INTERPOL

INTERPOL's Rules on the Processing of Data

[III/IRPD/GA/2011 (2025)]

REFERENCES

Rules on International Police Cooperation and on the Internal Control of INTERPOL's Archives adopted by the General Assembly at its 51st session (Torremolinos, Spain, 1982) by Resolution AGN/51/RES/1.

Rules on the Deletion of Police Information Held by the General Secretariat adopted by the Executive Committee at its 84th session (Saint Cloud, France, 4-6 March 1987) following the powers delegated to it by the General Assembly at its 55th session by Resolution AGN/55/RES/2.

Rules Governing a Database of Selected Information at the ICPO-INTERPOL General Secretariat and Direct Access by NCBs to that Database adopted by the General Assembly at its 59th session (Ottawa, Canada, 1990) by Resolution AGN/59/RES/7.

Rules Governing Access by an Intergovernmental Organization to the INTERPOL Telecommunications Network and Databases adopted by the General Assembly at its 70th session (Budapest, Hungary, 2001) by Resolution AG-2001-RES-08.

Rules on the Processing of Information for the Purposes of International Police Cooperation adopted by the General Assembly at its 72nd session (Benidorm, Spain, 2003) by Resolution AG-2003-RES-04.

Implementing Rules for the Rules on the Processing of Information for the Purposes of International Police Cooperation adopted by the General Assembly at its 76th session (Marrakesh, Morocco, 2007) by Resolution AG-2007-RES-09.

INTERPOL's Rules on the Processing of Data adopted by the General Assembly at its 80th session (Hanoi, Viet Nam, 2011) by Resolution AG-2011-RES-07, and the Rules on the Processing of Information for the Purposes of International Police Cooperation, the Implementing Rules for the Rules on the Processing of Information for the Purposes of International Police Cooperation, and the Rules Governing Access by an Intergovernmental Organization to the INTERPOL Telecommunications Network and Databases abrogated by the General Assembly on 30 June 2012.

The General Secretariat corrected the English version of the Rules on 14 March 2013, in application of the provisions of Article 33(3) of the Rules of Procedure of the ICPO-INTERPOL General Assembly.

Articles 1, 4, 8, 10, 13, 23, 27, 34, 40, 44, 49, 52, 53, 61, 68, 69, 81, 88, 89, 104, 105, 126 amended, Article 70 became Article 71, new Article 70 added, Article 71 became Article 72, and Articles 80 and 81 combined in Article 81. The English versions of Articles 1, 27, 93, 104, and the Arabic version of Article 82 were modified by the General Assembly at its 83rd session (Monaco, 2014) by Resolution AG-2014-RES-18.

Articles 5, 18, 121 amended and Article 121A added by the General Assembly at its 85th session (Bali, Indonesia, 2016) by Resolution AG-2016-RES-06.

Articles 13, 22, 32, 36, 37, 46, 49, 50, 51, 52, 53, 63, 69, 70, 71, 105, 125, 126, 134 amended by the General Assembly at its 88th session (Santiago, Chile, 2019) by Resolution GA-2019-88-RES-02.

Articles 1, 10, 21, 36, 64, 104, 105, 106 amended, Article 43A added and Article 65 deleted by the General Assembly at its 91st session (Vienna, Austria, 2023) by Resolution GA-2023-91-RES-08.

Articles 1, 22, 24, 42, 47, 67, 70, 71, 135 amended by the General Assembly at its 92nd session (Glasgow, United Kingdom, 2024) by Resolutions GA-2024-92-RES-07 and GA-2024-92-RES-08.

Article 94 deleted by the General Assembly at its 93rd session (Marrakech, Morocco, 2025) by Resolution GA-2025-93-RES-08.

CONTENTS

PREAMBLE

The General Assembly of the International Criminal Police Organization – INTERPOL,

CONSIDERING Article 2, paragraph 1 of the Organization's Constitution,

HAVING CONSULTED the Commission for the Control of INTERPOL's Files in accordance with Article 36, paragraph 2 of the Constitution,

CONSIDERING that it is the responsibility of the General Assembly, in accordance with Article 8(d) of the Constitution, to determine the operating rules for the INTERPOL Information System regarding data processing,

HAS ADOPTED THE FOLLOWING RULES:

Article 1: Definitions

For the purposes of the present Rules:

(1) "Ordinary-law crime" means any criminal offences, with the exception of those that fall within the scope of application of Article 3 of the Constitution and those for which specific rules have been defined by the General Assembly.

(2) "Data" means any item of information, irrespective of its source, pertaining to constituent elements of ordinary-law crimes, the investigation and prevention of such crimes, the prosecution of the offenders and punishment of the offences, and any information pertaining to missing persons and unidentified dead bodies.

(3) "Personal data" means any data about an identified natural person or a person who may be identified by means that may reasonably be used.

(4) The "INTERPOL Information System" means all the structured material resources and software used by the Organization – databases, communications infrastructure, advanced sensor technology and other services – to process data through its channels in the context of international police cooperation.

(5) "Processing" means any operation or set of operations performed on data, whether or not by automatic means, such as collection, recording, consultation, transmission, use, disclosure and deletion.

(6) "Source" means any National Central Bureau which processes data in the INTERPOL Information System, and which is ultimately responsible for those data, or any international entity or private entity whose data are processed in the INTERPOL Information System, or on behalf of which data are recorded in the System, and which is ultimately responsible for them.

(7) "National Central Bureau" means any body designated by a country to perform the liaison functions provided for under Article 32 of the Organization's Constitution.

(8) "National entity" means an entity legally authorized to fulfil the role of a public institution that has specifically been authorized by the National Central Bureau of its country, through an agreement and within the limits determined by that National Central Bureau, to directly consult data processed in the INTERPOL Information System or to directly provide data for one or more of the processing purposes listed in Article 10 of the present Rules.

(9) "International entity" means any international, intergovernmental or non-governmental organization which fulfils an international public interest mission, which has concluded an agreement with the Organization on the exchange of data and which has been granted direct or indirect access to a part of the INTERPOL Information System by the Organization.

(10) "Private entity" means any legal person governed by private law such as a business, company, commercial association or a not-for-profit organization, not covered by the category of international entities, which has concluded an agreement with the Organization on the exchange of data, and in particular, on the processing of data in the INTERPOL Information System.

(11) "Request for international cooperation" means any steps taken by a National Central Bureau, an international entity or the General Secretariat via the INTERPOL Information System to send a request for assistance to one or more of the Organization's Members to carry out a specific action in conformity with the Organization's aims and activities.

(12) "International alert" means any steps taken by a National Central Bureau, an international entity or the General Secretariat via the INTERPOL Information System to send a notification to one of more of the Organization's Members about specific threats to public safety, persons and property.

(13) "Notice" means any request for international cooperation or any international alert published by the Organization at the request of a National Central Bureau or an international entity, or at the initiative of the General Secretariat, and sent to all the Organization's Members.

(14) "Diffusion" means any request for international cooperation or any international alert from a National Central Bureau or an international entity, sent directly to one or several National Central Bureaus or to one or several international entities, and simultaneously recorded in a police database of the Organization.

(15) "Message" means any request for international cooperation, any international alert or any data that a National Central Bureau or international entity with powers of investigation and prosecution in criminal matters chooses to send directly to one or several National Central Bureaus or to one or several international entities through the INTERPOL Information System but that it chooses, unless otherwise indicated, not to simultaneously record in a police database of the Organization.

(16) "Direct access" means entering and obtaining data in the INTERPOL Information System by expressly authorized persons using automatic means and without assistance from the General Secretariat.

(17) "Indirect access" means entering and obtaining data in the INTERPOL Information System with assistance of the General Secretariat.

(18) "Particularly sensitive data" means any personal data revealing racial or ethnic origin; political opinions; religious or philosophical convictions; trade-union membership; concerning health or sexuality; or biometric data.

(19) "Interconnection" means any electronic link which involves connecting a part of the INTERPOL Information System to a part of another information system.

(20) "Download" means any operation involving the exportation of data from the INTERPOL Information System into another information system.

(21) "Upload" means any operation involving the importation of data from another information system into the INTERPOL Information System.

(22) "Crime analysis" means the methodical identification and provision of insight into the relationship between data carried out in the context of international police cooperation.

(23) "Status of a person" means information about a person in connection with an event which warrants the processing of data in the INTERPOL Information System.

(24) "Positive query result" means a presumed match between data already recorded in the INTERPOL Information System and other data that are entered in this system.

(25) "Advanced sensor technology" means technology which facilitates the identification of persons and objects through automated data processing and may allow semi-automated decision-making, which requires human intervention for verification purposes.

(26) "Large data set" means a collection of structured or unstructured data shared by a source of data with the General Secretariat, which is not verified or categorized and which, due to its volume or complexity, cannot be assessed in accordance with all the requirements of the present Rules when initially processed by the General Secretariat.

(27) "Permanent operational police database" means a permanent police database created by the General Secretariat, irrespective of the particular data processing technology used, according to the requirements specified in Article 29 of the present Rules.

(28) "Recording" means inserting data or other items of information into a police database or a crime analysis file, according to the conditions for recording outlined in the present Rules.

(29) "Publicly available information" means information, not subject to any legal restriction, which is obtained without special legal status or authority, and which includes, but is not limited to, news and media sources, books and journals, online materials, academic materials, commercial databases, and subscription services available to any member of the public.

(30) "Biometric data" means personal data, relating to physical, biological, behavioural, or physiological characteristics, such as fingerprints, facial images, or DNA profiles, that have been subject to specific technical processing to enable or confirm the identification of an individual.

Article 2: Aim

The aim of the present Rules is to ensure the efficiency and quality of international cooperation between criminal police authorities through INTERPOL channels, with due respect for the basic rights of the persons who are the subject of this cooperation, in conformity with Article 2 of the Organization's Constitution and the Universal Declaration of Human Rights to which the said Article refers.

Article 3: Subject

The present Rules lay down the general principles, the responsibilities and the arrangements for the functioning of the INTERPOL Information System.

Article 4: Scope

(1) The processing of data through INTERPOL channels shall be done exclusively in the INTERPOL Information System.

(2) The present Rules shall apply to all data-processing operations performed in the INTERPOL Information System.

(3) Notwithstanding the applicable provisions of the present Rules, the General Assembly may adopt a separate legal framework whereby the Organization's Members agree to follow rules governing the processing of data for purposes of international judicial cooperation.

TITLE 1:
GENERAL PRINCIPLES

CHAPTER I:
PRINCIPLES CONCERNING INTERNATIONAL POLICE COOPERATION

Article 5: Compliance with the principles of governance and responsibilities associated with the processing of data

(1) International police cooperation through INTERPOL channels shall take place in accordance with the basic rules governing the Organization's operations, in particular its Constitution.

(2) The processing of data in the INTERPOL Information System shall be performed in conformity with, in particular, Articles 2, 3, 26, 31, 32, 36 and 41 of the Constitution.

(3) The Organization's Members shall endeavour to exchange a maximum of information of interest for the purposes of international police cooperation, with due observance of the Organization's political neutrality, independence and mandate, and of their respective national legislations and international conventions to which they are parties.

(4) At the national level, the National Central Bureaus shall play a central role concerning the processing of data in the INTERPOL Information System.

(5) The source shall be fully responsible for the data it processes in the INTERPOL Information System, regardless of the method used for such processing, and for the consequences directly resulting from such processing, and shall take appropriate measures to correct any incorrect processing of data.

(6) INTERPOL shall be fully responsible for any unauthorized or incorrect use and/or storage of data by INTERPOL and for the consequences directly resulting from such unauthorized or incorrect use and/or storage of data, and shall take appropriate measures to correct any incorrect processing of data by the Organization.

(7) Recipients of data processed in the INTERPOL Information System shall be fully responsible for:

(a) any action taken at the national level based on data they have received;

(b) taking the appropriate measures so that data received are immediately updated at the national level once they have been informed of any modification or deletion.

Article 6: Access to the INTERPOL Information System

(1) National Central Bureaus are entitled to direct access to the System in the performance of their functions pursuant to the Constitution. This access shall include:

(a) the recording, updating, and deletion of data directly in the Organization's police databases, as well as the creation of links between data;

(b) direct consultation of the Organization's police databases, subject to specific conditions determined for each database and to restrictions and confidentiality rules laid down by their sources;

(c) use of INTERPOL's notices and diffusions allowing the transmission of requests for cooperation and international alerts;

(d) following up on positive query results;

(e) transmission of messages.

(2) Access by national entities and international entities to the INTERPOL Information System is subject to authorization, and to the conditions provided for in Articles 21 and 27, respectively, of the present Rules.

Article 7: Control of data processing

(1) National Central Bureaus and international entities shall retain, at all times, control over the processing of their data, in accordance with the present Rules. Any National Central Bureau or international entity shall be free, in particular, to restrict the access to or the use of its data in one of the Organization's police databases, under the conditions provided for in Article 58 of the present Rules.

(2) Data processed in the INTERPOL Information System shall be those provided by National Central Bureaus, national entities and international entities. Nevertheless, data supplied by private entities in application of Article 28 of the present Rules or those recorded by the General Secretariat in application of Article 24(2) of the present Rules, may also be processed in the System.

Article 8: Use of INTERPOL notices and diffusions

(1) Requests for cooperation and international alerts through INTERPOL channels shall be sent by means of INTERPOL notices or diffusions.

(2) National Central Bureaus are entitled to use INTERPOL notices and diffusions in the performance of their functions pursuant to the Constitution. For international entities, entitlement shall be subject to authorization.

(3) The publication of INTERPOL notices and the transmission of diffusions shall be in accordance with Articles 73 et seq. of the present Rules.

(4) National Central Bureaus may send requests for cooperation and international alerts by means of messages, in accordance with Article 9 below. For international entities with powers of investigation and prosecution in criminal matters, this option shall be subject to authorization.

Article 9: Direct communication using messages

(1) The INTERPOL Information System enables direct communication between National Central Bureaus by means of messages.

(2) National Central Bureaus are entitled to send messages in the performance of their functions pursuant to the Constitution. For international entities, entitlement shall be subject to authorization.

(3) National Central Bureaus or international entities shall, prior to sending a message, ensure that it is in conformity with the present Rules.

(4) The General Secretariat may not record a message in one of the Organization's police databases without the prior consent of the National Central Bureau or international entity that sent the said message. The National Central Bureau or international entity is presumed to have given prior consent if the General Secretariat is one of the recipients of the said message.

(5) Further entitlements to communicate directly by means of messages may be granted in the context of specific projects or initiatives. In exceptional circumstances, a National Central Bureau may entitle expressly authorized persons who are not members of its staff to send such messages.

CHAPTER II: PRINCIPLES CONCERNING INFORMATION PROCESSING

Article 10: Purposes of international police cooperation

(1) The processing of data in the INTERPOL Information System may only be carried out for a given, explicit purpose which is in conformity with the Organization's aims and activities.

(2) Data shall be processed in the INTERPOL Information System for at least one of the following purposes:

(a) to search for a wanted person with a view to his/her detention, arrest or restriction of movement;

(b) to locate a person or an object of interest to the police;

(c) to provide or obtain information related to a criminal investigation or to the criminal history and activities of a person;

(d) to warn of a person, an event, an object or a modus operandi related to criminal activities;

(e) to identify a person or a dead body;

(f) to carry out forensic analyses;

(g) to carry out security checks that directly pertain to international police cooperation and are aimed at preventing or detecting crime;

(h) to carry out border management and border control activities;

(i) to identify threats, crime trends and criminal networks, including for crime analysis.

(3) The National Central Bureaus, national entities and international entities shall be responsible for determining the purpose of processing their data and for performing regular reviews, particularly once this purpose may have been achieved.

(4) The General Secretariat shall put in place mechanisms and tools to guarantee compliance with the said purpose at all times, under the conditions provided for in Articles 125 to 127 of the present Rules.

(5) The National Central Bureaus, national entities and international entities shall comply with this purpose when using data.

(6) National Central Bureaus, national entities and international entities shall only be allowed to process data for other purposes of international police cooperation or for administrative purposes if the processing is in conformity with the Organization's aims and activities, and is not incompatible with the purpose for which the data were initially processed in the INTERPOL Information System. The source shall be notified of such processing and shall retain the right to oppose it, under the conditions provided for in Article 64 of the present Rules. Such processing shall be the sole responsibility of the National Central Bureau, national entity or international entity choosing to process the data for purposes other than those for which the data had initially been processed.

(7) Data may also be processed for any other legitimate purpose distinct from international police cooperation, under the conditions provided for in Articles 132 et seq. of the present Rules.

Article 11: Lawfulness

(1) Data processing in the INTERPOL Information System should be authorized with due regard for the law applicable to the National Central Bureau, national entity or international entity and should respect the basic rights of the persons who are the subject of the cooperation, in accordance with Article 2 of the Organization's Constitution and the Universal Declaration of Human Rights to which the said Article refers.

