be.

5.3. Human Rights Committee

The Human Rights Committee, in General Comment No. 32, para. 13, links equality of arms to each party's reasonable opportunity to respond to the other's arguments and evidence. Since the CCF is not a court or tribunal within the meaning of Article 14 of the ICCPR, this standard is not directly applicable. However, it confirms the functional idea that participation becomes formal if a party is unaware of the substance of the assertion used against them.

In certain national security reviews, the Committee also emphasized the need to provide sufficiently specific information about the allegations or grounds to enable the individual to explain or challenge them. For the CCF, this material is relevant only by analogy and given its more limited oversight mandate.

5.4. UN Security Council Ombudsperson

The 1267 Committee's Ombudsperson mechanism demonstrates how a non-judicial international mechanism handles highly sensitive information. The Ombudsperson collects information from the applicant, states, and organizations, preparing a comprehensive report with key arguments and recommendations, while the Committee publishes narrative summaries of the reasons for designating individuals and organizations. The full confidential file is not made publicly available.

This mechanism is particularly useful as a structural analogy: the independent expert has access to more extensive material than the applicant, but the procedure still strives to convey a clear essence of the reasons. For CCF, a similar tool could be the Full Confidential Decision and party-specific reasoned versions.

5.5. International Criminal Court

Rome Statute Article 67(2) and the Rules of Procedure and Evidence, in particular Rule 81, permit disclosure restrictions to protect witnesses, ongoing investigations, the internal workings of the parties, and information obtained in confidence. The Trial Chamber oversees exceptions, may order summaries or other measures, and must take into account the rights of the affected party.

ICC proceedings are fundamentally different from CCF proceedings, so criminal defense standards are not directly applicable. The ladder of measures itself is useful: protecting a source or witness does not always require complete exclusion of content; redaction, delayed disclosure, summaries, and other forms determined by an independent body are also possible.

5.6. General comparative conclusion

All the systems examined share the same institutional principle: the decision-making body may have more complete access to the materials than the party, but it must independently assess the necessity of restrictions and maintain the broadest possible understanding of the grounds. The intensity of guarantees and legal bindingness vary, but the technical set of solutions is consistent with the ARGA model.

Appendix 6. Sources & Verification Table

All sources below are primary official materials. The verification date for this version is the same: August 22, 2026.

Legal statement	Source	Article / paragraph	Official URL	Date	Status
Information is available to parties upon request with restrictions	CCF Statute	Art. 35(1)	interpol.int/content/download/5695/	August 22, 2026	Direct rule
The owner of the information is consulted before disclosure.	CCF Statute	Art. 35(2)	interpol.int/content/download/5695/	August 22, 2026	Direct rule
Four grounds for limitation	CCF Statute	Art. 35(3)(a)–(d)	interpol.int/content/download/5695/	August 22, 2026	Direct rule
The restriction is justified; partial information/summary is considered	CCF Statute	Art. 35(4)	interpol.int/content/download/5695/	August 22, 2026	Direct rule
The decision is written and reasoned.	CCF Statute	Art. 38(2)	interpol.int/content/download/5695/	August 22, 2026	Direct rule
The decision is communicated to the applicant and the source of the data, taking into account confidentiality.	CCF Statute	Art. 38(3); 41(3)	interpol.int/content/download/5695/	August 22, 2026	Direct rule
Revision is based on new facts and a six-month period	CCF Statute	Art. 42(1)–(2)	interpol.int/content/download/5695/	August 22, 2026	Direct rule

