INTERPOL

BACKGROUND NOTE

ON INTERPOL'S INFORMATION SYSTEM SAFEGUARDS FOR THE PROCESSING OF PERSONAL DATA

OVERVIEW

The following document is meant to serve as an authoritative description of certain key INTERPOL rules, procedures, and mechanisms in relation to the protection of personal data in the course of police cooperation and data exchange among and between INTERPOL members as well as with selected partners such as other international organizations.

The first section of the document sets forth, at a very general level, an overview of the organization's establishment as well as a brief description of the INTERPOL Information System. It then goes on in greater detail to explain the INTERPOL Red Notices System. This sub-section notes, inter alia, the requirements for publication of Red Notices, the pre-publication review of each individual Notice, and circumstances under which Red Notices are removed.

The second section provides an in-depth summary of the legal framework underpinning INTERPOL's practices with respect to the protection of individuals' personal data and privacy. This section describes INTERPOL's long-standing experience in data processing and protection. It explains in the context of INTERPOL's Constitution and Rules on the Processing of Data how the Organization addresses key principles and tenets of data protection such as: lawfulness; purpose specification and limitation; data quality; transparency; data confidentiality and security; and independent oversight and individual redress (rights of individual access, correction, and deletion) including rules regarding data retention, access, and transfers. It goes on to provide a detailed summary of the role, independence, and supervisory and oversight authorities of the Commission for the Control of INTERPOL's Files (CCF), which ensure that this independent body can provide an effective remedy to individuals.

This document does not serve as a fully comprehensive account of INTERPOL data protection mechanisms, nor does it supplant or otherwise qualify the actual rules and procedures that govern such cooperation (and to which this document frequently cites and refers). Rather, the aim is to summarize and contextualize some of the most salient aspects of INTERPOL's sophisticated data management and data protection regime. Appendices to this document provide key primary materials, such as INTERPOL's Constitution and Rules on the Processing of Data (RPD), for ease of reference.

INTRODUCTION

This document sets forth a broad overview of INTERPOL's status and operations as an international organization constituted to facilitate international police and law enforcement cooperation, with a particular emphasis on its Red Notices System and internal regulations and practices regarding the processing and protection of personal data. Section 1 outlines the organization generally and its Information System and Red Notices System. Section 2 describes the legal, regulatory, and operational structures with respect to data protection and privacy that underpin the organization's and member countries' use of these systems. The binding legal mechanisms described in this paper serve as linchpins in INTERPOL's longstanding commitment to effective and secure data management and protection, including – in particular – with respect to personal data.

SECTION 1:
GENERAL OVERVIEW OF INTERPOL AND ITS INFORMATION AND RED NOTICES SYSTEMS

I. INTERPOL – GENERAL OVERVIEW

The International Criminal Police Organization - INTERPOL [hereinafter "INTERPOL"] is an international organization constituted under public international law.

Since its creation in 1923, INTERPOL has worked to facilitate international police cooperation. This mandate is enshrined in Article 2 of INTERPOL's Constitution adopted in 1956, as follows:

1) To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the "Universal Declaration of Human Rights;"

2) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes."

INTERPOL's seat is in Lyon, France. The Organization has 194 member countries, each of which appoints a National Central Bureau (NCB). NCBs serve as the country's point of contact for INTERPOL-related matters and to act as liaisons between the various departments in the country and the Organization's General Secretariat as well as NCBs in other countries (Art. 32, Constitution).

INTERPOL's activities and its members' use of its information system are governed by INTERPOL's Constitution and rules, notably its RPD, as will be further elaborated below.

II. THE INTERPOL INFORMATION SYSTEM

By providing its member countries with access to its communication system, INTERPOL serves as the only organization to facilitate structured cooperation on police matters around the globe. This structured and regulated exchange of police information indeed lies at the core of the Organization's mandate, as among INTERPOL's strategic goals is to serve as an information hub to facilitate effective law enforcement cooperation.