(2) The National Central Bureaus, national entities and international entities shall be responsible for ensuring lawfulness of the collection and entry of their data in the INTERPOL Information System.

(3) The National Central Bureaus, national entities and international entities shall also be responsible for ensuring the lawfulness of the consultation of the data entered in the INTERPOL Information System.

Article 12: Quality

(1) Data processed in the INTERPOL Information System must be accurate, relevant, not excessive in relation to their purpose and up to date, to allow them to be used by National Central Bureaus, national entities and international entities.

(2) The National Central Bureaus, national entities and international entities shall be responsible for the quality of the data they record and transmit in the INTERPOL Information System.

(3) The General Secretariat shall put in place the mechanisms and tools to guarantee compliance with the aforementioned quality at all times.

(4) The National Central Bureaus, national entities and international entities are required to check the quality of data before using them, under the conditions provided for in Article 63 of the present Rules.

Article 13: Transparency

(1) The processing of data in the INTERPOL Information System should guarantee at all times that the processing rights of National Central Bureaus, national entities and international entities are respected in accordance with the present Rules.

(2) The General Secretariat shall be responsible for ensuring the transparency of data-processing operations and of the functioning of the Organization's databases:

(a) It shall request the opinion of the Commission for the Control of INTERPOL's Files if it intends to carry out any operations involving the processing of personal data referred to in Articles 27 to 31, 55, 56, 61, 68(4,d), 73(2) and 97(3) of the present Rules;

(b) It shall inform the Commission for the Control of INTERPOL's Files of any steps taken in application of Articles 51(7), 59, 118 and 125(2,b) of the present Rules;

(c) It shall submit to the Executive Committee any project or request relating to the processing of data in the INTERPOL Information System for which its prior authorization is required in accordance with Articles 17(5), 22(3), 23, 29, 30, 31, 55(3), 68(8), 97(3) and 131(3) of the present Rules, and shall attach the opinion of the Commission for the Control of INTERPOL's Files whenever so required by the present Rules. The Executive Committee shall report to the General Assembly on the authorizations it grants under the conditions provided for in Article 55(6) of the present Rules;

(d) It shall inform the Executive Committee of the measures taken in application of Articles 59, 68(4) and 118 of the present Rules;

(e) Under the conditions provided for in Article 126 of the present Rules, it shall keep up-to-date registers of the following:

(i) National Central Bureaus, national entities and international entities to which access has been granted to the INTERPOL Information System or which have supplied the data processed in the system;

(ii) the Organization's police databases, including analysis files;

(iii) interconnection operations;

(iv) the downloading and uploading operations performed;

(v) the data-processing operations recorded in the databases;

(vi) the data-management tools implemented by the General Secretariat;

(vii) comparison operations carried out for verification purposes.

These registers shall be available at all times to the National Central Bureaus. They shall also be available to international entities according to the access rights they have been granted, as well as to national entities through their National Central Bureaus.

(f) The General Secretariat shall keep an up-to-date list of the maximum data retention periods as defined by the Executive Committee in accordance with these Rules, and shall make this list publicly available.

Article 14: Confidentiality

(1) The confidentiality of data processed in the INTERPOL Information System should be determined according to the risks linked to their disclosure for those who are the subject of cooperation, the sources and the Organization. Data should only be accessible to persons authorized to know such information.

(2) National Central Bureaus, national entities and international entities are responsible for attributing levels of confidentiality to the data they enter in the INTERPOL Information System and for observing the confidentiality of the data they consult, transmit or use for external processing purposes, under the conditions provided for in Articles 112 et seq. of the present Rules.

(3) The General Secretariat shall ensure that all data are processed in the INTERPOL Information System according to the confidentiality level attributed by the National Central Bureau, national entities or international entities which carried out the processing.

(4) The General Secretariat shall take, in accordance with the present Rules, all necessary and appropriate measures to increase the confidentiality level attached to data to protect against risks that their disclosure may have for those who are the subject of cooperation, the sources of data and the Organization.

Article 15: Security

(1) The data processed in the INTERPOL Information System should be protected against risks violating their integrity and confidentiality, and remain available at all times to the National Central Bureaus, national entities and international entities having direct access to the INTERPOL Information System.

(2) The General Secretariat shall be responsible for setting up an information security management system. To that end, in consultation with the National Central Bureaus or with their representatives on the advisory bodies set up for the purpose, it shall establish and regularly update a security policy based on internationally accepted standards and on a risk assessment.

(3) The General Secretariat shall be responsible for developing the communication infrastructure and databases in order to preserve the security of data, in compliance with the security policy established.

(4) The General Secretariat shall be responsible for defining authorization or security-clearance procedures for its staff for each level of data confidentiality, under the conditions provided for in Articles 112 et seq. of the present Rules.

(5) National Central Bureaus and international entities shall be responsible for the access they grant to the INTERPOL Information System, the security of the facilities which enable them to access that system, compliance with the established rules of security and for maintaining data at a level of security at least equivalent to that laid down by the General Secretariat in cases of external processing.

(6) The General Secretariat shall take, in accordance with the present Rules, all appropriate measures to protect the security of data processed in the INTERPOL Information System.

Article 16: External processing for police purposes

(1) The data initially processed in the INTERPOL Information System may be processed outside the system if this processing is necessary and carried out for police purposes. Any external processing must be in compliance with the above-mentioned data-processing principles.

(2) The National Central Bureaus and international entities shall be responsible for implementing the arrangements for external processing, under the conditions provided for in Articles 114(4) and 116 of the present Rules.

(3) The General Secretariat shall advise the National Central Bureaus and international entities in implementing these arrangements.

Article 17: Effective implementation

(1) The present Rules must be effectively implemented.

(2) National Central Bureaus, national entities and international entities shall be responsible for defining and establishing effective and appropriate measures to guarantee the compliance of their operations with the principles and obligations laid down in the present Rules, in particular through staff training.

(3) National Central Bureaus shall be responsible for defining and establishing procedures to guarantee the compliance of the operations of their national entities with the principles and obligations laid down in the present Rules, prior to granting them authorization to directly consult data processed in the INTERPOL Information System or to directly provide data for processing purposes in the System.

(4) The National Central Bureaus shall be responsible for regularly evaluating the operation of each of their national entities in the light of the present Rules, and shall, within the limits set by the present Rules, take all necessary and appropriate corrective measures vis-à-vis these national entities to terminate any non-compliant processing of data. They may take all necessary precautionary measures to take account of the risk inherent in any clearly non-compliant use of data.

(5) The General Secretariat shall be responsible for regularly evaluating the operation of the National Central Bureaus in the light of the present Rules. It shall take all necessary and appropriate corrective measures to terminate any non-compliant processing of data, under the conditions provided for in Article 131 of the present Rules. Any measures which may result in the long-term suspension of the processing rights of a National Central Bureau shall be submitted to the Executive Committee for prior approval.

(6) The General Secretariat shall be responsible for regularly evaluating the operation of the international entities in the light of the present Rules, and shall adopt any necessary and appropriate corrective measures to terminate any non-compliant processing of data, under the conditions provided for in Article 131 of the present Rules.

Article 18: Rights of access, correction and deletion of data

(1) Any person or entity shall be entitled to submit directly to the Commission for the Control of INTERPOL's Files a request for access to, or correction and/or deletion of data processed in the INTERPOL Information System concerning that person or entity.

(2) These rights of access to, or correction and deletion of data shall be guaranteed by the Commission for the Control of INTERPOL's Files and be governed by separate rules. Unless otherwise specified in those rules, requests for access to, or correction and/or deletion of data may not be processed in the INTERPOL Information System.

TITLE 2:
PARTICIPANTS

CHAPTER I:
ROLE OF THE NATIONAL CENTRAL BUREAUS

Article 19: Coordination of data flow

(1) The National Central Bureaus shall be responsible for coordinating at the national level the processing in the INTERPOL Information System of data provided by their countries.

(2) The National Central Bureaus shall be responsible, with due respect for the present Rules, for providing the institutions of their countries with data processed in the INTERPOL Information System and necessary for the performance of their duties.

Article 20: Coordination of criminal inquiries

(1) Matters relating to criminal inquiries shall be coordinated in conjunction with the National Central Bureaus.

(2) The National Central Bureaus shall be responsible for coordinating at the national level the processing of requests for cooperation and international alerts sent to them by means of INTERPOL notices, diffusions and messages. As such, they shall be free to determine the most appropriate means, at the national level, for effective international cooperation.

(3) The National Central Bureaus shall be responsible for following up on requests for cooperation and international alerts that they have sent at the request of the institutions of their respective countries, by means of INTERPOL notices, diffusions and messages.

Article 21: Granting authorizations to directly access the INTERPOL Information System at the national level

(1) The National Central Bureaus alone shall be entitled to authorize the entities of their countries to access the INTERPOL Information System and determine the extent of their access and processing rights.

(2) Prior to granting authorizations for direct access, the National Central Bureaus must ensure that all the following conditions are met:

(a) the entity to which it intends to grant direct access to the INTERPOL Information System is a national entity as defined in Article 1(8) of the present Rules;

(b) the nature of the activities and tasks of this entity do not violate the aims or the neutrality of the Organization;

(c) the national laws do not prohibit such access by this entity;

(d) the entity will be able to observe the present Rules;

(e) the access and processing rights it intends to grant are limited, strictly necessary and proportionate to the execution of the tasks and functions of this entity.

(3) When a National Central Bureau grants an authorization to directly access the INTERPOL Information System, it shall be subject to a prior agreement between the National Central Bureau and the new national entity. The agreement must comply with the "Charter relating to access to the INTERPOL Information System by national entities" appended to the present Rules.

(4) When a National Central Bureau grants authorization to a new national entity, it shall immediately notify the General Secretariat and all National Central Bureaus and international entities.

(5) National entities shall process their data in the INTERPOL Information System within the limits of the processing rights granted to them.

(6) National Central Bureaus shall communicate to their national entities the necessary information for them to exercise these processing rights.

(7) National Central Bureaus shall be responsible for the processing of data by the national entities they authorize to access the INTERPOL Information System.

CHAPTER II:
ROLE OF THE GENERAL SECRETARIAT

Article 22: Administration of the system

(1) The General Secretariat shall be responsible for the general administration of the INTERPOL Information System.

(2) It shall design, organize and administer the INTERPOL Information System and decide upon which technologies it should be based. When implementing data processing technologies, the General Secretariat shall ensure that the requirements of these Rules are integrated by design and by default as early as possible through appropriate technical and organizational measures.

(3) It shall examine and process, under the Executive Committee's supervision and with due respect for the present Rules, downloading and interconnection requests submitted by the National Central Bureaus, under the conditions laid down in Articles 55 and 56 of the present Rules.

(4) It shall house the Organization's databases.

(5) It shall manage the processing of data in the INTERPOL Information System and ensure that the conditions for processing data in the Organization's databases are duly observed. It shall put in place the tools for managing data and access to the System. It shall perform a management role when conducting spot checks and resolving processing incidents.

(6) It shall manage INTERPOL's communications infrastructure to enable direct exchanges of data through the INTERPOL Information System. Notwithstanding any obligation applicable to it in Title 1, Chapter II and Article 22(5) of the present Rules, where the General Secretariat is not a recipient of, or has not accessed the exchange, its role shall be limited in the following manner:

   (a) It shall ensure the security of such data exchanges, in accordance with Article 15 of the present Rules;

   (b) It shall take action to examine and ensure compliance with the present Rules when it becomes aware of a potential violation of the present Rules, or of the terms and conditions applicable to a specific project, including applying measures under Title 4, Chapter III of the present Rules;

   (c) With the exception of actions required to exercise its role under paragraph (b) above, it shall not access INTERPOL's communications infrastructure for the content of the direct exchanges without explicit authorization by the entity concerned.

Article 23: Additional measures to enhance cooperation

(1) The General Secretariat shall be entitled to propose to the General Assembly the conclusion of agreements relating to data processing, and to propose to the Executive Committee the establishment of databases, INTERPOL notices or diffusions under the conditions laid down in Articles 27, 28, 29, 73 and 97 respectively of the present Rules.

(2) The General Secretariat may, within the limits set by the present Rules, carry out tests to examine and draw up the above proposals.

Article 24: Recording data

(1) In accordance with the present Rules, the General Secretariat shall record, update, and delete data in the Organization's police databases:

   (a) on behalf of sources which do not have direct access to the INTERPOL Information System;

   (b) on its own initiative, when the data constitutes publicly available information or are received from persons or entities who have contacted the General Secretariat, the National Central Bureaus, international entities, or private entities, under the conditions set forth in Article 47 of the present Rules, or when the data are the result of crime analyses conducted by the General Secretariat;

   (c) in exceptional circumstances, at the request or on behalf of a National Central Bureau, national entity or international entity with direct access to the INTERPOL Information System.

(2) The General Secretariat may only record data on behalf of sources which do not have access to the INTERPOL Information System or on its own initiative if procedures for updating and deleting the information have been established beforehand.

Article 25: Coordination

(1) The General Secretariat shall facilitate cooperation between the National Central Bureaus. It shall request from them or forward to them, in accordance with the present Rules and the restrictions and rules of confidentiality laid down by the source, all the data that it believes may improve the coordination of international cooperation.

(2) If the purposes of international cooperation so require, the General Secretariat may exercise a role of direct coordination with the national entities, subject to express authorization by their respective National Central Bureaus.

(3) The General Secretariat shall, whenever necessary, facilitate cooperation between the National Central Bureaus and international and private entities.

(4) In order to improve international coordination, the General Secretariat may publish notices on its own initiative, under the conditions laid down in Article 103 of the present Rules.

Article 26: Emergency measures

(1) If the cooperation mechanisms established by the Organization, its independence or the fulfilment of its commitments are under serious and imminent threat and the proper functioning of the INTERPOL Information System is likely to be interrupted, the Secretary General shall take, with regard to data processing, the appropriate measures required under these circumstances after official consultation with the President of the Organization. He shall notify the National Central Bureaus and the Commission for the Control of INTERPOL's Files. These measures should be prompted by the desire to ensure, within the shortest possible time, that the National Central Bureaus have the means of performing their functions pursuant to the Constitution.

(2) When there is a real and imminent threat to people or property, and the data allowing a National Central Bureau, a national entity or an international entity to prevent this threat are subject to access restrictions placed against them, the General Secretariat shall be authorized to apply the emergency procedure provided for in Article 59 of the present Rules.

CHAPTER III: RELATIONS WITH THE INTERNATIONAL ENTITIES AND PRIVATE ENTITIES

Article 27: Conditions relating to the processing of data by international entities

(1) Whenever it considers it desirable, and when it is consistent with the aims and objects provided in its Constitution, the Organization may establish relations with international entities in order to collaborate with them on data processing on a regular basis. The establishment of regular relations between the Organization and an international entity shall be laid down in an agreement.

(2) The General Secretariat shall request the opinion of the Commission for the Control of INTERPOL's Files about all draft agreements that involve the processing of personal data.

(3) The General Secretariat shall submit all draft agreements to the General Assembly for approval. To justify its request, the General Secretariat shall provide:

(a) the purposes, conditions and implications of the agreement;

(b) the outcome of any tests conducted by the General Secretariat;

(c) the opinion of the Commission for the Control of INTERPOL's Files if the draft agreement concerns the processing of personal data;

(d) the text of the draft agreement.

(4) Data processing by international entities shall be subject to all the following conditions:

(a) The international entity is an international, intergovernmental or non-governmental organization performing a public-interest role at the international level;

(b) Such processing is strictly limited to the purposes of cooperation envisaged between the international entity and INTERPOL;

(c) The processing of personal data is strictly limited to the entity's need to know about such data;

(d) The international entity undertakes, in the agreement, to observe the processing principles and the general obligations incumbent upon any source, as set out in the present Rules;

(e) The international entity and INTERPOL have concluded an agreement on the procedures for processing data transmitted between both parties.

(5) Direct access by international entities to part of the INTERPOL Information System shall be subject to the following additional conditions:

(a) The international entity accepts and agrees to comply with the present Rules and the specific provisions of the agreement;

(b) The international entity accepts and agrees to comply with such security rules and administrative procedures as may be established by the INTERPOL General Secretariat pursuant to the present Rules to allow access to and use of the INTERPOL Information System;

(c) The international entity accepts that regular checks may be performed, either remotely or on the premises, on its processing of data transmitted by INTERPOL;

(d) Access shall only be granted to one unit or department within the said entity;

(e) Access may not result in the interruption or delay of the transmission of requests for cooperation and alerts, or access to such requests and alerts by the National Central Bureaus;

(f) The international entity wishing to be able to transmit data by means of a message to one or several National Central Bureaus or one or more international entities has powers of investigation and prosecution in criminal matters;

(g) The international entity wishing to request the publication of INTERPOL notices or to transmit diffusions has powers of investigation and/or prosecution in criminal matters. However, the use of the special notice system shall be examined on a case-by-case basis.