The work and files of the Commission are confidential.	Operating Rules 2026	Rules 13, 29	interpol.int/content/download/24270/	August 22, 2026	Direct rule
The reason for inadmissibility is reported by the applicant.	Operating Rules 2026	Rule 31(3)	interpol.int/content/download/24270/	August 22, 2026	Direct rule
Reasoning is reported in misconduct measures	Operating Rules 2026	Rule 32(3)–(4)	interpol.int/content/download/24270/	August 22, 2026	Direct rule
Reasoned conclusions are provided with due regard to confidentiality.	Operating Rules 2026	Rule 33(1)	interpol.int/content/download/24270/	August 22, 2026	Direct rule
Revision must explain the materiality of the new fact	Operating Rules 2026	Rule 30(7)–(8)	interpol.int/content/download/24270/	August 22, 2026	Direct rule
Confidentiality is determined by the risk of disclosure	RPD 2025	Art. 14(1)	interpol.int/content/download/5694/	August 22, 2026	Direct rule
Source assigns a privacy level	RPD 2025	Art. 14(2)–(3)	interpol.int/content/download/5694/	August 22, 2026	Direct rule
Source retains control over data processing	RPD 2025	Art. 7	interpol.int/content/download/5694/	August 22, 2026	Direct rule
Access restrictions and their confidentiality	RPD 2025	Arts. 58–59	interpol.int/content/download/5694/	August 22, 2026	Direct rule
Classification and protection measures	RPD 2025	Arts. 112–114	interpol.int/content/download/5694/	August 22, 2026	Direct rule
Particularly sensitive data	RPD 2025	Art. 42	interpol.int/content/download/5694/	August 22, 2026	Direct rule
The essence of the grounds for protecting security	CJEU, ZZ, C-300/11	Para. 65	curia.europa.eu, EU:C:2013:363	August 22, 2026	Comparative
Checking the factual basis of the reasons	CJEU, Kadi II	Paras. 114–129	curia.europa.eu, EU:C:2013:518	August 22, 2026	Comparative
Strict non-disclosure requirement	ECtHR, Jasper v UK [GC]	Paras. 51–53	hudoc.echr.coe.int, 27052/95	August 22, 2026	Comparative
Open information should allow for an answer	ECtHR, A. and Others v UK [GC]	Paras. 205–220	hudoc.echr.coe.int, 3455/05	August 22, 2026	Comparative
Compensatory guarantees for closed materials	ECtHR, Regner v Czech Republic [GC]	Paras. 146–149	hudoc.echr.coe.int, 35289/11	August 22, 2026	Comparative
Information on the factual basis	ECtHR, Muhammad and Muhammad v Romania [GC]	Paras. 125–157	hudoc.echr.coe.int, 80982/12	August 22, 2026	Comparative
Equality of arms and the ability to respond	HRC General Comment No. 32	Para. 13	ohchr.org, CCPR/C/GC/32	August 22, 2026	Comparative
Narrative summary and independent Ombudsperson	UNSC 1267 mechanism	Res. 2734 (2024); mandate	main.un.org/securitycouncil/en/ombudsperson	August 22, 2026	Comparative
Restrictions on disclosure and protective measures	ICC Rules of Procedure and Evidence	Rule 81	icc-cpi.int/RulesProcedureEvidenceEng.pdf	August 22, 2026	Comparative
Duty to disclose with exceptions provided	Rome Statute	Art. 67(2)	icc-cpi.int/Rome-Statute-eng.pdf	August 22, 2026	Comparative

Main primary sources

1. INTERPOL, Fourth Call for Contributions from Civil Society to the CPD (20 July 2026)
2. Statute of the Commission for the Control of INTERPOL's Files, current text (Articles 35, 38, 42)
3. Operating Rules of the CCF, amendments adopted 26 March 2026
4. INTERPOL Constitution, Article 3
5. INTERPOL's Rules on the Processing of Data, current 2025 text
6. CJEU, ZZ v Secretary of State for the Home Department, C-300/11, 4 June 2013
7. CJEU, Commission and Others v Kadi, Joined Cases C-584/10 P, C-593/10 P and C-595/10 P
8. ECtHR, Jasper v. the United Kingdom [GC], no. 27052/95, 16 February 2000
9. ECtHR, A. and Others v. the United Kingdom [GC], no. 3455/05, 19 February 2009
10. ECtHR, Regner v. the Czech Republic [GC], no. 35289/11, 19 September 2017
11. ECtHR, Muhammad and Muhammad v. Romania [GC], no. 80982/12, 15 October 2020
12. UN Human Rights Committee, General Comment No. 32, CCPR/C/GC/32
13. UN Security Council, Office of the Ombudsperson to the ISIL (Da'esh) and Al-Qaida Sanctions Committee
14. International Criminal Court, Rules of Procedure and Evidence

15.Rome Statute of the International Criminal Court