The importance of and benefits in using INTERPOL's communication network and databases have been recognized in international and regional conventions[1] as well as in a significant number of resolutions adopted by the United Nations Security Council and General Assembly, including those in relation to combating terrorism and transnational organized crime[2].

III. THE INTERPOL RED NOTICES SYSTEM

Among the most important tools available to INTERPOL's members is its Red Notices System. A Red Notice is a request to locate and provisionally arrest an individual pending extradition. A member country may, based on a valid national arrest warrant, request that INTERPOL's General Secretariat issue a Red Notice. Red notices may also be issued upon the request of entities such as international tribunals.

As noted, a Red Notice is based on national arrest warrants issued in accordance with the national laws of the requesting country. A Red Notice is not an international arrest warrant. It is entirely up to each country to decide whether to request the issuance of Red Notices. INTERPOL does not have the authority to issue warrants or Red Notices upon its own initiative.

The issuance of a Red Notice, moreover, does not require any other INTERPOL member country to take any action whatsoever regarding the notice or the individual in question. Whether to act on Red Notices issued upon the request of other countries is at each member's discretion according to its own domestic law.

All Red Notice requests must of course meet the requirements prescribed by the national legislation of the requesting country and any relevant conventions to which the requesting country is a party. Crucially, all requests must also meet the requirements set forth in INTERPOL's Constitution and rules, most notably INTERPOL's RPD.

For example, for a Red Notice to be issued, a request must concern a serious ordinary law crime[3]. It must meet a penalty threshold[4]. It must contain sufficient identifiers and descriptions of the criminal act at issue[5]. A request may not be of a political, military,

1 For example: 1) the possible use of INTERPOL's channels to transmit European Arrest Warrants; 2) the possible use of INTERPOL's channels to exchange request for Mutual Legal Assistance is mentioned in UNTOC and UNCAC; and 3) the recent Council of Europe Convention on Offences relating to Cultural Property ('Nicosia Convention', 2017) calls upon State Parties to contribute to the Interpol database on stolen works of art.

2 For example: 1) UNSC Resolution 2462 (2019) encourages UN Member States to make best use of INTERPOL policing capabilities, such as relevant databases and analytical files, in order to prevent and counter the financing of terrorism; and 2) UN General Assembly Resolution 71/19, which recognized and called for greater cooperation with INTERPOL, particularly in the fields of counter-terrorism, transnational crime, cybercrime, corruption and financial crime, and environmental crimes. For further information on key UN Resolutions related to INTERPOL see INTERPOL's public website at https://www.interpol.int/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations/UNGA-and-UNSC-resolutions-highlighting-INTERPOL-s-role.

3 Art. 83, RPD.

4 Art. 83, RPD.

5 Art. 83, RPD.

religious, or racial character, or regard political offenses such as treason or espionage[6]. Requests must comply with internationally recognized human rights standards as reflected by the "spirit of the Universal Declaration of Human Rights" (Art. 2(1), Constitution). For example, in accordance with INTERPOL's refugee policy, a Red Notice may not be published if the individual's status as a refugee has been confirmed.

To ensure compliance with INTERPOL's rules, and to prevent misuse of the system, each request for issuance of a Red Notice is subject to independent, individualized review by the General Secretariat prior to the Notice's publication and circulation to INTERPOL member countries (Art. 86, RPD). To that end, a dedicated multidisciplinary task force conducts a robust quality and legal compliance review.

The Red Notices System has facilitated numerous cases of successful arrests and extradition of serious offenders across INTERPOL's membership[7].

Once published, Red Notices may be deleted in one of the following ways:

- The NCB that requested the publication withdraws the Red Notice.
- The General Secretariat concludes that the Red Notice may no longer be maintained. This can be done based on various grounds[8], including if the Red Notice no longer meets INTERPOL's rules or conditions for publication.
- The Commission for the Control of INTERPOL's Files (CCF), an independent supervisory body, concludes that the Red Notice does not comply with INTERPOL's rules. As will be explained below, such a decision is final and binding on the Organization and the General Secretariat promptly implements it[9].
- Following a settlement of disputes procedure: Under INTERPOL's rules, a country may protest in relation to a Red Notice issued upon the request of another country. If such a dispute cannot be resolved through consultations, the matter will be submitted to INTERPOL's Executive Committee to decide whether the Notice should be maintained[10].