(6) The Organization's decision to authorize a new international entity to access the INTERPOL Information System shall be notified to the National Central Bureaus and other international entities by the General Secretariat. Access shall only become effective after completion of a procedure to safeguard the control by the other National Central Bureaus and other international entities over the rights granted to the new entity to process their data, under the conditions laid down in Article 109 of the present Rules.

(7) The list of agreements concluded shall be forwarded each year to the Executive Committee, to the Commission for the Control of INTERPOL's Files and to the General Assembly.

Article 28: Conditions relating to the processing of data by private entities

(1) Insofar as it is relevant to the accomplishment of its aims, the Organization may establish relations with private entities wishing to cooperate with it in data-processing matters. The establishment and conduct of relations between INTERPOL and a private entity shall be laid down in an agreement.

(2) The General Secretariat shall request the opinion of the Commission for the Control of INTERPOL's Files about all draft agreements that involve the processing of personal data.

(3) The General Secretariat shall submit all draft agreements to the General Assembly for approval. To justify its request, the General Secretariat shall provide:

(a) the purposes, conditions and implications of the agreement;

(b) the outcome of any tests conducted by the General Secretariat;

(c) the opinion of the Commission for the Control of INTERPOL's Files if the draft agreement concerns the processing of personal data;

(d) the text of the draft agreement.

(4) Cooperation with a private entity must:

(a) respect INTERPOL's Constitution and in particular the principle of national sovereignty. Any National Central Bureau which has recorded data in the INTERPOL Information System or on whose behalf data have been recorded in the system may oppose the forwarding of that data to a private entity;

(b) be subject to agreements, the conclusion of which has previously been authorized by the Executive Committee and then approved by the General Assembly.

(5) Such cooperation may only be considered if:

(a) the private entity is a legal person governed by private law;

(b) the processing is in conformity with the Organization's aims and activities;

(c) the purpose of the cooperation is clearly stated and corresponds to one of the prevention activities related to ordinary-law crimes;

(d) it is of interest for the purposes of international police cooperation in relation to the purpose concerned;

(e) durable cooperation is envisaged;

(f) the type of data to which access is made possible is identified in a specific manner;

(g) the data supplied by the private entity are identified as such and cannot be confused with the data obtained from other sources;

(h) the independence of the Organization in its cooperation with the private entity is guaranteed;

(i) cooperation with the private entity does not interfere with the transmission of international cooperation requests and alerts;

(j) the private entity undertakes, in the agreement, to respect the processing principles and the general obligations incumbent upon all sources, as set out in the present Rules.

(6) Data supplied to private entities must be limited to analytical data and may not be personal in nature. Nevertheless, in exceptional cases, data supplied to private entities may be extended, as part of a specific project, to include personal data (but not nominal data, unless the National Central Bureaus or international entities which have supplied the data give their express authorization to do so) and/or data used in an operational context. In that case, the following additional conditions must be met:

(a) the scope of the project must be clearly defined;

(b) the project must be the subject of a prior agreement with the entities concerned;

(c) access to these data is strictly limited to the entity's need to know such data;

(d) the use made of the data must be proportional to the aims referred to in Article 10(2) of the present Rules.

(7) The conditions relating to the processing of data by private entities shall be set out in the agreement concluded between the private entity and the Organization.

(8) Before providing private entities with data, according to the authorizations and conditions under the agreement, the General Secretariat shall notify the source of that data. The source shall have 45 days with effect from the date of notification to signify its opposition to this data communication.

(9) The ways in which data are communicated to private entities must be defined in the agreement in order to guarantee the security and integrity of the data processed in the INTERPOL Information System.

(10) The General Secretariat shall ensure that the means used by private entities to supply or obtain data processed in the INTERPOL Information System allow those entities to access only the data authorized, in conformity with the agreements concluded to that effect. The General Secretariat shall ensure that private entities are not able to access operational data, to compromise, or to interfere with police communications.

(11) Under no circumstances shall the INTERPOL Information System be used to circumvent restrictions imposed by any national laws governing police cooperation with private entities.

(12) The list of agreements concluded shall be forwarded each year to the Executive Committee, to the Commission for the Control of INTERPOL's Files and to the General Assembly.

TITLE 3:
PROCEDURES FOR PROCESSING DATA

CHAPTER I:
POLICE DATABASES

SECTION 1: AUTHORIZATION

Article 29: Creation of a database

(1) The General Secretariat shall submit any proposal to create a police database to the Executive Committee for approval.

(2) To justify its request, the General Secretariat shall provide:

(a) the reasons that led it to develop this project, as well as the financial implications of such a project;

(b) the list of the general characteristics of this database drawn up in consultation with the National Central Bureaus or with their representatives on the advisory bodies set up for that purpose;

(c) the outcome of any tests conducted by the General Secretariat;

(d) the opinion of the Commission for the Control of INTERPOL's Files, if the database contains personal data or is linked to such data.

(3) Any creation of a police database shall immediately be notified to the National Central Bureaus. It shall also be notified to the international entities according to the access rights they have been granted to the INTERPOL Information System.

Article 30: Modification of an existing database

(1) The General Secretariat shall be entitled to modify police databases.

(2) The General Secretariat shall request the opinion of the Commission for the Control of INTERPOL's Files on any proposal to modify a database that would result in the modification of its general characteristics if the database contains personal data or is linked to such data.

(3) The General Secretariat shall submit to the Executive Committee for approval any proposal to modify a database that would result in the modification of its general characteristics.

(4) To this end, the General Secretariat shall provide:

(a) the reasons that led it to propose a modification of this database, as well as the financial implications of such a modification;

(b) the revised list of the characteristics of this database, drawn up in consultation with the National Central Bureaus or with their representatives on the advisory bodies set up for the purpose;

(c) the outcome of any tests conducted by the General Secretariat;

(d) the opinion of the Commission for the Control of INTERPOL's Files, if the database contains personal data or is linked to such data.

(5) Any modifications to the general characteristics of a police database shall immediately be notified to the National Central Bureaus. They shall also be notified to the international entities according to the access rights they have been granted to the INTERPOL Information System.

Article 31: Deletion of an existing database

(1) The General Secretariat shall report to the Commission for the Control of INTERPOL's Files any intention to delete a database and the processing of data contained in that database.

(2) The General Secretariat shall submit to the Executive Committee for approval any intention to delete a database.

(3) To this end, the General Secretariat shall provide:

(a) the reasons that led it to propose the deletion, as well as the financial implications of the deletion;

(b) the report it submitted to the Commission for the Control of INTERPOL's Files and the Commission's opinion.

(4) Any deletion of a police database shall immediately be notified to the National Central Bureaus. It shall also be notified to the international entities according to the access rights they have been granted to the INTERPOL Information System.

Article 32: Authorizations granted by the Executive Committee

(1) Each year, the Executive Committee shall report to the General Assembly the authorizations it has granted for the creation, modification or deletion of police databases belonging to the Organization, indicating in particular their position in the overall INTERPOL Information System, the purpose of each, the nature of the data they store, and the processing rights attaching to each database.

(2) The Executive Committee shall also report to the General Assembly on the maximum retention period it has set for each type of data processed in the INTERPOL Information System, indicating the underlying reasons.

Article 33: Register of existing databases

(1) The General Secretariat shall keep an updated register of the Organization's police databases. The register shall specify the general characteristics of each database.

(2) National Central Bureaus may consult this register at any time. International entities may consult part of this register according to the access rights they have been granted to the INTERPOL Information System.

SECTION 2: FUNCTIONING

Article 34: Compliance with the Organization's Constitution

(1) In conformity with Article 5 of the present Rules, prior to any recording of data in a police database, the National Central Bureau, national entity or international entity shall ensure that the data are in compliance with Article 2 of the Organization's Constitution, and also that it is authorized to record such data pursuant to applicable national laws and international conventions and to the fundamental human rights enshrined in the Universal Declaration of Human Rights to which the said Article refers.

(2) In conformity with Article 5 of the present Rules, prior to any recording of data in a police database, the National Central Bureau, national entity or international entity shall ensure that the data are in compliance with Article 3 of the Organization's Constitution.

(3) To determine whether data comply with Article 3 of the Constitution, all relevant elements shall be examined, such as:

(a) nature of the offence, namely the charges and underlying facts;

(b) status of the persons concerned;

(c) identity of the source of the data;

(d) the position expressed by another National Central Bureau or another international entity;

(e) obligations under international law;

(f) implications for the neutrality of the Organization;

(g) the general context of the case.

(4) In light of the directives issued by the General Assembly and of developments in international law, the General Secretariat may compile repositories of practice on the application of Articles 2 and 3 of the Constitution, and make them available to the National Central Bureaus, national entities and international entities.

Article 35: Interest of the data for the purposes of international police cooperation

(1) In conformity with Article 5(3) of the present Rules, prior to any recording of data in a police database, the National Central Bureau, national entity or international entity shall ensure that the data are of interest for the purposes of international police cooperation.

(2) Compliance with this condition for recording data shall be assessed in relation to:

(a) the purposes specific to international police cooperation which are laid down in Article 10(2) of the present Rules; and

(b) the international nature of the data and, in particular, the extent to which the data may be used by National Central Bureaus, national entities or international entities other than the source.

Article 36: General characteristics of databases

(1) Each police database shall be defined with regard to the following characteristics:

(a) specific purpose of the database;

(b) nature of the data it contains, especially personal or particularly sensitive data;

(c) sources likely to contribute to the database;

(d) applicable confidentiality levels;

(e) applicable types of restrictions;

(f) applicable security measures;

(g) National Central Bureaus, national entities or international entities likely to record data in the database;

(h) minimum conditions for recording data;

(i) procedures for recording data, in particular any specific processing carried out on data during the recording due to their nature;

(j) procedures for updating recorded data;

(k) retention period of the data and the specific methods for extending or deleting this period;

(l) procedures and mechanisms used to check the compliance of the data;

(m) National Central Bureaus, national or international entities likely to consult the database;

(n) procedures for consulting the database, especially any type of direct access or any interconnection and uploading operations;

(o) procedures for using the data;

(p) procedures to follow if a positive query result is generated on the basis of data recorded in the database;

(q) data which may be disclosed to the public in conformity with Article 61 of the present Rules.

(2) All of the general characteristics above determine the legal framework applicable to each of the Organization's databases.

Article 37: Minimum conditions for recording data in the databases

(1) Minimum conditions shall be set for recording data in each database.

(2) Regardless of the database, the recording of data about a person, object or event must include:

(a) the identity of the source of the data;

(b) the date on which the data were recorded;

(c) the specific purpose for the recording;

(d) for any personal data, the status of the person and the data connecting this person to an event;

(e) the level of confidentiality of the data;

(f) the retention period of the data;

(g) access restrictions;

(h) any additional information ensuring that all the data are relevant to the purpose and of interest for the purposes of international police cooperation.

(3) These conditions shall be established by the General Secretariat in consultation with the National Central Bureaus or with their representatives on the advisory bodies set up for the purpose and communicated to all National Central Bureaus. They shall also be communicated to international entities according to the access rights they have been granted.

(4) All National Central Bureaus, national entities and international entities shall ensure that the minimum recording conditions are met when recording data in a police database.

(5) All National Central Bureaus, national entities and international entities shall keep any items on the basis of which the data were recorded or which justify retaining the information in the database.

Article 38: Additional conditions for recording data on persons

(1) Additional conditions for recording data on persons shall be applicable in the following cases:

(a) data on deceased persons;

(b) data on victims or witnesses;

(c) data on minors;

(d) particularly sensitive data.

(2) All National Central Bureaus, national entities and international entities shall observe these additional recording conditions when recording information in a police database.

Article 39: Additional conditions for recording data on deceased persons

(1) Data on deceased persons shall be recorded only in the following cases:

(a) for identification purposes;

(b) if the person has played a part in a criminal case or an event that has been processed in the Organization's police databases and the data concerning this person are necessary to understand the case or the event;

(c) for crime-analysis purposes.

(2) Data shall be recorded for the time strictly required to achieve one of the processing purposes above.

(3) The status of these persons and the purpose for recording the data shall be specified in a manner such that the data cannot be confused, in any way whatsoever, with data on persons who are the subject of cooperation.

Article 40: Additional conditions for recording data on persons who are victims or witnesses

(1) Data on persons who are victims or witnesses shall be recorded exclusively in the context of the events or acts of which they were victims or to which they were witnesses, and may not be used in relation to other events or acts. The status of these persons and the purpose for recording the data shall be specified in a manner such that the data cannot be confused, in any way whatsoever, with data on persons suspected of, accused of or convicted for these same acts.

(2) An additional indication shall be inserted to the effect that no restrictive measures may be taken against them.

Article 41: Additional conditions for recording data on minors

(1) The additional indication "MINOR" must be inserted whenever the person was a minor at the time of the event or act which is being recorded. The age at which a minor attains majority shall be determined in the light of the national laws of the National Central Bureau or the national entity that recorded the data or, in the case of an international entity, in the light of the applicable rules.

(2) In this case, the National Central Bureau, national entity or international entity which records the data shall specify any particular conditions imposed by applicable national laws.

Article 42: Additional conditions for processing particularly sensitive data

(1) Particularly sensitive data may only be processed in the INTERPOL Information System if:

(a) they are relevant and of particularly important criminalistic value for achieving the aims of the Organization and the purposes of the processing as described in Article 10(2) of the present Rules;

(b) they are described objectively and contain no judgment or discriminatory comments.

(2) Biometric data are considered to be relevant and of particularly important criminalistic value when processed in the INTERPOL Information System:

(a) to identify or confirm the identity of an individual, or the unidentified dead body or human remains of an individual;

(b) to avoid the misidentification of an individual in the context of international police cooperation; and/or

(c) to enable the establishment of links between crimes and crime scenes.

(3) When recorded in one of the Organization's databases, particularly sensitive data shall be recorded in a manner which enables them to be identified as such when they are consulted.

(4) The forwarding of any particularly sensitive data shall be carried out in accordance with Article 67 of the present Rules.

(5) Particularly sensitive data shall not be processed, in any form whatsoever, for any discriminatory purpose.

Article 43: Additional conditions for recording copied or uploaded data

(1) Data from one of the Organization's police databases may only be copied into another of the Organization's police databases or into part of the INTERPOL Information System if all the following conditions are met:

(a) if the data are copied for the same purpose, the source of the data has not objected within 10 days;

(b) if the data are copied for another purpose, the source has agreed to their processing for this new purpose;

(c) copying the data is unlikely to prejudice the integrity and the confidentiality of the data copied;

(d) the data are copied exactly;

(e) the data are regularly updated.

(2) The General Secretariat shall ensure that these additional recording conditions are complied with when the data of one of the Organization's police databases are copied into another of the Organization's police databases.

(3) Data may only be uploaded into the INTERPOL Information System if all the following conditions are met:

(a) the uploading is carried out by a National Central Bureau, a national entity, an international entity, or the General Secretariat, and is done with due respect for the provisions of the present Rules;

(b) the data are copied exactly;

(c) the National Central Bureau, national entity or international entity uploading the data ensures they are regularly updated.

Article 43A: Additional conditions for temporarily processing large data sets

(1) The General Secretariat may temporarily process large data sets to determine their potential interest for the purposes of international police cooperation and to assess their compliance with the present Rules.

(2) In consultation with the source of the data, such temporary processing may include, inter alia, data structuring, formatting, assessing, categorizing and comparing against data already processed in the INTERPOL Information System.

(3) The temporary processing shall meet the following conditions:

(a) the data shall comply with the applicable general principles as defined in Title 1 of the present Rules;

(b) the data shall be processed in a protected data-processing environment within the INTERPOL Information System. The data shall be separated from other operational or analytical data and shall be distinguished from data provided by other sources;

(c) the retention period of the data in this environment shall be determined by the source, but shall not exceed the maximum retention period determined by the Executive Committee;

(d) access to the data shall be restricted to authorized departments or members of staff of the General Secretariat to whom specific access has been granted;

(e) any other conditions defined by the source of the data.

(4) Following an assessment of the data, the General Secretariat shall communicate the results of the assessment to the source of the data and shall promptly delete any non-compliant data.

(5) The source of the data may process any compliant data for one or more of the processing purposes listed in Article 10 of the present Rules.

(6) The General Secretariat shall then delete the remaining data from the temporary processing environment and shall inform the source of the data accordingly.