Red Notices are regularly updated based on information made available to the General Secretariat from the requesting NCB or another source.

One relatively straightforward example may arise if a country communicates that a request for extradition concerning the subject of a Red Notices was denied. In such an instance, this update is added to the file of the individual and is visible to all member countries.

A similar, if potentially more complex example, can be found in INTERPOL's practice to add such a notification to an individual's file when a non bis in idem/double jeopardy concern has been raised. Here, INTERPOL begins from the requirement under Article 2(1) of its Constitution to act in the spirit of the "Universal Declaration of Human Rights," and therefore in accordance with Article 14(7) of the International Covenant on Civil and Political Rights (ICCPR) which provides that "no one shall be liable to be tried or punished again for

6 Art. 3, Constitution; Art. 5 and 34, RPD.

7 Some examples of successful arrests based on red notices have been reported on INTERPOL's public website. See, for example, the following links: 1) https://www.interpol.int/News-and-Events/News/2019/Finnish-fugitive-arrested-in-Albania-with-INTERPOL-support; 2) https://www.interpol.int/News-and-Events/News/2018/INTERPOL-facial-recognition-nets-most-wanted-murder-fugitive; and 3) https://www.interpol.int/News-and-Events/News/2018/INTERPOL-fugitive-probe-nets-most-wanted-suspect.

8 For the full list of grounds for deletion of a Red Notice see Art. 81 of the RPD.

9 Statistics on CCF cases are published every year as part of the CCF annual report, available on INTERPOL's public website.

10 For the settlement of disputes procedure see Art. 135 of the RPD. In exceptional cases, the Executive Committee may decide to submit the dispute to the General Assembly. See INTERPOL's General Assembly Resolution GA-2017-86-RES-05.

an offence for which he has already been finally convicted or acquitted in accordance with the law and penal procedure of each country[11]."

Accordingly, to respect the laws of 194 member countries and their various bilateral/multilateral instruments and treaties, INTERPOL implemented the following practice to comply with the requirements derived from its Constitution. Generally, when a member country asserts that the principle of non bis in idem applies to a Red Notice published in INTERPOL's Information System upon the request of another country, the General Secretariat requests additional information from both countries to make a preliminary assessment of the compliance of the data. Following receipt and review of this information, if the source of data (the country requesting the Notice) asserts that the principle does not apply, opposes deletion of the Notice on this basis, and confirms the individual is still wanted, the General Secretariat will add a caveat to the Notice reflecting the position of the member country asserting that the non bis in idem principle does apply. The caveat serves to alert all member countries that there may be cause to examine application of non bis in idem in light of applicable national laws and international agreements. This practice also preserves INTERPOL's principle of neutrality[12].

SECTION 2:
INTERPOL'S LEGAL FRAMEWORK AND DATA PROTECTION STANDARDS GOVERNING THE USE OF THE INTERPOL INFORMATION SYSTEM AND ISSUANCE OF RED NOTICES

1. INTERPOL'S LONGSTANDING EXPERTISE IN DATA PROTECTION

Data protection is fundamental to INTERPOL's mission and activities, and its centrality in the organization's operations reflects INTERPOL's commitment to privacy, good governance, and accountability. As INTERPOL facilitates cooperation and communication amongst international law enforcement in a trusted environment, it is essential that the information exchanged is in line with evolving data protection standards.

The importance of privacy in INTERPOL operations was formally recognized as early as 1974, when INTERPOL's General Assembly adopted a Resolution entitled "Privacy of Information" (AGN/43/RES1), which urged NCBs and the General Secretariat to take into account the privacy of the individual when exchanging criminal justice information.

Furthering these commitments, INTERPOL created an independent data protection authority in 1982, shortly after the conclusion of Convention 108 of the Council of Europe[13], the first ever binding international convention on data protection. The mandate of this body – known today as the CCF – was enshrined in INTERPOL's Constitution in 2008 and is set forth in greater detail below.

In 1984, INTERPOL's first rules on data protection, the Rules on International Police Cooperation and on the Internal Control of INTERPOL's Archives, came into force.

11 OHCHR Fact Sheet No. 30: The UN Human Rights Treaty System, 3, 6-7. The ICCPR has been ratified by 172 member states.

12 Implementation of the principle of non bis in idem is typically carried out through operation of extradition treaties between INTERPOL members and is traditionally recognized in relation to the requested State, i.e., the extradition will be opposed if the individual concerned has already been acquitted or finally convicted of the same offence(s) by the requested State. In addition, the rule has no single, universally agreed upon application in practice, its interpretation varies among legal systems, and it is not broadly applied with respect to violations of penal laws of multiple sovereigns. INTERPOL's notification practice with respect to non bis in idem therefore facilitates the principle's application in accordance with applicable extradition treaties and the domestic laws of its members.

13 Convention 108 of the Council of Europe of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

To provide safeguards in a fast-paced globalized and digitized world and in line with evolving international data protection standards, INTERPOL regularly assesses[14] and updates its rules on data protection – on average – about every three years. As will be further discussed below, the current set of rules came into force in July 2012 and since then has been subject to a number of substantive amendments.

2. APPROPRIATE SAFEGUARDS IN INTERPOL'S LEGALLY BINDING FRAMEWORK

INTERPOL's relationship with its member countries is based on institutionalized and regulated cooperation. It is governed by public international law and the rules and regulations adopted by its own constituent bodies in a hierarchy of legally binding mechanisms, which are applicable to all member countries when using INTERPOL's facilities, including the INTERPOL Information System.

From a data-protection perspective, the legally binding rules which set out those safeguards are: INTERPOL's Constitution; INTERPOL's RPD; and the Statute of the Commission for the Control of INTERPOL's Files.

2.1. INTERPOL's Constitution

INTERPOL's Constitution sets forth the superstructure under which its operations and the cooperation of its members occur, including key parameters and limitations such as:

- the requirement to operate in the spirit of the Universal Declaration of Human Rights (Article 2);
- the independence and neutrality of the Organization, through a prohibition on "any intervention or activities of a political, military, religious or racial character" (Article 3);
- the establishment and functioning of an independent oversight body – the CCF (Article 36); and
- the creation of the rule-making process which empowers the General Assembly to determine whether and what internal operational rules and restrictions are necessary (Article 8(d)).

With respect to data protection and privacy specifically, the General Assembly has adopted throughout the years various rules on data processing, including the current rules. The adoption of such rules requires a two-thirds majority vote at the General Assembly.

2.2. Safeguards and Supervision - INTERPOL's Rules on the Processing of Data (RPD) and Data Protection Officer (IDPO)

INTERPOL's current set of data processing rules – the RPD – was adopted by INTERPOL's General Assembly in 2011 and entered into force in July 2012. They govern all data processing in the INTERPOL Information System, including that surrounding the publication and circulation of Red Notices.

The RPD are unique in scope considering their international application to 194 countries as a legally binding data protection instrument, encompassing 135 detailed provisions.

14 INTERPOL's Standing Committee on Data Processing is a permanent body created in 2019 to ensure the continuous assessment of and propose updates to applicable data protection rules with due consideration of international data protection standards. The Standing Committee replaced the Working Group on the Processing of Information (GTI), which had been in place since 2002. In addition, the Commission for the Control of INTERPOL's Files (CCF) commissioned the Centre de Recherche Information, Droit et Société (CRIDS) of the University of Namur in 2011 to carry out an assessment of INTERPOL's data protection framework. The study concluded that INTERPOL's legal framework governing data processing is among the more advanced that the Centre had evaluated.