Article 44: Status of persons

(1) When recording any data concerning a person who is the subject of international police cooperation, the National Central Bureau, national entity or international entity must specify the status of that person from the following list:

(a) Convicted: a person who, following a court ruling, has been found guilty of committing an ordinary-law crime;

(b) Charged: a person against whom criminal proceedings have been initiated for allegedly committing an ordinary-law crime;

(c) Suspect: a person who, as part of a criminal investigation, is considered to be a possible offender but against whom no charges have been filed;

(d) Criminal history: a person who is known to law-enforcement departments because of a previous conviction, or previous criminal conduct for which he/she has not been exonerated;

(e) Witness: a person who is not a suspect and who might be able to provide information relevant to a criminal investigation or an investigation into a disappearance;

(f) Victim: a person against whom a crime has been committed;

(g) Missing: a person whose whereabouts are unknown and who has been reported as missing;

(h) Unidentified person: a person, alive, whether criminal or not, the identification of whom is sought;

(i) Unidentified body: a dead person, whether criminal or not, the identification of whom is sought;

(j) Deceased: a person on whom data is kept in INTERPOL's police databases following the confirmation of his/her death;

(k) Possible threat: a person who presents or is likely to present a danger to public safety;

(l) Subject to UN sanctions: a person subject to sanctions decided upon by the United Nations Security Council.

(2) Other statuses may be established by the General Secretariat in consultation with the National Central Bureaus and the international entities or with their representatives on the advisory bodies set up for the purpose.

Article 45: Definition of specific conditions of use when recording data

In accordance with Article 12(1) of the present Rules, any National Central Bureau, national entity or international entity which records data shall specify the conditions for use of these data once they have been entered in the INTERPOL Information System and, in particular, any conditions linked to using the data as evidence in criminal proceedings.

Article 46: Updates

(1) The National Central Bureau, national entity or international entity that recorded data shall update them regularly.

(2) When the purpose for which the data were recorded has been achieved, these data may only be updated or retained in the Organization's police database if the National Central Bureau, national entity or international entity that recorded them determines and justifies a new purpose for their recording.

(3) The National Central Bureau, national entity or international entity that updates data shall ensure that the conditions for recording those data are met.

(4) The National Central Bureau, national entity or international entity that recorded data may also modify, at any time:

(a) the retention period of the data;

(b) their level of confidentiality;

(c) restrictions on access to data;

(d) conditions for consultation;

(e) conditions for use.

Article 47: Additional conditions for recording publicly available information and other information received from persons or entities

(1) The following additional conditions shall apply to the recording of publicly available information and information received from persons or entities who have contacted the General Secretariat, National Central Bureaus, international entities, or private entities:

(a) The recording of information shall be in conformity with, and relevant for achieving, the aims and activities of the Organization, and relevant for the purposes of international police cooperation as defined in Article 10(2) of the present Rules;

(b) The information shall be processed in accordance with Article 10(2) of the present Rules where it complements data already recorded in the INTERPOL Information System;

(c) The origin of the information shall be clearly identified, and the information shall be processed in a manner which enables it to be clearly distinguished from data, as defined in Article 1(2) of the present Rules, recorded in the INTERPOL Information System;

(d) Prior to its recording, the General Secretariat shall assess such information in light of Articles 11 and 12 of the present Rules;

(e) In accordance with policies put in place by the General Secretariat and Article 50 of the present Rules, such information shall be time stamped as to its time of recording, updated or corrected as relevant, and automatically deleted after a maximum retention period defined by the Executive Committee;

(f) When making available such information to National Central Bureaus, national entities, international entities, or private entities, the General Secretariat shall clearly indicate its origin and the General Secretariat's assessment of the quality and reliability of such information;

(g) Prior to using any report or other output of the General Secretariat, which is based wholly or partly on such information, National Central Bureaus, national entities, international entities, or private entities should conduct, in accordance with their applicable law, their own assessment of the quality and reliability of the information on which such output was based;

(h) Information covered under this provision may not serve as the sole basis for the application of coercive measures by any National Central Bureau, national entity, or international entity.

(2) The source of the information, covered under this Article, shall be:

(a) the General Secretariat when:

(i) publicly available information is collected by or at the initiative of the General Secretariat; or

(ii) information originates from persons or entities other than the sources referred to in Article 1(6) of the present Rules.

(b) the source referred to in Article 1(6), of the present Rules, when such information is received from such a source.

Article 48: Supplementary information and corrections

(1) If a National Central Bureau, national entity or international entity other than the one which recorded the data has specific, relevant reasons for considering that data are incorrect, it shall immediately inform the National Central Bureau which recorded the data or on whose behalf a national entity recorded them, or the international entity which recorded the data.

(2) If a National Central Bureau, national entity or international entity other than the one which recorded the data wishes to supplement them, it may send the supplementary information to the Bureau or to the international entity concerned.

(3) The recording National Central Bureau, national entity or international entity shall promptly examine the information and, if necessary, modify, correct or delete the data immediately.

Article 49: Retention period

(1) In conformity with Article 10 of the present Rules, the data may only be retained in the Organization's police databases for the time required to achieve the purpose for which they were recorded.

(2) Data shall initially be recorded for the maximum period determined by the Executive Committee for this type of data, unless a shorter retention period is set by the source or the purpose has been achieved.

(3) The retention period shall begin from the date on which the data are recorded.

(4) The suspension of a cooperation request or alert, as referred to in Articles 81 and 100 of the present Rules, shall have no bearing on the retention period of the data.

Article 50: Periodic assessments

(1) In order to reassess the purpose of processing data and their quality, in conformity with Articles 10 and 12 of the present Rules, the National Central Bureau, national entity or international entity must, on expiry of the retention period, examine the need for retaining that data and, if necessary, check that the conditions for recording them are still being met.

(2) The General Secretariat shall ask the National Central Bureau, national entity or international entity that recorded the data, at the latest six months before the expiry date, to examine the need to retain the data.

(3) The General Secretariat shall specify, in particular:

(a) if the data are connected with other data from the same National Central Bureau or the same entity;

(b) if the data are processed as part of an analysis project;

(c) if the data concern a form of serious crime or a special crime area for which the General Assembly has defined a specific retention policy implemented by the General Secretariat.

(4) If the National Central Bureau, national entity or international entity decides to retain the data, it shall specify the reasons for the retention. Data shall be recorded for a further period not exceeding the maximum retention period, unless a shorter retention period is set by the source or the purpose has been achieved.

(5) If the National Central Bureau, national entity or international entity decides that the purpose for which the data were recorded has been achieved but that retaining data in the Organization's police databases continues to be of interest for the purposes of international police cooperation, particularly if those data belong to one of the three categories mentioned above, it shall determine and justify a new purpose for recording that data. Data shall be recorded for a further period not exceeding the maximum retention period for this new purpose, unless a shorter retention period is set by the source or the purpose has been achieved.

(6) The National Central Bureau, national entity or international entity that decides to retain the data shall ensure that the conditions for recording the data continue to be met.

(7) For a given database of the Organization, the Executive Committee is empowered to waive the above requirements regarding reassessment, provided such a waiver is necessary.

Article 51: Deletion of data

(1) If the National Central Bureau, national entity or international entity decides not to retain data serving one of the purposes set in Article 10, they shall be deleted for that specific purpose.

(2) The data shall also be deleted automatically on expiry of the retention period if the National Central Bureau, national entity or international entity has not indicated the need to retain the data for the purpose they serve.

(3) When the purpose for which the data were recorded has been achieved, the National Central Bureau, national entity or international entity that recorded the data shall delete them from the police databases, unless it has decided to determine and justify a new purpose for recording them.

(4) When the General Secretariat has specific, relevant reasons for considering that the purpose for which data were recorded has been achieved or that the data no longer meet the minimum conditions for recording, it shall promptly request the National Central Bureau, national entity or international entity that recorded the data to examine the need to retain these data.

(5) When the General Secretariat deletes data recorded by a National Central Bureau, a national entity or international entity concerning a person who is the subject of an international cooperation request or an alert, it shall inform the National Central Bureau or international entity that recorded that data, and explain the reasons for its action.

(6) When data have been deleted from one of the Organization's police databases, all copies of those data contained in the INTERPOL Information System shall also be deleted, unless data are retained for a separate purpose as set out in Article 10, and subject to the prior consent of the National Central Bureau, national entity or international entity that initially recorded the data.

(7) When it is impossible to delete data because of the cost and volume of work involved, the General Secretariat shall take all appropriate steps to ensure that the data cannot be used, to prevent access to that data and their use for the purposes of a criminal investigation, or to indicate clearly that the data must be considered to be non-existent. It shall inform the Commission for the Control of INTERPOL's Files of such measures.

Article 52: Temporary retention of criminal history

(1) The National Central Bureau, national entity or international entity that withdraws an international alert or cooperation request concerning a person who has been convicted, charged, is suspected or constitutes a potential threat may choose to temporarily retain the data on this person in order to provide information about his/her criminal history.

(2) The temporary retention of the criminal history of a person who has been convicted, charged, is suspected or constitutes a threat, but who has been cleared of the charges which led to the data about him/her initially being recorded, shall be prohibited.

(3) The National Central Bureau, national entity or international entity which retains data for reference purposes shall ensure that retention is lawful under national law. The international entity shall ensure that the retention is lawful under its applicable rules.

(4) The purpose of this recording as well as the status of the person concerned shall be specified in accordance with, respectively, Articles 10 and 44(1) of the present Rules, in a manner such that the data cannot be confused with data concerning persons who are the subject of alerts or requests for international cooperation. A record shall be kept of the status initially attributed to the person concerned.

(5) These data may be retained for a period not exceeding the maximum retention period determined by the Executive Committee from the moment at which the National Central Bureau, national entity or international entity indicates that the initial purpose has been achieved, unless a shorter retention period is set by the source. On expiry of the retention period, the data shall be automatically destroyed unless the National Central Bureau, national entity or international entity decides to retain the data for the purposes of redirecting enquiries in conformity with Article 53 below.

Article 53: Retention of data for purposes of redirecting enquiries

(1) The National Central Bureau or entity that deletes data it has recorded about a person suspected, accused or convicted of criminal offences shall indicate whether it wishes to retain those data items that would allow another National Central Bureau or entity to address to it any subsequent enquiries it may have about this person.

(2) The General Secretariat may not retain, for purposes of redirecting enquiries, data it has deleted from the police databases without the express authorization from the National Central Bureau or entity that recorded those data.

(3) The only data that may be retained for purposes of redirecting enquiries are: the name of the National Central Bureau or entity that recorded the data; the reference of the recording; the person's name and forenames; the identity document number and the nature of that document; date and place of birth; and fingerprints and DNA profile.

(4) These data may be retained for a maximum retention period determined by the Executive Committee, unless a shorter retention period is set by the source.

SECTION 3: CONSULTATION

Article 54: Direct access

(1) In accordance with Article 6 of the present Rules, National Central Bureaus may directly consult the Organization's police databases, subject to the restrictions and confidentiality rules laid down by the source. National entities and international entities may also directly consult the Organization's police databases subject to the same restrictions and confidentiality rules and according to the access rights they have been granted.

(2) In accordance with Article 36(1,n), the type of data that can be directly consulted is specified in the list of the general characteristics of this database.

Article 55: Interconnection

(1) Interconnection operations must meet all of the following conditions:

(a) The purpose, the nature and the scope of the interconnection are specified, explicit and conform to the aims and activities of the Organization;

(b) The interconnection is of interest for the purposes of international police cooperation;

(c) The information system to be interconnected offers a level of security at least equivalent to that of the INTERPOL Information System;

(d) The interconnection allows for compliance with the processing conditions established by the sources of data contained in the INTERPOL Information System and in the information system to be interconnected;

(e) The interconnection allows the National Central Bureau, national entity or international entity that entered the data into the INTERPOL Information System, and the General Secretariat, to be notified immediately of any element deriving from the interconnected data that is likely to be of interest for the purposes of international police cooperation.

(2) All requests for interconnection from a national entity must be sent through its National Central Bureau.

(3) The General Secretariat shall submit to the Executive Committee for approval all requests for interconnection. It shall provide:

(a) a copy of the request for interconnection it received, specifying the person who will be responsible for overseeing the interconnection at the National Central Bureau, national entity or international entity;

(b) the assessment of the request by the General Secretariat as well as the financial implications of that request for the Organization;

(c) the outcome of any tests conducted by the General Secretariat;

(d) the opinion of the Commission for the Control of INTERPOL's Files if the database contains or is linked to personal data.

(4) If the Executive Committee authorizes the interconnection, the General Secretariat shall give prior notification to the sources of the data recorded in the database to be interconnected. The Secretariat shall specify the conditions of interconnection.

(5) The General Secretariat shall keep an updated register of interconnection operations which specifies the conditions of each operation. National Central Bureaus may consult this register at any time. International entities may also consult this register according to the access rights they have been granted.

(6) The Executive Committee shall report to the General Assembly each year the authorizations it has granted for interconnection operations.

Article 56: Downloading for the purposes of international police cooperation

(1) All downloading operations must meet all the following conditions:

(a) the purpose of the downloading is specified, explicit and conform to the aims and activities of the Organization;

(b) the request is of interest for the purposes of international police cooperation;

(c) an interconnection operation cannot be carried out due to its cost and the functional or technical characteristics of the information system to be interconnected;

(d) the information system of the National Central Bureau, national entity or international entity offers a level of security at least equivalent to that of the INTERPOL Information System;

(e) the conditions established by the sources for the processing and use of the downloaded data are strictly observed;

(f) the downloading operation is for a set period not exceeding six months;

(g) downloaded data are updated at least once a week, including when such updating implies the deletion of data;

(h) the data are not copied within the information system into which they are downloaded;

(i) the downloaded data must systematically be deleted when the purpose for which they were downloaded has been achieved, and at the very latest when the aforementioned period of six months has expired;

(j) the National Central Bureau, national entity or international entity that downloads data immediately notifies the National Central Bureau, national entity or international entity that entered the data into the INTERPOL Information System, and the General Secretariat, of any item derived from the downloaded data that is likely to be of interest for the purposes of international police cooperation.

(2) All downloading requests from a national entity must be sent through its National Central Bureau.

(3) The General Secretariat shall be empowered to authorize a downloading operation, subject to:

(a) compliance with the conditions above; and

(b) written assurances provided by the National Central or international entity that requested to carry out the downloading operation, by which it undertakes to comply with those conditions, the purpose of the downloading, its nature and its scope; and

(c) the designation of a person to be responsible for overseeing the downloading at the National Central Bureau, national entity or international entity.

(4) If, for technical or other reasons, the General Secretariat cannot comply with one or more of the processing conditions linked to the data to be downloaded, it shall not authorize the downloading of the said data.

(5) The General Secretariat shall notify National Central Bureaus and international entities of any downloading operation it has authorized. It shall specify all the conditions of downloading, particularly the characteristics of the information system of the National Central Bureau or international entity it has authorized to proceed with the downloading. With effect from the date of

notification by the General Secretariat, a National Central Bureau, a national entity or an international entity has 15 days to signify its opposition to any possibility of processing by the requesting National Central Bureau or entity of the data that it entered into the INTERPOL Information System. At the end of the prescribed period, the General Secretariat shall be empowered to proceed with the downloading, with the exception of data about which an opposition has been signified.

(6) The General Secretariat shall inform the Executive Committee of the downloading authorization it has granted by providing:

(a) its assessment of the request as well as the financial implications for the Organization;

(b) the characteristics of the information system of the National Central Bureau or national entity or international entity into which the data were downloaded;

(c) a copy of the written assurances provided by the National Central Bureau or international entity which requested to carry out a downloading operation;

(d) the opinion of the Commission for the Control of INTERPOL's Files if the downloaded data contained personal data or were linked to such data.

(7) The General Secretariat shall be responsible for checking that the conditions for downloading are being met throughout the period for which the downloading has been authorized. It shall take all necessary and appropriate measures to perform these checks.

(8) The General Secretariat shall keep a register of the data downloaded which specifies the conditions of each downloading operation. National Central Bureaus may consult this register at any time. International entities may also consult this register according to the access rights they have been granted.

Article 57: Indirect access

(1) When a police database cannot be consulted directly or an international entity only has indirect access to a database, the General Secretariat shall determine the procedures for consulting that database and inform the National Central Bureaus of them. It shall also inform international entities according to the access rights they have been granted.

(2) When a police database can be consulted directly, the General Secretariat may authorize a request for indirect access to the data contained in that database in the following cases:

(a) the international entity does not have direct access rights, or

(b) direct access is temporarily inoperative, or

(c) the request is specific or complex and the data cannot be obtained through direct consultation.

(3) All requests for indirect access from a national entity must be submitted through its National Central Bureau.

(4) When examining a request for indirect access, the General Secretariat shall ensure that:

(a) the request has been made by a National Central Bureau, a national entity, an international entity or a private entity;

(b) if made by an international entity or a private entity, the request corresponds to the purpose for which access to the INTERPOL Information System was granted;

(c) the request is clear and reasoned;

(d) the National Central Bureau or international entity that recorded data likely to correspond to the request has not imposed any access restrictions on the requesting National Central Bureau, international entity or private entity.

Article 58: Access restrictions

(1) In accordance with Article 7(1) of the present Rules, any National Central Bureau or international entity may, at any time, place general restrictions on access by other National Central Bureaus, international entities or private entities to the data it has recorded in a police database. General access restrictions placed by a National Central Bureau shall apply to the data recorded by the national entities it has authorized.

(2) Any National Central Bureau or international entity may, at any time, place additional restrictions on access by other National Bureaus, international entities or private entities to recorded data concerning a person, object or event.

(3) National Central Bureaus and international entities may not place access restrictions applicable solely to the national entities of other National Central Bureaus. Any restrictions on access by a National Central Bureau shall apply to all the national entities that it has authorized.

(4) Access restrictions to data shall apply regardless of the method used to consult the police database.

(5) When a National Central Bureau or an international entity consults a database and it cannot access the data that may match its search, the General Secretariat may forward the request to the National Central Bureau or international entity that placed the access restriction.

(6) Messages for which a National Central Bureau or international entity has authorized the recording in one of the Organization's databases shall be considered to be restricted to their initial recipients, unless otherwise specified by the said Bureau or entity.

(7) Access restrictions may not be lifted by the General Secretariat except in urgent situations, according to the applicable procedure, or when the data have become public.

(8) Access restrictions are confidential data that shall be processed in accordance with Article 112 of the present Rules.

Article 59: Disclosure of data subject to restrictions

The disclosure of data subject to restrictions may only be carried out in the urgent situations referred to in Article 26(2) of the present Rules and according to the following procedure:

(a) The General Secretariat shall notify the National Central Bureau, national entity or international entity that recorded the said data, that the conditions set out in Article 26(2) of the present Rules have been met, and shall set a deadline, proportionate to the threat, for the said National Central Bureau or entity to object to the removal of the restrictions;

(b) All requests to a national entity concerning the removal of restrictions must be sent through its National Central Bureau;

(c) The restrictions will be considered to be lifted upon expiry of the deadline set by the General Secretariat and in the absence of an express objection by the National Central Bureau, national entity or international entity that recorded the restricted data relating to the threat;

(d) The General Secretariat shall inform the Executive Committee and the Commission for the Control of INTERPOL's Files as soon as possible that it has applied this emergency procedure.

Article 60: Access by third parties

(1) The General Secretariat may process requests for access submitted by international organizations or legal persons governed by private law with which the Organization is considering establishing relations for cooperation in data processing.

(2) When a third party requests access to data contained in a police database, the General Secretariat may forward the data only with the express prior authorization of the source of the data.

Article 61: Disclosure of data to the public

(1) The General Secretariat shall request the opinion of the Commission for the Control of INTERPOL's Files on any policy that it may, in accordance with the conditions set out in paragraph 2 below, decide to adopt regarding disclosure to the public of data processed in the INTERPOL Information System, whenever the processing of personal data is concerned.

(2) Data processed in the INTERPOL Information System may only be disclosed to the public if all the following conditions are met:

(a) The disclosure is for at least one of the following purposes:

(i) to alert the public;

(ii) to request help from the public;

(iii) for any other purpose intended to promote international police cooperation;

(b) The source of the data has authorized the disclosure beforehand, including details of the type of data to be disclosed, the method of disclosure, and the potential recipients of the disclosure, and the source has indicated any specific conditions concerning the disclosure;

(c) The disclosure complies with the aims and activities of the Organization and respects the basic rights of the persons who are subjects of international police cooperation;

(d) The disclosure is not such that it might prejudice the Organization's image or interests, or those of its Members;

(e) The disclosure does not concern an offender or an alleged offender who, at the time of the offence in question, was considered to be a minor under the law applicable in the country of the National Central Bureau or of the international entity which entered the data in the system, unless that National Central Bureau or international entity and the General Secretariat consider that such disclosure is essential to international police cooperation, and if the disclosure in question complies with the applicable principles of the national laws and of international law.

(3) If a notice or the data it contains is disclosed by a National Central Bureau, a national entity or an international entity other than the source of the data, in addition to the conditions listed in paragraph 2 above, the following conditions shall be met:

(a) The General Secretariat shall have first authorized such disclosure;

(b) The data contained in the notice shall be copied identically and be updated regularly to ensure they remain accurate.

SECTION 4: USE OF DATA

Article 62: Conditions of use

All National Central Bureaus, national entities and international entities about to use data processed in the INTERPOL Information System shall determine the following:

(a) the accuracy and relevancy of the data;

(b) the purpose for which they are about to use the data;

(c) any special conditions of use;

(d) any access restrictions placed on these data applicable to another National Central Bureau or another international entity to which they are to be forwarded.

Article 63: Verification of the accuracy and relevance of data

(1) All National Central Bureaus, national entities and international entities about to use data processed in the INTERPOL Information System for the purposes of applying coercive measures, including but not limited to detention, arrest, or restriction of movement, must ensure that these data are still accurate and relevant. Notwithstanding the above, any such measures permitted under national law and applicable international treaties may be taken prior to or while the data verification process is carried out.

(2) A National Central Bureau shall conduct the necessary checks directly with the National Central Bureau that recorded the data or, if the data were recorded by a national entity, with the National Central Bureau of this national entity. If the data were recorded by an international entity, it shall conduct the necessary checks with the General Secretariat.

(3) A national entity shall conduct these checks through its National Central Bureau.

(4) An international entity shall conduct these checks with the National Central Bureau or international entity solely through the General Secretariat, unless it has been granted access rights.

Article 64: Use of data for a criminal investigation purpose other than the initial purpose or for an administrative purpose

(1) In accordance with Article 10(6) of the present Rules, all National Central Bureaus, national entities or international entities about to use data for a criminal investigation purpose other than the specific purpose of international police cooperation for which the data were initially recorded in the Organization's police databases, or for an administrative purpose as specified by the source of the data pursuant to paragraph (2) below, or in the absence of such specification, under the applicable law of the entity intending to use the data, shall ensure that this purpose and use:

(a) complies with the aims and activities of the Organization;

(b) is not incompatible with the initial purpose;

(c) is lawful under the applicable law.

(2) Each source of data shall have the right to specify which purposes, other than those listed under Article 10(2) of the present Rules, are considered an administrative purpose under its applicable law.

(3) National Central Bureaus or entities intending to use data as described in paragraph (1) above shall inform in advance the source of the data, as follows:

(a) A National Central Bureau shall directly inform the National Central Bureau that recorded the data or, if the data were recorded by a national entity, the National Central Bureau of this national entity. If the data were recorded by an international entity, it shall inform the General Secretariat;

(b) A national entity shall inform the National Central Bureau, national entity or international entity that recorded the data through its National Central Bureau;

(c) An international entity shall inform the National Central Bureau, national entity or international entity that recorded the data through the General Secretariat, unless it is an international entity with powers of investigation and prosecution in criminal matters which, in conformity with Article 27(5,f) of the present Rules, has been authorized to send the data directly as a message.

(4) With effect from the date of notification, the source has 10 days to signify its opposition or to request additional information or time to respond to the request to use the data for the envisaged purpose. This period may be reduced by the General Secretariat in urgent cases.

Article 65: Use of data for administrative purposes *[deleted]*

Article 66: Special conditions for use

(1) In accordance with Article 45 of the present Rules, when any data are consulted, the General Secretariat shall draw attention to the special conditions for use established by a National Central Bureau, a national entity or an international entity when the data were recorded, in particular any conditions relating to the use of data as evidence in criminal proceedings.

(2) Any National Central Bureau, national entity or international entity which is about to use data recorded in a police database shall observe the special conditions for use established by the National Central Bureau, national entity or international entity that recorded them.

(3) The General Secretariat shall ensure that any National Central Bureau, national entity or international entity that consults the data is aware of those special conditions for use, so that it may take any necessary measures to ensure they are observed.

Article 67: Forwarding data

(1) Prior to forwarding to another National Central Bureau or another international entity data contained in the Organization's police databases or data received by means of a message, a National Central Bureau or international entity shall check with the General Secretariat or the National Central Bureau, national entity, or international entity which recorded these data or sent these data by means of a message that the data are not subject to restrictions:

   (a) A National Central Bureau shall conduct the necessary checks directly with the National Central Bureau that recorded or sent the data or, if the data were recorded or sent by a national entity, with the National Central Bureau of this national entity. If the data were recorded or sent by an international entity, it shall conduct the necessary checks with the General Secretariat;

   (b) An international entity shall conduct the necessary checks with the National Central Bureau, national entity, or international entity solely through the General Secretariat, unless it is an international entity with powers of investigation and prosecution in criminal matters which has been authorized, in application of Article 27(5,f) of the present Rules, to send data directly by means of a message.

(2) Prior to forwarding particularly sensitive data contained in the Organization's police databases or in a message it has received, a National Central Bureau, international entity or the General Secretariat shall ensure that the data to be forwarded are relevant and of particularly important criminalistic value to achieve the aims of the Organization and are strictly necessary for the purposes of the processing as provided in Article 10(2) of the present Rules.

(3) When forwarding data, the National Central Bureau or international entity and the General Secretariat shall, in cases of indirect access, indicate:

   (a) the source of the data;

   (b) the specific conditions for use established by the source;

   (c) the level of confidentiality of the data;

   (d) the date they were recorded and their retention period in the police databases;

   (e) the person's status and the type of action to be taken regarding him/her, in the case of personal data;

   (f) any specific methods for processing the data.

(4) It shall send an exact copy of the forwarded data to the source of the data if it deems it necessary or if the source so requires.

(5) In accordance with Article 58(6) of the present Rules, the General Secretariat may not forward a message it has received to a National Central Bureau or an international entity which is not a recipient without the prior consent of the National Central Bureau or the international entity that originally sent it.

SECTION 5: SPECIFIC RULES RELATING TO CRIME ANALYSIS FILES

Article 68: Analysis files

(1) Analysis files are temporary databases created for crime-analysis purposes, in accordance with a list of general characteristics drawn up on the basis of Article 36(1) of the present Rules and in consultation with the National Central Bureaus, national entities and international entities that may be involved in the crime analysis project concerned.

(2) The processing principles and conditions for recording data in the Organization's databases set out in the present Rules shall be applicable to analysis files, subject to the provisions below.

(3) Analysis files shall be created by the General Secretariat for an initial period not exceeding five years.

(4) The General Secretariat shall inform the Executive Committee about any crime-analysis project involving the creation of an analysis file, and shall provide:

(a) the reasons that led it to develop this project, as well as the financial implications of such a project;

(b) the list of the National Central Bureaus, national entities and international entities that may be involved in the project;

(c) the list of the general characteristics of the analysis file constituting its legal framework;

(d) the opinion of the Commission for the Control of INTERPOL's Files, if the analysis file contains personal data or is linked to such data.

(5) The Executive Committee may refuse or cancel the creation of an analysis file, if it considers that the requirements set by the present Rules are not met.

(6) The creation of an analysis file, as well as its purpose and the applicable legal framework, shall immediately be notified to the National Central Bureaus and international entities that may be involved in the project. Subsequent participation by a National Central Bureau, a national entity or an international entity in the crime analysis project is subject to the agreement of all the National Central Bureaus international entities already participating in the project.

(7) National Central Bureaus shall be responsible for making necessary notifications to their respective national entities.

(8) The General Secretariat shall submit any proposal to extend an analysis file for a period not exceeding five years to the Executive Committee for approval.

Article 69: Use of analysis files

(1) Access to analysis files shall be restricted to authorized departments or members of staff of the General Secretariat involved in the crime analysis and to whom specific access has been granted.

(2) The General Secretariat shall be entitled, when required, to authorize staff of National Central Bureaus, national entities and international entities participating in the project and involved in the crime analysis to access a given analysis file, and to determine the extent of their access and processing rights. Access and processing rights shall be granted to staff of national entities in consultation with the National Central Bureaus concerned.

(3) The analysis files may or may not be connected to the Organization's police databases, depending on the purpose of the files in question and the required security and confidentiality conditions.

(4) Data recorded in an analysis file may be copied into a database of the Organization, or, conversely, data recorded in a database of the Organization may be copied into an analysis file provided that the data meet the minimum conditions for recording information in the said database, and that the copying is subject to the express consent of the National Central Bureau, national entity or international entity that supplied the data.

(5) If the data or other items of information recorded in an analysis file are such that they might allow updates to one or several of the Organization's other databases or conversely if the data recorded in other databases might allow updates to one or several analysis files, the General Secretariat must take all appropriate measures to that end.

Article 70: Additional conditions for recording data for criminal analysis purposes

(1) Data referred to in Article 1(2) of the present Rules, as well as other items of information, including publicly available information, that may be necessary for crime analysis, may be recorded in analysis files.

(2) Data and other items of information recorded in analysis files shall be retained for a maximum retention period determined by the Executive Committee, unless a shorter retention period is set by the source or the crime-analysis file which contains them is closed earlier.

(3) If the data are recorded both in an analysis file and in one of the Organization's police databases, the purposes for recording the data shall be specified in a manner such that the data cannot be confused.

(4) When recording in an analysis file any data or other items of information about a person who is the subject of international police cooperation, the status of that person shall be specified with reference to the following list, which shall only be used in the context of criminal analysis:

(a) The statuses listed in Article 44(1) of the present Rules;

(b) Other statuses below created in application of Article 44(2) of the present Rules:

(i) Associate: person who has sporadic or regular contact with a person of interest in a criminal investigation, and/or against whom criminal proceedings have been initiated;

(ii) Person of interest: person who can provide information about an ordinary-law crime.

Article 71: Crime analysis reports

(1) Crime analysis reports prepared for analysis files must:

(a) make a clear distinction between the information obtained by the General Secretariat and the conclusions that the General Secretariat has drawn from that information;

(b) indicate the sources of the information cited, the status of the persons mentioned and the date when the analysis was made;

(c) specify that, prior to making any use of such reports and the data and other items of information they contain, the General Secretariat and the sources of the data should be consulted to ascertain the rights and restrictions attaching to them.

(d) specify where any information or conclusions that the General Secretariat has drawn from that information are based wholly or partially on publicly available information, as well as the time stamp and origin of that information.

(2) Crime-analysis reports shall be disclosed to the National Central Bureaus, national entities and international entities participating in the crime analysis project concerned. Crime-analysis reports may be disclosed to other National Central Bureaus, national entities and international entities, subject to authorization by the General Secretariat and any access restrictions that may be determined by the sources of the data contained in the reports. Disclosure must comply with the confidentiality level assigned to the analysis file by the General Secretariat, as well as any other applicable security measures.

(3) The crime-analysis reports may be retained for a maximum retention period determined by the Executive Committee after the completion of the analysis project concerned, provided that they are used in a manner that is relevant and in compliance with the processing rules set out in the present Rules.

Article 72: Completion of crime analysis projects

(1) When a crime analysis project is completed:

(a) the analysis files concerned, as well as the data and other items of information recorded in them, must be destroyed;

(b) the crime analysis report may be retained provided that steps are taken to prevent any use which is not relevant or is contrary to the processing rules set out in the present Rules.

(2) Disclosure of a crime analysis report or any of the data it contains must conform to any restrictions that may have been imposed by their sources on the data it contains and any other measures attaching to it concerning security or confidentiality.

CHAPTER II: NOTICES AND DIFFUSIONS

SECTION 1: PROVISIONS COMMON TO NOTICES

Article 73: INTERPOL notices system

(1) The INTERPOL notices system consists of a set of colour-coded notices published for specific purposes, and special notices published within the framework of specific cooperation not covered by the previous categories of notices.

(2) A category of notices or special notices may only be created with the approval of the General Assembly which, if the notice contains or is linked to personal data, shall have obtained the opinion of the Commission for the Control of INTERPOL's Files.

(3) The conditions for publishing notices are defined for each category of notice or special notice. These conditions are at least identical to the general conditions required for recording these data in the Organization's databases.

(4) The conditions for publishing each category of notice are defined below. The conditions for publishing each category of special notice are specified in an agreement.

Article 74: Role of the General Secretariat

(1) The General Secretariat shall be responsible for publishing INTERPOL notices on behalf of the Organization.

(2) In particular, it is responsible for:

(a) checking the compliance of all notice requests with the present Rules and publishing, as soon as possible, any notice requests it deems to be in compliance;

(b) simultaneously recording any published notices in a database of the Organization for direct consultation by National Central Bureaus, national entities and international entities according to the access rights they have been granted;

(c) translating any notices into the Organization's working languages according to the directives decided upon by the General Assembly;

(d) assisting National Central Bureaus and international entities in the event of a positive query result;

(e) ensuring that published notices continue to comply with the conditions for their publication and are regularly assessed by the National Central Bureau or international entity that requested their publication. To that end, the General Secretariat shall review published notices on a regular basis and shall consult the National Central Bureaus and international entities that requested their publication, as well as the other National Central Bureaus.