The RPD adhere to the fundamental principles of data protection, as reflected in various international and regional instruments, such as lawfulness, purpose limitation, data quality, transparency, confidentiality, and security (Title 1, Chapter II, RPD). They explicitly provide for the right of access, correction, and deletion of data through a submission of a request to the CCF (Art. 18, RPD).

The RPD clearly define the roles and responsibilities of all the users of the INTERPOL Information System. They reiterate and elaborate upon the compliance requirements such as with the aforementioned Articles 2 and 3 of INTERPOL's Constitution (Art. 34, RPD). Additional noteworthy safeguards are defined retention periods (Art. 49-50, RPD), access restrictions (Art. 58), and the duty placed on end-users to verify the accuracy and relevancy of data prior to acting on it (Art. 63, RPD).

With regard to Notices, the RPD define the conditions for publication of each Notice including Red Notices (Art. 82-87, RPD). The RPD detail the obligation to review Notices prior to publication (Art. 77, RPD), to ensure compliance following publication (Art. 74, RPD), and to delete those Red Notices that no longer meet the conditions set out by the rules (Art. 81, RPD).

Considering the nature of the data processed via INTERPOL's channels (police data) and to ensure respect of individuals' rights, the RPD define confidentiality levels for the data processed, and impose requirements on limited access to data (Art. 112-114, RPD). A dedicated confidentiality desk was created at the General Secretariat to ensure compliance with those provisions. In addition, the rules provide for management of the security system through the appointment of a security desk, performance of risk assessments, addressing security incidents, etc. (Art. 115-118, RPD).

With respect to any prospective onward transfer of data, the RPD further define the conditions for external processing for police purposes: data initially processed in the INTERPOL Information System may be processed outside the system only if this processing is necessary; is carried out for police purposes; and is in compliance with the data-processing principles set forth in the RPD (Art. 16(1), RPD). The NCBs engaged in such processing must also ensure implementation of confidentiality and security requirements as provided by the RPD (Art. 16(2), RPD).

Additionally, granting access to the INTERPOL system to national law enforcement authorities (referred to in the RPD as "national entities") must follow a procedure established by the RPD. The NCBs must ensure, inter alia, that the national entity is able to observe the RPD, must conclude an agreement with the national entity based on a charter appended to the RPD, and must inform the General Secretariat and all other NCBs on the granting of access rights (Art. 21, RPD).

In some aspects, the RPD provide additional safeguards that may not necessarily be found in other data protection instruments, for instance by including the "effective implementation" of the Rules through supervision and monitoring as an additional data protection principle (Art. 17 RPD).

The principle of "effective implementation" is ensured, inter alia, through a full title in the Rules focusing on "supervision and monitoring" (Title 4). This title defines the different levels of supervision exercised and the tools to carry out supervision and monitoring. It enables an NCB to request information on how other NCBs are using its data (Art. 122, RPD). It also requires NCBs to evaluate the operations of national entities they have authorized to directly access the system, and to report to the General Secretariat on spot checks conducted, security incidents handled, and training provided (Art. 123, RPD). To ensure compliance with the Rules, the General Secretariat is authorized to set up compliance management databases (Art. 125, RPD).

Further, under Title 4, the General Secretariat is required to apply interim measures if a doubt arises on compliance with the Rules and for the purposes of preventing prejudice the data may cause to the Organization, member countries, or the individual concerned (Art. 129, RPD). Such steps may include, for example, provisional blocking of a Red Notice pending further review. The General Secretariat is also entitled to apply corrective measures to ensure compliance of data with the rules (e.g., correction of processing errors, supervision by the General Secretariat of processing operations carried out by an NCB, suspension of access and processing rights, etc. – Art. 131, RPD), and is empowered to ask an NCB to apply corrective measures to a national entity or terminate access of the national entity to the system if that entity repeatedly has processed data in non-compliance manner (Art. 123(4), RPD).

Based on this title, a Data Protection Office at the General Secretariat was established in 2016 (Art.121A, RPD). As provided by this provision, the INTERPOL Data Protection Officer (IDPO) is independent in the performance of his/her duties and reports directly to the Secretary General. Among his/her duties, the IDPO monitors the lawfulness and compliance of data processed in the INTERPOL Information System, provides advice including data protection impact assessments in relation to processing operations likely to affect the rights and freedoms of individuals, provides training, and liaises with the CCF and DPOs in NCBs as well as with other institutions and bodies.

This title also includes the requirement for the 194 member countries to designate a Data Protection Officer in their NCBs (NCB DPO), which act as the gatekeepers at the end-points of the INTERPOL Information System. In addition, each NCB is required to appoint a security officer to ensure compliance with procedures related to information security.

Since the adoption of the RPD, amendments were introduced in 2014 and 2016. To ensure that INTERPOL's legal framework continues to reflect the developments in the field from many operational perspectives, including that of data protection, a dedicated working group comprised of INTERPOL's member countries was tasked by INTERPOL's General Assembly in 2018 to review the RPD and propose additional amendments as needed. A number of proposed amendments were adopted by the General Assembly at its session in October 2019.

2.3. Oversight and Remedies – The Statute of the Commission for the Control of INTERPOL's Files

As mentioned above, the CCF was created in 1982 as an independent and impartial body responsible for ensuring that INTERPOL processes personal data in accordance with its rules and has appropriate redress mechanisms for data subjects.

Over the years, the function of the CCF has been elevated, for instance when it gained accreditation and recognition as a data protection authority with the International Conference of Data Protection and Privacy Commissioners in 2003, and when its role and mandate were incorporated in INTERPOL's Constitution in 2008.

In 2016, INTERPOL's General Assembly adopted a new legal framework governing the CCF. The new CCF Statute, which entered into force in March 2017, strengthens the CCF's status and capacities to carry out its functions.

In accordance with the CCF Statute, the CCF consists of two chambers:

1) A Supervisory and Advisory Chamber, which has the power to carry out checks to ensure compliance with INTERPOL's rules and, in that capacity, may issue binding decisions on the Organization as to measures required to remedy any incidence of non-compliance with the rules (Art. 26(1), CCF Statute). This Chamber also gives opinions on matters involving the processing of personal data (Art. 26(2), CCF Statute). For example, under the RPD

there is a requirement to seek the CCF's opinion before the creation of a new database containing personal data or the conclusion of an agreement with another entity which involves exchange of personal data.

2) A Requests Chamber, which has the exclusive power to examine and decide on requests by individuals for access to, or correction and/or deletion of, data processed in the INTERPOL Information System (Art. 28(1)(b), CCF Statute).

Importantly, the CCF Statute ensures that the CCF can provide an **effective remedy** to individuals, based on the principles identified in jurisprudence, notably that of the European Court of Human Rights (cf. case of Waite and Kennedy). Specifically, the following criteria are met:

- **Direct accessibility:** Individuals can apply directly and free of charge to the CCF (Art. 18, RPD; Art. 29 and 30(3), CCF Statute) and their applications remain confidential (art. 20(2), CCF Statute; Rules 13 and 29, CCF Operating Rules).
- **Independence and impartiality:** The CCF Statute reinforced the independence of the CCF as enshrined in Art. 36 of INTERPOL's Constitution (Art. 4, 5(1), 11, 15(4), CCF Statute), as well as the impartiality of the CCF and its members (Art. 12 and 13, CCF Statute).
- **Specialized expertise and knowledge:** The CCF members are experts in the relevant subject matters, as required for similar bodies (e.g., a data protection expert, a human rights expert, etc. – Art. 8, CCF Statute).
- **Free and unlimited access:** The CCF has free and unlimited access to all data processed in the INTERPOL Information System (Art. 19, CCF Statute).
- **Equality of arms:** The CCF Statute ensures equality of arms between the individual and the country that processed data concerning him/her, for example in relation to communication of information (Art. 35, CCF Statute) and the binding nature of the decisions on all parties (Art. 38(1), CCF Statute).
- **Timeliness of the procedure:** Specific procedural timeframes were introduced in the Statute (Art. 31(1), 32(1), 40, 41, CCF Statute).
- **Binding/final/reasoned decisions:** The CCF's decisions are final and binding on the Organization (Art. 38(1), CCF Statute). In accordance with the Statute, the decisions must be reasoned (Art. 38(2), CCF Statute). Subject to confidentiality requirements, selected decisions are made public on INTERPOL's website at https://www.interpol.int/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF/CCF-sessions-and-reports. (Art. 44, CCF Statute; INTERPOL's website). Though the CCF's decisions are final, applications for revision may be submitted to the CCF under certain conditions (Art. 42, CCF Statute).
- **Remedies:** The CCF is empowered to decide on "any appropriate remedy" to be granted to individuals (Art. 39, CCF Statute).