Article 75: Structure of INTERPOL notices

(1) The General Secretariat, in consultation with the National Central Bureaus, or with their representatives on the advisory bodies set up for the purpose, shall define and modify, when necessary, the structure of each category of notices, in due compliance with the conditions for their publication, as well as any other directives or decisions taken by the General Assembly or by the Executive Committee.

(2) Without prejudice to the principles set out in Title 1 of the present Rules, the international entity and the Organization shall define the structure of special notices in an agreement.

(3) A notice may contain data from different sources if all the following conditions have been met:

(a) the sources have agreed to the processing;

(b) the processing is of specific interest to the requesting National Central Bureau or international entity for this cooperation request or alert;

(c) the data are clearly identified as having been submitted by different sources;

(d) the processing does not incur significant additional costs.

Article 76: Requests for the publication of notices

(1) Notice requests shall be submitted in at least one of the Organization's working languages.

(2) Prior to requesting the publication of a notice, the National Central Bureau or international entity shall ensure:

(a) the quality and lawfulness of the data it provides in support of its request;

(b) that the conditions attached to its request for publication are met;

(c) that the data are of interest for the purposes of international police cooperation;

(d) that its request complies with INTERPOL's rules, specifically with Articles 2(1) and 3 of the Constitution, as well as with the obligations imposed on the requesting entity under international law.

Article 77: Examination of requests by the General Secretariat

(1) All notice requests shall be examined by the General Secretariat for compliance with the present Rules.

(2) The General Secretariat may not publish a notice on behalf of the Organization if:

(a) the data provided do not meet the conditions for publishing a notice;

(b) publication of the notice is not, in the case in point, of interest for the purposes of international police cooperation. This interest is assessed in light of the possibility that the request could be processed by all the Organization's Members;

(c) publication of the notice could prejudice the Organization's or its Members' interests.

(3) While requests for notices are being examined by the General Secretariat, they are temporarily recorded in a database of the Organization. An additional indication must be inserted so that, when consulted, these requests can be identified as such and not be confused with published notices.

Article 78: Incomplete or non-compliant requests for notices

(1) When a request is incomplete, the requesting National Central Bureau or international entity shall provide, at the earliest opportunity and after consultation with the General Secretariat, all additional data required to publish the notice.

(2) The General Secretariat shall propose to the requesting National Central Bureau or international entity, whenever possible, the publication of other notices when the data provided are insufficient to allow publication of the requested notice but correspond to the purposes and conditions for publication of another notice.

(3) The General Secretariat shall propose to the requesting National Central Bureau or international entity, whenever possible, that it circulates a diffusion when the request is not intended for all the Organization's Members, or when the data provided are insufficient for the requested notice to be published but correspond to the purpose and conditions for recording a diffusion.

Article 79: Publication of notices

(1) Notices shall be published by the General Secretariat for the attention of all National Central Bureaus as follows:

(a) National Central Bureaus shall be informed of the publication of a notice on the day of its publication;

(b) National Central Bureaus shall be able to directly consult all published notices on a police database of the Organization, subject to the interim measures referred to in Article 129 of the present Rules.

(2) Notices may also be consulted by:

(a) national entities, according to the access authorizations they have been granted by their respective National Central Bureaus;

(b) international entities, when expressly provided for in the agreement concluded with the Organization.

(3) Notwithstanding Article 58 of the present Rules, any National Central Bureau or international entity which requests a notice shall agree not to place restrictions on access to the data it provides by any National Central Bureau or national entity that the said National Central Bureau has authorized to consult notices. It shall retain the possibility of placing restrictions on access to the data it provides by international entities that do not have powers of investigation and prosecution in criminal matters.

Article 80: Implementation of notices

(1) National Central Bureaus shall forward to:

(a) all relevant national authorities, as soon as possible and in accordance with their national laws, all the data contained in the notices they receive, as well as the updates regarding those notices;

(b) the requesting National Central Bureau or international entity, as well as the General Secretariat, all available data concerning the person or purpose for which the notice was published, in particular, whenever those data could enable the purpose of the notice to be achieved. A national entity must submit those data via its National Central Bureau;

(c) the General Secretariat any information that may give rise to doubts about the conformity of a notice with the present Rules.

(2) The National Central Bureau or international entity which originally requested the notice shall:

(a) continue to ensure that the data it has provided in the notice remains accurate and relevant;

(b) forward to the General Secretariat any data that would modify the content of the published notice, and assess whether the modifications require the said notice to be withdrawn.

Article 81: Suspension, withdrawal or cancellation of a notice

(1) The requesting National Central Bureau or international entity can suspend its cooperation request or its alert for a period not exceeding six months. It shall indicate the reasons for this suspension to the General Secretariat, which will then suspend the notice.

(2) The National Central Bureau or international entity requesting a notice shall withdraw its cooperation request or its alert and ask the General Secretariat to cancel the notice immediately:

(a) once the purpose of this request or alert has been achieved; or

(b) if this request or alert is linked to one or several other requests or alerts whose purpose has been achieved and without which it cannot be maintained; or

(c) if it no longer wishes to maintain the request; or

(d) if the notice no longer meets the conditions for publication of the notice.

(3) The General Secretariat shall cancel a notice if:

(a) the purpose of the cooperation request or the alert on the basis of which the notice was published has been achieved, and this information has been confirmed by the source National Central Bureau or international entity; or

(b) if this request or alert is linked to one or several other requests or alerts whose purpose has been achieved and without which it cannot be maintained; or

(c) the notice no longer meets the conditions for publishing a notice; or

(d) the National Central Bureau or international entity that requested the notice obtains data allowing it to carry out the required action but has not taken any steps to this end and, after being consulted, has not provided reasonable grounds for its lack of action.

SECTION 2: PROVISIONS SPECIFIC TO RED NOTICES

Article 82: Purpose of red notices

Red notices are published at the request of a National Central Bureau or an international entity with powers of investigation and prosecution in criminal matters in order to seek the location of a wanted person and his/her detention, arrest or restriction of movement for the purpose of extradition, surrender, or similar lawful action.

Article 83: Specific conditions for publication of red notices

(1) Minimum criteria

(a) Red notices may be published only if the following cumulative criteria are met:

(i) The offence concerned is a serious ordinary-law crime.

Red notices may not be published for the following categories of offences:

- offences that in various countries raise controversial issues relating to behavioural or cultural norms;
- offences relating to family/private matters;
- offences originating from a violation of laws or regulations of an administrative nature or deriving from private disputes, unless the criminal activity is aimed at facilitating a serious crime or is suspected of being connected to organized crime.

The General Secretariat shall keep, update and share with National Central Bureaus and international entities a non-exhaustive list of specific offences that fall within the above categories.

(ii) Penalty threshold:

- if the person is sought for prosecution, the conduct constituting an offence is punishable by a maximum deprivation of liberty of at least two years or a more serious penalty;
- if the person is sought to serve a sentence, he/she is sentenced to at least six months of imprisonment and/or there is at least six months of the sentence remaining to be served.

(iii) The request is of interest for the purposes of international police cooperation.

(b) The General Secretariat may decide to publish a red notice where the criteria in (i) and/or (ii) above are not met if, following consultation with the requesting National Central Bureau or international entity, it considers that publication of the requested red notice would be of particular importance to international police cooperation.

(c) Several offences: if the request includes several offences, the red notice may be published for all offences that meet INTERPOL's Rules provided that at least one offence meets the above criteria.

(2) Minimum data

(a) Identity particulars:

Red notices may be published only when sufficient identifiers have been provided. Sufficient identifiers will be considered to include at least one of the following two combinations of identifiers:

(i) family name, forename, sex, date of birth (at least the year) and one of the following identifiers:

- physical description; or
- DNA profile; or
- fingerprints; or
- data contained in identity documents (e.g. passport, national identity card).

(ii) photograph of good quality with some additional data (e.g. alias, name of the parent(s), further physical description, DNA profile, fingerprints, etc.).

(b) Judicial data:

Red notices may be published only when sufficient judicial data has been provided. Sufficient judicial data will be considered to include at least:

(i) summary of facts of the case, which shall provide a succinct and clear description of the criminal activities of the wanted person, including the time and location of the alleged criminal activity; and

(ii) charge(s); and

(iii) law(s) covering the offence (whenever possible, and subject to national law or the rules governing the operation of the international entity, the requesting National Central Bureau or international entity shall provide the wording of the relevant penal provision(s)); and

(iv) maximum penalty possible, sentence imposed, or sentence remaining to be served; and

(v) reference to a valid arrest warrant or judicial decision having the same effect (whenever possible, and subject to national law or the rules governing the operation of the international entity, the requesting National Central Bureau or international entity shall provide a copy of the arrest warrant or judicial decision).

Article 84: Assurances provided by the requesting National Central Bureau or international entity

The requesting National Central Bureau or international entity shall ensure that:

(a) the authority which issued the arrest warrant or handed down the judicial decision has the necessary power;

(b) the red notice request has been coordinated with the relevant authorities responsible for extradition, and assurances have been given that extradition will be sought upon arrest of the person, in conformity with national laws and/or the applicable bilateral and multilateral treaties;

(c) if the arrest warrant has not been issued by a judicial authority, the laws of the requesting country or the rules governing the operation of the international entity provide for a mechanism of appeal before a judicial authority.

Article 85: Provision of documents that could support extradition or surrender proceedings

When it considers it useful and appropriate, the requesting National Central Bureau or international entity shall provide the General Secretariat with additional documents that could support extradition or surrender proceedings. The General Secretariat could serve as a repository for such documents and provide them upon request to the relevant countries.

Article 86: Legal review by the General Secretariat

The General Secretariat shall conduct a legal review of all red notices prior to their publication to ensure compliance with INTERPOL's Constitution and Rules, in particular with Articles 2 and 3 of INTERPOL's Constitution.

Article 87: Steps to be taken following the location of the person

If a person who is the subject of a red notice is located, the following steps shall be taken:

(a) The country where the person has been located shall:

(i) immediately inform the requesting National Central Bureau or international entity and the General Secretariat of the fact that the person has been located, subject to limitations deriving from national law and applicable international treaties;

(ii) take all other measures permitted under national law and applicable international treaties, such as provisionally arresting the wanted person or monitoring or restricting his/her movement.

(b) The requesting National Central Bureau or international entity shall act immediately once it has been informed that the person has been located in another country and, in particular, shall ensure the swift transmission – within the time limits defined for the case in question – of data and supporting documents requested by the country where the person was located or by the General Secretariat.

(c) The General Secretariat shall provide assistance to the relevant National Central Bureaus or international entities by, *inter alia*, facilitating the transfer of documents related to the provisional arrest or the extradition procedures in accordance with the relevant national laws and international treaties.

SECTION 3: PROVISIONS SPECIFIC TO OTHER NOTICES

Article 88: Blue notices

(1) Blue notices are published in order to:
   (a) obtain information on a person of interest in a criminal investigation, and/or
   (b) locate a person of interest in a criminal investigation, and/or
   (c) identify a person of interest in a criminal investigation.

(2) Blue notices may only be published under the following conditions:
   (a) The subject of the notice has been convicted or charged, or is a suspect, a witness or a victim;
   (b) Additional information on the possible criminal history, location or identity of the person or any other information relevant to the criminal investigation is sought;
   (c) Sufficient data relating to the criminal investigation or the person are provided to allow the cooperation requested to be effective.

(3) A blue notice may only be published if it contains sufficient identifiers. Sufficient identifiers mean at least:
   (a) If the person is identified:
      (i) either the family name, forename, sex, date of birth (at least the year), along with the physical description, DNA profile, fingerprints or data contained in identity documents (passport or national identity card, for example); or
      (ii) a photograph of good quality, along with at least one identifier such as an alias, the name of one of the parents, or a specific physical characteristic not visible in the photograph.
   (b) If the person is unidentified:
      (i) a photograph of good quality, and/or
      (ii) fingerprints, and/or
      (iii) DNA profile.

Article 89: Green notices

(1) Green notices are published to warn about a person's criminal activities.

(2) Green notices may only be published under the following conditions:
   (a) The person is considered to be a possible threat to public safety;
   (b) This conclusion has been drawn from an assessment by a national law-enforcement authority or an international entity;
   (c) This assessment is based on the person's previous criminal conviction(s) or other reasonable grounds;
   (d) Sufficient data concerning the threat are provided for the warning to be relevant.

(3) A green notice may only be published if it provides sufficient identifiers. Sufficient identifiers mean at least:
   (a) either the family name, forename, sex, date of birth (at least the year), along with the physical description, DNA profile, fingerprints or data contained in identity documents (passport or national identity card, for example); or
   (b) a photograph of good quality, along with at least one identifier such as an alias, the name of one of the parents, or a specific physical characteristic not visible in the photograph.

(4) The National Central Bureaus and national entities that receive green notices shall take the appropriate measures, in conformity with their national laws.

Article 90: Yellow notices

(1) Yellow notices are published to locate a missing person or to identify a person unable to identify himself/herself.

(2) Yellow notices may only be published under the following conditions:
   (a) The person's disappearance or discovery has been reported to and recorded by the police;
   (b) The whereabouts of the missing person or the identity of the discovered person are unknown to the police;
   (c) If the person is an adult, applicable national privacy laws do not prevent a request being made;
   (d) Sufficient data on a person or the circumstances surrounding the disappearance or discovery of the person are provided for his/her identification.

(3) A yellow notice may only be published if it provides sufficient identifiers. Sufficient identifiers mean at least:
   (a) If it concerns a missing person:
      (i) the family name, forename, sex, date of birth (at least the year); and
      (ii) physical description, a photograph of good quality, DNA profile or fingerprints;

(b) If it concerns a person who is unable to identify him/herself:

(i) physical description, sex of the person; and

(ii) photograph of good quality, fingerprints or DNA profile.

Article 91: Black notices

(1) Black notices are published to identify dead bodies.

(2) Black notices may only be published under the following conditions:

(a) the discovery of a dead body has been recorded by the police;

(b) this dead body has not been identified;

(c) enough data on this dead body or the circumstances surrounding its discovery are provided for its identification.

(3) A black notice may only be published if it provides sufficient identifiers. Sufficient identifiers mean at least:

(a) a photograph of good quality, and/or

(b) fingerprints, and/or

(c) DNA profile.

Article 92: Purple notices

(1) Purple notices are published in order to:

(a) warn about modi operandi, objects, devices or concealment methods used by offenders, and/or

(b) request information on offences to resolve them or assist in their investigation.

(2) A purple notice may only be published under the following conditions:

(a) If the facts are no longer under investigation:

(i) the modus operandi is known in detail, is complex or different from other identified modi operandi for similar offences;

(ii) the publication of the notice is intended to prevent these offences from being repeated;

(iii) the request includes enough data on the modus operandi, objects, equipment or hiding places used by perpetrators of these crimes to allow effective prevention;

(iv) the request provides sufficient identifiers for matches to be made with similar offences in order to resolve them.

(b) If the facts are still under investigation:

(i) they are serious offences;

(ii) the offences draw the attention of the Organization's Members to a specific modus operandi, object, device or concealment method;

(iii) the request includes enough data on this modus operandi and these objects, equipment or hiding places for matches to be made.

Article 93: Orange notices

(1) Orange notices are published to notify about an event, a person, an object, a process or a modus operandi representing an imminent threat to public safety and likely to cause serious damage to property or injury to persons.

(2) Orange notices may only be published under the following conditions:

(a) In the case of a person:

(i) he/she is considered to represent an imminent threat to public safety, or is preparing to commit, or is imminently about to commit a particularly serious ordinary-law crime;

(ii) this conclusion is based on an assessment by a national law-enforcement authority or an international entity;

(iii) this assessment is based on the person's previous criminal conviction(s) and/or other reasonable grounds;

(b) In the case of an object, event or modus operandi:

(i) it is considered an imminent threat to public safety;

(ii) this conclusion is based on an assessment by a national law-enforcement authority.

(3) An orange notice may only be published if sufficient data relating to the imminent threat are provided for the alert to be relevant.

(4) The National Central Bureaus and national entities that receive orange notices shall take the appropriate measures, in conformity with their national laws.

(5) When the threat which led to the publication of an orange notice is no longer imminent, the General Secretariat, in consultation with the National Central Bureau or international entity which requested its publication, may replace it with any other appropriate notice.

Article 94: Stolen work of art notices *[deleted]*

Article 95: INTERPOL-United Nations Security Council Special Notices

(1) INTERPOL-United Nations Security Council Special Notices are published in order to inform INTERPOL's Members that an individual or an entity is subject to UN Security Council Sanctions.

(2) INTERPOL-United Nations Security Council Special Notices are published consistent with the Arrangement on Cooperation between the International Criminal Police Organization-INTERPOL and the United Nations in relation to the United Nations Security Council Sanctions Committees.

(3) The conditions for publication of these special notices shall be established in accordance with procedures agreed upon by the United Nations Secretariat and INTERPOL in consultation with the relevant Committees.

Article 96: Other special notices

(1) The purpose, conditions for publication and the structure of any other category of special notices shall be established under the agreement referred to in Article 28 of the present Rules, in conformity with the Organization's aims and activities set out in Title 1 of the present Rules.

(2) A special notice may only be published if the data satisfy the conditions for publishing this category of special notices, as laid down in the said agreement.

SECTION 4: DIFFUSIONS

Article 97: Diffusions system

(1) The diffusions system consists of standardized requests for cooperation and alerts each corresponding to a specific purpose:
   (a) to arrest, detain or restrict the movements of a convicted or accused person;
   (b) to locate and trace;
   (c) to obtain additional information;
   (d) for identification purposes;
   (e) to warn about a person's criminal activities;
   (f) for information purposes.

(2) The conditions for sending a diffusion are the same as the general conditions for recording data in the Organization's police databases.

(3) The General Secretariat shall submit any proposal to create a new category of diffusion to the Executive Committee for approval. To justify its request, the General Secretariat shall provide:
   (a) the reasons that led it to propose this creation, as well as the financial implications of such a creation;
   (b) the specific purpose of this new category of diffusion, the conditions for its circulation as well as the type of data it will contain;
   (c) the outcome of any tests conducted by the General Secretariat;
   (d) the opinion of the Commission for the Control of INTERPOL's Files, if the new category of diffusion contains personal data or is linked to such data.

Article 98: Diffusion forms

(1) The General Secretariat shall make tools and mechanisms available to the National Central Bureaus and international entities to enable them to carry out the automated and standard processing of diffusions in the INTERPOL Information System and to consult them directly.

(2) The General Secretariat shall provide National Central Bureaus and international entities with the necessary forms to enable them to send cooperation requests and alerts by means of a diffusion.

(3) The General Secretariat, in consultation with the National Central Bureaus or with their representatives on advisory bodies set up for the purpose, shall define and modify, when necessary, the structure of each form.

Article 99: Circulation of diffusions

(1) Diffusions shall be circulated in at least one of the Organization's working languages.

(2) Before circulating a diffusion, the National Central Bureau or international entity shall ensure:
   (a) the quality and lawfulness of the data it provides in support of its diffusion;
   (b) that its diffusion complies with the general conditions for recording data;

(c) that the data are of interest for the purposes of international police cooperation;

(d) that its request complies with INTERPOL's rules, specifically with Articles 2(1) and 3 of the Constitution, as well as with the obligations imposed on the requesting entity under international law.

(3) A National Central Bureau or international entity must use a diffusion rather than a notice if:

(a) it wishes to limit the circulation of its cooperation request or alert to selected National Central Bureaus or international entities;

(b) it wishes to limit the access to the data contained in its cooperation request or alert to a restricted number of National Central Bureaus or international entities;

(c) its request does not justify or does not qualify for the publication of a notice.

Article 100: Suspension or withdrawal of a diffusion

(1) The National Central Bureau or international entity that has sent an alert or a cooperation request by diffusion may suspend its diffusion for a period not exceeding six months. It shall indicate to the General Secretariat the reasons for the suspension.

(2) The National Central Bureau or international entity that has sent an alert or a cooperation request by diffusion must assess the need to maintain its diffusion whenever any changes are made to data contained in the diffusion.

(3) The National Central Bureau or international entity that has sent an alert or a cooperation request by diffusion must notify the National Central Bureaus, international entities, and the General Secretariat of its withdrawal once the purpose of the diffusion has been achieved or if it no longer wishes to maintain the request.

Article 101: Recording of cooperation requests or alerts circulated in messages

(1) In conformity with Article 9(4) of the present Rules, a National Central Bureau or an international entity may ask the General Secretariat to record in one of the Organization's police databases a request for cooperation or an international alert that it initially circulated in a message of which the General Secretariat was not initially a recipient.

(2) The General Secretariat shall record the cooperation request or alert in accordance with the present Rules and any rules on restricted access and conditions for use of data which may have been established by the National Central Bureau or international entity.

SECTION 5: NOTICES AND DIFFUSIONS PUBLISHED AT THE INITIATIVE OF THE GENERAL SECRETARIAT

Article 102: Requests for information

(1) The General Secretariat may request information from sources for cooperation purposes in the following cases:

(a) The request is made in the context of either a specific project or an event with specific interest for the purposes of international police cooperation;

(b) It has reasons to believe that this is necessary to achieve the objectives of the Organization and is in keeping with the aims pursued.

(2) The General Secretariat must obtain the prior authorization of the National Central Bureau concerned if it wishes to request information from a national entity. This authorization shall be deemed to have been granted if the National Central Bureau has not replied to the General Secretariat within 30 days of the request for authorization. It is understood that the National Central Bureau retains the right to oppose this request for information from one of its national entities at any moment.

Article 103: Publication of notices

(1) In conformity with Article 25(4) of the present Rules, the General Secretariat may publish notices at its own initiative:

(a) for the purposes of issuing an alert;

(b) to request information.

(2) Before publishing a notice at its own initiative, the General Secretariat shall ensure that:

(a) the publication of the notice complies with the conditions for its publication;

(b) the source(s) of the data have consented to this publication and, in particular, that any access restrictions have been lifted and the confidentiality level set for these data permits their publication;

(c) the publication of the notice is not likely to interfere with a pending cooperation request and that no similar notice request has been submitted by a National Central Bureau or an international entity.

SECTION 6: POSITIVE QUERY RESULTS

Article 104: Generation of positive query results

(1) A positive query result is generated in the INTERPOL Information System whenever sufficient correlation is established between the query and data recorded in one of the Organization's permanent operational police databases. The establishment of a sufficient correlation will depend on the characteristics of each database.

(2) When a positive query result is generated, subject to the characteristics of each database, a notification shall be sent to the National Central Bureau or international entity that consulted the database, and to the General Secretariat. A notification shall also be sent to the National Central Bureau or the international entity that recorded the initial data, depending on its indicated preference for receiving positive query result notifications.

(3) The notification of the positive query result shall include, at the very least, the reference of the National Central Bureau or international entity that consulted the database and that of the National Central Bureau or the international entity which recorded the initial data, as well as the main data relating to the recorded person, object or event.

(4) When data are processed by private entities in the context of specific projects, all the conditions and modalities relating to the positive query results shall be laid down in the agreements concluded between the Organization and the private entities pursuant to Article 28 of the present Rules.

Article 105: Procedure for managing positive query results

(1) The National Central Bureau or the international entity that generated the positive query result shall contact the National Central Bureau or the international entity that recorded the initial data in accordance with Article 63(1).

(2) The National Central Bureau or international entity that recorded the initial data shall examine the relevance of the positive query result as soon as possible.

(3) Procedures shall be determined by the General Secretariat, in consultation with National Central Bureaus or with their representatives on the advisory bodies set up for that purpose, to define the measures to be taken and response deadlines, according to the nature of the cooperation request.

(4) The National Central Bureaus shall determine the procedures for notifying positive query results to their national entities, with due regard to the applicable national laws.

Article 106: Record of positive query results

(1) The General Secretariat shall keep a record of the positive query results generated for a given cooperation request. This record shall be retained for such time as the data are recorded in the police databases.

(2) The National Central Bureau or international entity that recorded the initial data may consult this record.

CHAPTER III: DATA SECURITY

SECTION 1: MANAGEMENT OF RIGHTS OF ACCESS TO THE INTERPOL INFORMATION SYSTEM

Article 107: Designation of a new National Central Bureau

(1) The General Secretariat shall inform the National Central Bureaus and the international entities of any new membership to the Organization and designation of a National Central Bureau.

(2) With effect from the date of notification by the General Secretariat, a National Central Bureau or an international entity shall have 45 days to signify its opposition to granting this new National Central Bureau the right to process the data it has recorded in the police databases.

Article 108: Granting a right of access to a new national entity

(1) Prior to granting a new national entity a right of access to the INTERPOL Information System, the National Central Bureau shall take all the necessary measures to ensure that the said national entity observes the obligations arising from the present Rules.

(2) Each National Central Bureau shall notify the General Secretariat of any rights it has granted to a new national entity to access the INTERPOL Information System.

(3) It shall specify the scope of the authorizations granted.

Article 109: Granting a right of access to a new international entity

(1) The General Secretariat shall notify National Central Bureaus and international entities of any new right of access granted by the Organization to a new international entity.

(2) It shall specify the scope of authorizations granted under the agreement concluded with the Organization.

(3) With effect from the date of notification by the General Secretariat, a National Central Bureau or an international entity shall have 45 days to signify its opposition to granting this international entity the right to access the data it has recorded in the police databases.

Article 110: Register of rights of access to the INTERPOL Information System

The General Secretariat shall keep an up-to-date register of all the National Central Bureaus, and all national entities, international entities and private entities authorized to process data, directly or indirectly, in the INTERPOL Information System and ensure it is permanently available for consultation. This register shall specify the purpose, the nature and the scope of processing rights, and shall record any recent changes to these rights.

Article 111: Individual rights to access the INTERPOL Information System

(1) In conformity with Article 15(4) and (5) of the present Rules, the rights to access the INTERPOL Information System shall be granted to expressly authorized persons, solely on a need-to-know basis, taking into account the confidentiality levels.

(2) These rights shall be defined by:
   (a) the National Central Bureaus for their staff and staff of their national entities;
   (b) the General Secretariat for its staff and the staff of international entities.

(3) The National Central Bureaus and international entities shall be required to take all appropriate measures to ensure that their authorized users of the INTERPOL Information System observe the provisions of the present Rules.

(4) The National Central Bureaus and the international entities shall:
   (a) use all appropriate means to ensure that the authorized users are aware of and are able to observe the provisions of the present Rules and that they receive necessary training for that purpose;
   (b) forward the information communicated by the General Secretariat to the authorized users.

(5) The National Central Bureaus, international entities and the General Secretariat shall keep a register of the names of persons and the access rights they have been granted. They shall indicate the databases and the data to which they are authorizing user access.

(6) A National Central Bureau may choose to delegate to a national entity the management of access rights for the national entity's users. It shall ensure that the said national entity observes the obligations set out above. The delegation arrangements shall be defined in the agreement concluded between the National Central Bureau and the national entity in conformity with Article 21(3) of the present Rules. The National Central Bureau shall regularly check that these obligations and the defined arrangements are being observed by the entity.

SECTION 2: CONFIDENTIALITY

Article 112: Confidentiality levels

(1) There are three confidentiality levels reflecting the increasing risks that may arise from unauthorized disclosure of data:
   (a) "INTERPOL FOR OFFICIAL USE ONLY"
   (b) "INTERPOL RESTRICTED"
   (c) "INTERPOL CONFIDENTIAL".

(2) The data shall be classified:
   (a) "INTERPOL FOR OFFICIAL USE ONLY" if their unauthorized disclosure is likely to adversely affect law-enforcement action or to disadvantage or discredit the Organization, its staff, its Members, National Central Bureaus, national entities, and international entities or persons concerned by the data;
   (b) "INTERPOL RESTRICTED" if their unauthorized disclosure could compromise law-enforcement action or cause harm to the Organization or its staff, its Members, National Central Bureaus, national entities, and international entities or persons concerned by the data;
   (c) "INTERPOL CONFIDENTIAL" if their unauthorized disclosure might seriously compromise law-enforcement action or cause serious harm to the Organization or its staff, its Members, National Central Bureaus, national entities, international entities or persons concerned by the data.

(3) If no confidentiality level is attributed to the data by their source, the data shall be classified "INTERPOL FOR OFFICIAL USE ONLY".

(4) If a National Central Bureau, national entity or international entity needs, in a specific case, to classify certain data at a higher level of confidentiality than above, the General Secretariat shall assess with the National Central Bureau or entity concerned whether it is possible. If it is possible, they shall conclude a special arrangement defining the conditions attached to the processing of these data.

(5) A National Central Bureau, national entity or international entity may, at any time, modify the level of confidentiality that it has attributed to data, in particular by attributing a lower confidentiality level than the one previously indicated, if it considers that the data requires less protection.

Article 113: Additional measures taken by the General Secretariat

(1) The General Secretariat may, with the consent of the National Central Bureau, national entity or international entity that recorded the data, attribute a confidentiality level to the data which is higher than that attributed by the source, in the light of the risks to international police cooperation or to the Organization, its staff, and its Members that the processing and, more particularly, disclosure of the data might entail.

(2) The General Secretariat shall determine, in the same way, the confidentiality level of the value it adds to data, in particular when it carries out analysis work or publishes a notice. In such cases, it shall inform the source or sources of the data of this additional measure.

(3) The General Secretariat may also classify a database in the same conditions as those mentioned above.

(4) When the General Secretariat attributes a confidentiality level to data which is higher than that attributed by the National Central Bureau, national entity or international entity which recorded them, it may modify that higher confidentiality level at any time.

Article 114: Respecting confidentiality in the INTERPOL Information System

(1) The General Secretariat shall be responsible for determining authorization procedures or a system of security clearance at each data-confidentiality level. Access to a given confidentiality level shall be understood to be subject to any restrictions determined by the National Central Bureaus, international entities or the General Secretariat.

(2) The communication facilities and infrastructure used for processing data shall, depending on the confidentiality level attributed to the data, be equipped with the appropriate security controls to prevent the risk of unauthorized disclosure or to detect such a disclosure.

(3) The General Secretariat shall develop the administrative and technical processing procedures which must be observed by its staff for each confidentiality level.

(4) The National Central Bureaus, national entities and international entities shall put in place internal administrative and technical processing procedures, at least equivalent to those established by the General Secretariat, in order to ensure that the confidentiality level requested by the National Central Bureau, national entity or international entity which recorded the data is duly observed.

(5) The General Secretariat shall, in coordination with the National Central Bureaus and the entities concerned, draw up equivalence tables for its levels of classification and those used by the National Central Bureaus, national entities and international entities, whenever necessary.

SECTION 3: MANAGEMENT OF THE SECURITY SYSTEM

Article 115: Security rules

(1) In conformity with Article 15 of the present Rules, the General Secretariat shall lay down security rules defining procedural, technical and administrative security controls that ensure appropriate levels of confidentiality, integrity and availability for the INTERPOL Information System.

(2) The General Secretariat shall perform the necessary risk assessment.

(3) The General Secretariat shall develop appropriate control mechanisms to ensure that the security of data is maintained.

(4) The General Secretariat may, if necessary, establish specific security rules for a part of the communication infrastructure, a database or a specific department.

Article 116: Implementation by the National Central Bureaus and entities

The National Central Bureaus, national entities and international entities shall be responsible for adopting an appropriate level of security at least equivalent to the minimum level of security laid down in the security rules established by the General Secretariat.

Article 117: Appointment of a security officer

(1) Each National Central Bureau, national entity or international entity shall appoint one or more security officers to carry out security operations for their country or international organization in the INTERPOL Information System.

(2) The security officer shall, in particular:

(a) ensure compliance with the security procedures established by his/her National Central Bureau, national entity or international entity;

(b) update these procedures, notably in the light of the rules adopted by the General Secretariat;

(c) conduct further training on data security for the staff in his/her National Central Bureau, national entity or international entity.

(3) Whenever necessary, the security officer shall coordinate with the data protection officer.

(4) The security officer shall ensure the necessary coordination with the General Secretariat with regard to security matter.

SECTION 4: SECURITY INCIDENTS

Article 118: Information on security incidents

(1) In the event of intrusion or serious attempted intrusion affecting the network or one of the Organization's databases, or of violation or attempted violation of the integrity or confidentiality of data, the General Secretariat shall inform the source of that data, the National Central Bureau if the source is an entity that it has authorized, the Executive Committee, and the Commission for the Control of INTERPOL's Files.

(2) In the event of violation or attempted violation of the integrity or confidentiality of data initially processed in the INTERPOL Information System and processed in the information system of a National Central Bureau or an international entity, the latter shall inform the source of that data and the General Secretariat, and the Commission for the Control of INTERPOL's Files if the security incident concerns personal data. When any violation or attempted violation occurs in the information system of a national entity, the National Central Bureau that authorized it to access the INTERPOL Information System shall inform the source of the data and the General Secretariat.

Article 119: Partial or complete restoration of the INTERPOL Information System

The General Secretariat shall take all necessary and appropriate steps to be able to restore, as quickly as possible, in the event of damage, the proper functioning of the INTERPOL Information System, in particular its databases and its communications infrastructure.

TITLE 4:
SUPERVISION AND MONITORING

CHAPTER I:
TYPES OF SUPERVISION

Article 120: Supervision of users

(1) All National Central Bureaus, national entities and international entities shall regularly ensure that their users observe the present Rules, particularly with regard to the quality of the data they enter in the system and their use of the data consulted therein. Supervision shall be carried out in the context of spot checks and processing incidents.

(2) They shall take, within the limits set by the present Rules, all necessary measures to correct or to ensure the correction of possible processing errors.