3. GLOBAL IMPACT OF INTERPOL'S ROLE IN PROMOTING DATA PROTECTION STANDARDS

With its unique set of binding data protection rules and implementation measures, INTERPOL serves to elevate data protection levels worldwide through its 194 member countries.

INTERPOL's consistent efforts to remain abreast of evolving data protection standards and practices is an essential element of how it ensures that its own legal framework remains appropriately calibrated. Such efforts are reflected, for example, in recommendations made by INTERPOL's Regional Conferences – which are subsidiary bodies of the General Assembly – that urged INTERPOL member countries to closely monitor legislative data protection developments in the field[15], consider the need to promote the introduction of national legislation on data protection in the police sector, and to develop and implement appropriately protective practices in the field.

Further, the heads of NCBs have recognised the need for "strong data protection standards" and encouraged continued development of the network of NCB DPOs mandatorily appointed in accordance with the RPD. This network is unique as currently no other international organization brings together a truly global network of DPOs in the law enforcement context. To strengthen this network, NCB DPOs are regularly trained on data protection rules and standards[16], participate in conferences organized by the General Secretariat[17], and submit annual reports on data processing operations to the General Secretariat.

INTERPOL's robust data protection practices ensure mutual trust for police data-sharing and also help to deliver innovative policing capabilities. INTERPOL-designed solutions incorporate a "privacy- and data protection-by-design" approach to protect individuals' rights in the development of tools and systems that maintain key functions and efficacy for data sharing[18].

CONCLUSION

INTERPOL is an international organization constituted under public international law and has long-standing experience in data processing and protection, as well as the promotion of privacy. Its legal framework, based on institutionalized and regulated cooperation applicable to all member countries, has strengthened over decades and evolved into a comprehensive code of binding Rules on the Processing of Data elevating "effective implementation" as a fundamental data protection principle.

An effective remedy for data subjects is provided through the procedures and final and binding decisions of the Commission for the Control of INTERPOL's Files, INTERPOL's independent supervisory body.

15 Examples here include the evolution of regional data protection legislation such as the EU's General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED).

16 Training includes classroom DPO training, tailor-made webinars, and access to training material and relevant documents via the NCB dashboard. The mandatory DPO training is followed by an optional 5 days Instructor Development Course (train the trainers).

17 A first NCB DPO Conference was held in Lyon in October 2018.and will be renewed as a regular event

18 For instance, the hashing system used to make comparisons with images already present in INTERPOL's International Child Sexual Exploitation database represents such a solution. By using a hash function to compare data, even the most sensitive data can be processed effectively while protecting the rights and privacy of the individuals concerned.

INTERPOL's modern and rigorous legal framework governing data processing enables the Organization to conclude data exchange agreements with other relevant entities such as international tribunals.

By implementing the Rules on the Processing of Data, INTERPOL promotes and elevates data protection standards and safeguards worldwide.

Legal Documents:

Relevant documents governing INTERPOL's data practices, including:

- INTERPOL's Constitution;
- INTERPOL's Rules on the Processing of Data;
- The Statute of the Commission for the Control of INTERPOL's Files; and
- Operating Rules of the Commission for the Control of INTERPOL's Files

can be found at the following links:

1) https://www.interpol.int/en/Who-we-are/Legal-framework/Legal-documents
2) https://www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF/About-the-CCF.