Article 121: Designation of a data protection officer within National Central Bureaus and national and international entities

(1) All National Central Bureaus, national entities and international entities shall designate a data protection officer who shall be responsible for organizing and carrying out this monitoring. The duties of the data protection officer shall generally be carried out separately from the duties of the security officer.

(2) The data protection officer shall, in particular:

(a) establish processing procedures at his/her National Central Bureau, national entity or international entity which are in compliance with the present Rules;

(b) carry out supervision in the context of spot checks or processing incidents with the aim of guaranteeing compliance with the said Rules and procedures;

(c) update the said procedures and mechanisms;

(d) implement suitable ongoing training programmes in data processing for the staff of his/her National Central Bureau, national entity or international entity.

(3) Whenever necessary, the data protection officer shall cooperate with the security officer and with the INTERPOL data protection officer.

Article 121A: Designation of a data protection officer within the General Secretariat

(1) In accordance with Article 29 of the Constitution, and Articles 17(5,6) and 22(1,5) of the present Rules, after consulting the Executive Committee and the Commission for the Control of INTERPOL's Files, the Secretary General shall designate a data protection officer, hereinafter called the INTERPOL Data Protection Officer (IDPO).

(2) The IDPO shall be appointed for a period of five years, renewable once.

(3) In the performance of his/her duties, the IDPO shall be independent and shall report directly to the Secretary General.

(4) The IDPO shall, in particular:

(a) monitor the lawfulness and compliance of the processing of data in the INTERPOL Information System in accordance with the Organization's Constitution and rules;

(b) provide on his/her own initiative, or at the request of the General Secretariat, National Central Bureaus or other entities using the INTERPOL Information System with advice on processing operations which are likely to result in a high risk for the rights and freedoms of individuals, including data protection impact assessments, and monitor the actions taken in the light of that advice;

(c) liaise, collaborate and ensure coordination with all data protection officers designated pursuant to Article 121 of the present Rules, including through the provision of training and raising awareness on data protection issues;

(d) examine the yearly reports of data protection officers submitted in accordance with Article 17(4,5,6) and Article 123(3) of the present Rules;

(e) provide training on and raise awareness of data processing issues among the General Secretariat's staff;

(f) liaise with the Commission for the Control of INTERPOL's Files on data processing issues;

(g) liaise with data protection officers of other institutions and bodies, in particular by exchanging experience and best practices.

(5) For the purpose of carrying out his/her functions effectively, the IDPO shall have free and unlimited access to all data processed in the INTERPOL Information System and to any system within the INTERPOL Information System for processing such data, irrespective of the place, form or medium involved.

(6) In performing his/her duties, the IDPO may submit to the General Secretariat:

(a) Recommendations regarding measures to be taken in relation to data processing issues within the General Secretariat, including the correction of processing errors;

(b) Recommendations regarding the need to apply corrective measures in accordance with Article 131 of the present Rules;

(c) Reports relating to the non-implementation of the IDPO's recommendations within the General Secretariat.

(7) The IDPO may, on his/her own initiative or at the request of the CCF, share with the CCF the recommendations made and reports issued for information, and for any action deemed appropriate by the Commission.

(8) The IDPO may seek expert advice on general matters related to his/her duties.

(9) The IDPO shall submit an annual report to the Executive Committee, which will be made available to the Commission for the Control of INTERPOL's Files.

(10) The Secretary General shall adopt implementing rules concerning the work of the IDPO, including with regard to specific tasks within the IDPO's mandate, internal procedures, and safeguards for the independence of the IDPO.

Article 122: Monitoring the use of data

(1) Any National Central Bureau may request information about how another National Central Bureau, a national entity or an international entity is using data which it or its national entities have processed in the INTERPOL Information System. If the data have been consulted or used by a national entity, it shall carry out checks through that national entity's National Central Bureau.

(2) The General Secretariat shall assist the international entities in exercising the same monitoring rights.

(3) Any National Central Bureau, national entity or international entity which is subject to such monitoring must provide the requested data.

Article 123: Evaluation of national entities

(1) In accordance with Article 17(4) of the present Rules, the National Central Bureaus shall evaluate the operations, in the light of the present Rules, of the national entities they have authorized to directly access the INTERPOL Information System.

(2) Due observance by a national entity of the obligations set out in the present Rules is an essential condition for the national entity to retain direct access to the INTERPOL Information System.

(3) Every year, each National Central Bureau shall report to the General Secretariat on the spot checks it has carried out, the processing incidents it has handled, the training resources it has provided to its staff and the new measures it has adopted to meet the obligations of these Rules.

(4) The General Secretariat shall be empowered either to ask the National Central Bureau to apply corrective measures to a national entity, or to terminate access to the INTERPOL Information System if the said entity has repeatedly processed data in a non-compliant manner, if no evaluations have been carried out by the National Central Bureau concerned, or if any such evaluations have been inadequate.

Article 124: Evaluation of National Central Bureaus

(1) In accordance with Article 17(5) of the present Rules, the General Secretariat shall evaluate the operation of the National Central Bureaus in the light of the present Rules.

(2) The evaluation of National Central Bureaus in the light of the present Rules shall be performed by the General Secretariat in accordance with the directives decided upon by the General Assembly.

CHAPTER II: SUPERVISORY TOOLS

Article 125: Compliance management database

(1) In accordance with Article 10(4) of the present Rules, the General Secretariat may set up any databases to ensure that data recorded in the Organization's police databases comply with the present Rules and to avoid unauthorized or erroneous processing of data in the databases.

(2) A compliance management database shall be set up under the following conditions:

(a) It shall contain only those data which are necessary to avoid unauthorized or erroneous processing of data;

(b) The retention of data in this database shall be limited to a maximum retention period determined by the Executive Committee. This may be extended, after the Commission for the Control of INTERPOL's Files has been notified, if the examination of compliance management has not been completed by the end of this period;

(c) Access to these databases shall be restricted to authorized departments and/or staff of the General Secretariat involved in the processing of data and to whom specific access has been granted.

(3) When the General Secretariat deletes data from a police database or a compliance management database, it may nevertheless retain, for a maximum retention period determined by the Executive Committee, those data making it possible to avoid unauthorized or erroneous processing of the said data.

Article 126: Register of processing operations

(1) In accordance with Article 13 of the present Rules, the General Secretariat shall keep an up-to-date register of processing operations in the INTERPOL Information System to record:

(a) accesses to the INTERPOL Information System by users;

(b) the data recorded by users;

(c) updates made by users;

(d) decisions made by users to retain data;

(e) decisions made by users to delete data;

(f) consultations by users with direct access;

(g) requests for information received and replies sent.

(2) The register shall contain only those data necessary for verifying the conformity of processing with the present Rules. To this end, it shall include: the user identifier, the name of the user's National Central Bureau, national entity or international entity, the type of the processing operation, the date, the database concerned, and any additional items of data intended for monitoring purposes.

(3) These records shall be retained for no longer than a maximum retention period determined by the Executive Committee.

(4) These records may be accessed:

(a) solely for monitoring and checking purposes;

(b) by General Secretariat staff authorized to carry out checking operations;

(c) by the source, for monitoring purposes, on request to the General Secretariat.

(5) These records may not be used for the purposes of a criminal investigation unless this investigation is linked to checking the compliance of data processing with the present Rules.

Article 127: Comparison of data for verification purposes

(1) Any National Central Bureau, national entity or international entity which has processed in its information system data that were initially processed in the INTERPOL Information System may send a request to the General Secretariat to compare them with the data currently contained in the INTERPOL Information System in order to verify their quality. All requests from a national entity must be sent through its National Central Bureau.

(2) Any data comparison for verification purposes may be carried out by either uploading or downloading the data:

(a) any data comparison made by uploading data must meet all the following conditions:

(i) the uploading is performed solely to allow the General Secretariat to verify, on behalf of the National Central Bureau or the international entity which sent the request, the quality of the data that it has entered in its information system;

(ii) the uploaded data are not further copied within the INTERPOL Information System into which they are uploaded;

(iii) the uploaded data are systematically deleted after the data-comparison operation.

(b) any data comparison made by downloading data must meet all the following conditions:

(i) the downloading is performed solely to allow the National Central Bureau, national entity or international entity to verify the quality of the data that it has entered in its information system;

(ii) the information system of the National Central Bureau, national entity or international entity offers a level of security at least equivalent to that of the INTERPOL Information System;

(iii) the downloaded data are not further copied within the information system into which they are downloaded;

(iv) the downloaded data are systematically deleted after the data-comparison operation.

(3) The General Secretariat shall be empowered to authorize comparisons of data for verification purposes, subject to:

(a) compliance with the conditions above; and

(b) written assurances provided by the National Central or international entity that requested to carry out an operation to compare data, by which it undertakes to respect those conditions, the purpose of the operation, its nature and its scope; and

(c) the designation of a person to be responsible for overseeing the comparison of data at the National Central Bureau, national entity or international entity.

(4) The General Secretariat shall keep an updated register of the data-comparison operations carried out by downloading or uploading.

CHAPTER III: SUPERVISION MEASURES

Article 128: Examination procedure

(1) Data are, a priori, considered to be accurate and relevant when entered by a National Central Bureau, a national entity or an international entity into the INTERPOL Information System and recorded in a police database of the Organization.

(2) If a doubt arises regarding compliance with the conditions for data processing, including cases where data have been processed by a national entity, the General Secretariat shall consult the National Central Bureau concerned in order to obtain clarifications or supplementary data which may remove the doubt. The General Secretariat shall also consult any international entity if there is any doubt over compliance with the conditions for processing data.

(3) The General Secretariat shall take any other appropriate steps to ensure that these conditions have actually been met.

(4) The examination procedure shall be deemed closed if the General Secretariat concludes that the processing of data:

(a) complies with the present Rules and validates the recording of data;

(b) does not comply with the present Rules and decides to correct the data processing or to delete the data.

(5) The General Secretariat shall inform the National Central Bureau or the international entity that the examination procedure has ended. If it decides to correct or delete the data, it shall indicate reasons for its action and the corrections made to the said National Central Bureau or international entity.

Article 129: Interim measures

(1) If a doubt arises regarding compliance with the conditions for data processing, the General Secretariat shall take all appropriate steps to prevent any direct or indirect prejudice the data may cause to the Organization, its staff, its Members, the National Central Bureaus, the national entities, the international entities or the individuals that the data concern.

(2) The General Secretariat shall inform the National Central Bureau or the international entity of any interim measures taken and shall specify reasons for them.

Article 130: Measures applicable to users

If users infringe the rules applicable to the processing of data in the INTERPOL Information System, the General Secretariat may:

(a) request the National Central Bureau or international entity to suspend or withdraw the access rights it granted them;

(b) suspend or withdraw the rights itself. It shall inform the Bureau or international entity concerned of the suspension or withdrawal.

Article 131: Corrective measures applicable to National Central Bureaus and international entities

(1) If a National Central Bureau or an international entity encounters difficulties when processing data in the INTERPOL Information System or does not fulfil its obligations under the present Rules, the General Secretariat shall be entitled to take the following corrective action:

(a) correction of processing errors;

(b) supervision, for a period no longer than three months, of the processing operations carried out by the National Central Bureau or international entity;

(c) suspension of the access rights granted to users of the National Central Bureau or the international entity;

(d) dispatching an assessment team to the National Central Bureau or the international entity.

(2) The General Secretariat may send the National Central Bureaus and international entities recommendations relating to the implementation of the present Rules with a view to helping them – for instance, through staff training or by enhancing working procedures – to resolve difficulties or bring processing incidents to an end.

(3) The General Secretariat shall submit to the Executive Committee for decision all proposals to take corrective measures which may result in the long-term suspension of the following processing rights of a National Central Bureau or international entity:

(a) the right to record data in one or several police databases of the Organization;

(b) the right to consult one or several databases;

(c) interconnection or downloading authorizations.

(4) Whenever necessary, and at least once a year, the General Secretariat shall remind the National Central Bureaus and international entities of their role and responsibilities connected with the data they process in the INTERPOL Information System.

TITLE 5: FINAL PROVISIONS

CHAPTER I: PROCESSING FOR ANY OTHER LEGITIMATE PURPOSE

Article 132: Definition of processing for any other legitimate purpose

(1) In accordance with Article 10(7) of the present Rules, when data have been deleted from a police database of the Organization or a compliance management database, the General Secretariat may nevertheless retain the data necessary for the pursuit of any other legitimate purpose.

(2) Any other legitimate purpose means:

(a) the defence of the Organization's interests, particularly in litigation and pre-litigation procedures and transactions;

(b) scientific, historical or journalistic research and publication;

(c) the compilation of statistics.

(3) When data initially processed for the purposes of police cooperation undergo further processing for any other legitimate purpose, they may no longer be used, in any way whatever, for the purposes of police cooperation and must not appear in the Organization's police databases.

(4) Only the processing of personal data carried out in application of paragraph 2(b) shall be subject to prior authorization by the source of the data. However, when personal data have been processed in application of paragraph 2(a) above, the source of the data shall be informed by the General Secretariat of their use or transmission.

(5) The General Secretariat shall take the necessary technical and organizational measures, particularly with regard to security, to guarantee that this further processing is not incompatible with the initial processing.

Article 133: Processing conditions

(1) When processing is carried out for any other legitimate purpose, the reasons must be specified. The specific purpose of this processing must be clearly indicated and the processing must be limited to those items of data which are strictly necessary for the purpose intended.

(2) Processing shall be carried out, if possible, using data which have been made anonymous or, failing that, encoded, whenever the intended purpose can be achieved by such means.

(3) The access to data processed for any other legitimate purpose shall be restricted to authorized departments or staff of the General Secretariat to whom specific access has been granted.

Article 134: Retention of data

(1) Data processed for any other legitimate purpose shall be retained for a period strictly necessary to achieve the purpose for which they were processed, and not exceeding a maximum retention period determined by the Executive Committee.

(2) This period may be extended solely when data have been retained for historical purposes or if the data have been made anonymous or encoded for processing, on condition that the extension itself remains necessary to accomplish the aims for which the processing is being carried out.

CHAPTER II:
SETTLEMENT OF DISPUTES

Article 135: Settlement of disputes

(1) Disputes involving National Central Bureaus, international entities, national entities, private entities, or the General Secretariat concerning compliance decisions that arise in connection with the application of the present Rules shall be governed by the following procedure:

   (a) Disputes should be solved by concerted consultation. If this fails, a final compliance decision shall be issued by the General Secretariat;

   (b) After a final compliance decision is issued, a party to the dispute may submit a policy question concerning the application or interpretation of the Constitution, Rules on the Processing of Data and/or relevant General Assembly Resolutions arising from the dispute to the Executive Committee. If the policy question is not within the Executive Committee's powers or if the Executive Committee otherwise deems it necessary, it shall submit the policy question to the General Assembly.

(2) Nothing shall prevent the relevant entities from resolving their disagreements amicably outside this dispute settlement procedure.

(3) The General Assembly shall adopt Implementing Rules governing the settlement of disputes.

****

APPENDIX:
CHARTER RELATING TO ACCESS TO THE INTERPOL INFORMATION SYSTEM BY NATIONAL ENTITIES

The purpose of the present Charter is to clearly set out the conditions under which national entities may be authorized by the National Central Bureaus of their respective countries, pursuant to Article 21 of INTERPOL's Rules on data processing, to directly consult data processed in the INTERPOL Information System or to directly supply data for processing purposes in this System.

(1) Direct access to the INTERPOL Information System shall be subject to the following conditions:

(a) Direct access to and use of the INTERPOL Information System shall be subject to INTERPOL's Rules on the Processing of Data;

(b) The national entity shall accept and agree to comply with the provisions of these Rules and with any procedures established in application of the said Rules to allow access to and use of INTERPOL's Information System;

(c) The national entity shall designate and assign a security officer and a data protection officer, and put in place procedures with the aim of ensuring on a permanent basis that its users are respecting the present Rules;

(d) The national entity shall agree, in particular, to allow the National Central Bureau that authorized it:

(i) to carry out regular checks, remotely or on site, on its processing of data entered or consulted in the INTERPOL Information System to ensure compliance with the Rules;

(ii) to take the necessary preventive or corrective measures against it in the event of a processing incident;

(iii) to withdraw the national entity's access to the INTERPOL Information System in the event of failure to comply with its obligations under these Rules or the repeated non-compliant processing of data.

(e) The national entity shall also agree that the INTERPOL General Secretariat:

(i) shall be responsible for the general administration of the INTERPOL Information System and ensure that the conditions for processing data in the Organization's databases are met;

(ii) may take any appropriate measures within the scope of these Rules to terminate any non-compliant processing of data, including withdrawing access to the INTERPOL Information System.

(2) The extent of the national entity's access rights to the INTERPOL Information System shall be determined by its National Central Bureau in accordance with INTERPOL's Rules on the Processing of Data.

****