## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Abbreviations</td>
<td>5</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Background</td>
<td>11</td>
</tr>
<tr>
<td>› Legal context</td>
<td>11</td>
</tr>
<tr>
<td>› Qualification</td>
<td>11</td>
</tr>
<tr>
<td>DACORE Mission</td>
<td>12</td>
</tr>
<tr>
<td>› General mission</td>
<td>12</td>
</tr>
<tr>
<td>› Administrative missions</td>
<td>12</td>
</tr>
<tr>
<td>› Technical missions</td>
<td>12</td>
</tr>
<tr>
<td>› Training</td>
<td>13</td>
</tr>
<tr>
<td>Organization</td>
<td>16</td>
</tr>
<tr>
<td>› Design and management</td>
<td>16</td>
</tr>
<tr>
<td>› Line management</td>
<td>16</td>
</tr>
<tr>
<td>› Enforcement</td>
<td>17</td>
</tr>
<tr>
<td>› Infrastructures</td>
<td>18</td>
</tr>
<tr>
<td>Operationalization of the System at National Level</td>
<td>19</td>
</tr>
<tr>
<td>› “Data entry” function</td>
<td>19</td>
</tr>
<tr>
<td>› “Data validation” function</td>
<td>20</td>
</tr>
</tbody>
</table>
› “Data validation” function 22
› “Check” function 22

USE OF THE SYSTEM BY THE COURTS 24
APPENDIX : QUALITY CONTROL 25
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIRCOP</td>
<td>Airport Communication Project</td>
</tr>
<tr>
<td>CCSS</td>
<td>Committee of Chiefs of Security Services</td>
</tr>
<tr>
<td>DACORE</td>
<td>Data Collection and Registration (Centre)</td>
</tr>
<tr>
<td>DEVCO</td>
<td>International Cooperation and Development</td>
</tr>
<tr>
<td>ECOWAS</td>
<td>Economic Community of West African States</td>
</tr>
<tr>
<td>EDF</td>
<td>European Development Fund</td>
</tr>
<tr>
<td>EEAS</td>
<td>European External Action Service</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUCAP</td>
<td>European Union Capacity Building Mission</td>
</tr>
<tr>
<td>EULOs</td>
<td>European Liaison Officers (platforms)</td>
</tr>
<tr>
<td>IFS</td>
<td>Instrument for Stability</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicators</td>
</tr>
<tr>
<td>LEA</td>
<td>Law Enforcement Agency</td>
</tr>
<tr>
<td>MoU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>NCB</td>
<td>INTERPOL National Central Bureau</td>
</tr>
<tr>
<td>PAJED</td>
<td>Programme d’Appui à la Justice et à l’État de Droit</td>
</tr>
<tr>
<td>PCMS</td>
<td>Plateforme de Coopération en Matière de Sécurité</td>
</tr>
<tr>
<td>PSCC</td>
<td>Programme Steering and Coordination Committee</td>
</tr>
<tr>
<td>RIP</td>
<td>Regional Indicative Programme</td>
</tr>
<tr>
<td>SEACOP</td>
<td>Seaport Cooperation Project</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SPOC</td>
<td>Single Point of Contact</td>
</tr>
<tr>
<td>TOC</td>
<td>Transnational Organized Crime</td>
</tr>
<tr>
<td>UNODC</td>
<td>United Nations Office on Drugs and Crime</td>
</tr>
<tr>
<td>UEMOA</td>
<td>West African Economic and Monetary Union</td>
</tr>
<tr>
<td>WANACO</td>
<td>WAPIS National Committee</td>
</tr>
<tr>
<td>WAPCCO</td>
<td>West African Police Chiefs Committee</td>
</tr>
<tr>
<td>WAPIS</td>
<td>West African Police Information System</td>
</tr>
</tbody>
</table>
The idea of creating a West African police information system (WAPIS) came from the ECOWAS member States, who expressed their concern over the outbreak of transnational organized crime and terrorism in the region. Security lapses at national, regional and international level have contributed to the fact that West Africa is facing increasing threats, especially drug smuggling, human trafficking and international terrorism. Without effective sharing of police data within the sub-region, as well as between the sub-region and the rest of the world, no law enforcement strategy can deal with these threats effectively.

In 2010, during a symposium organised jointly by INTERPOL and the Belgian Presidency of the European Union in Brussels, the West African Police Chiefs declared that, in order to tackle the security challenges facing the subregion, these countries needed an automated system for sharing police data, interconnected at both a regional and international level.

Since 2011, in the context of the West African Police Chiefs Committee (WAPCCO), the Police Chiefs and ministers responsible for security have expressed, year on year, great interest in the WAPIS programme.

In addition, the ECOWAS Commission considers the future WAPIS data sharing regional platform to be the natural counterbalance to the Commission’s initiative aiming to create an area of free movement and free settlement in the ECOWAS zone, through which the free movement of people would be accompanied by the possibility, for law enforcement agencies, of sharing and accessing information in the area of free movement.

The WAPIS programme aims to create or improve the national police electronic data systems in each country in West Africa. The national police information system will allow law enforcement agencies to create, manage and share files, relating in particular to:

- Criminal cases and misdemeanours
- Perpetrators of or accomplices in a crime or misdemeanor, as well as victims and witnesses of crimes and misdemeanours
- Stolen or reported weapons
- Items reported stolen or used to commit crimes
› Stolen vehicles, vehicles linked to a crime or misdemeanour and reported vehicles

› Identity documents that have been lost, stolen or reported missing and

› Administrative police data which contribute to the prevention of the commission of an offense and / or the preservation of law and order. These data include:

1. Category: Nominative administrative decisions
   • All nominative administrative decisions (ministerial or prefectural decision) whose non-compliance constitutes a criminal offense provided for and prohibited by the national legislation in force.

2. Category: Mentally-ill persons
   • Mentally ill persons placed in a psychiatric facility following an administrative decision, having escaped from such psychiatric facility.

3. Category: Foreigners
   • Concerns foreigners whose presence on the national territory constitutes a threat to public order and who are the subject of an administrative decision of expulsion (i.e. ministerial deportation order);
   • Concerns foreigners subject to an administrative prohibition to enter the national territory;
   • Concerns foreigners who have been the subject of an administrative expulsion decision that could not be executed for whichever reason;
   • Concerns foreigners subject to an administrative decision prohibiting return;
   • Concerns foreigners who have been the subject of a ministerial or other administrative order of house arrest;
   • Concerns foreigners subject to an administrative decision of interdiction to leave the territory of a country.

4. Category: Administrative measures concerning driving licenses
   • Consists of data coming from the administrative authorities authorized to take measures to restrict driving rights. (Suspension, withdrawal, cancellation)

5. Category: Runaway minors
   • Concerns only minors (following national legislation) who have left the parental home and have evaded the authority of those who have custody.
   • This measure will concern both domestic and foreign minors.

6. Category: Restriction against minors leaving the country
   • Concerns domestic and foreign minors residing in the national
7. **Category: Opposition to the issuance of identity documents**
   - Concerns the persons who are the subject of an administrative decision forbidding them to formulate an application for issuance or renewal of passports, or national identity card, etc., or, to whom it is advisable to withdraw administrative documents obtained unduly.

8. **Category: Unidentified persons**
   - Concerns unidentified cadavers and all living persons who cannot provide for their identity (amnesic persons, newborns, etc. ...)

9. **Missing persons being searched at the request of a family member**
   - Concerns persons reported as missing by a family member.

In addition, identifying criminals has been made considerably easier thanks to fingerprints. This is particularly true in West Africa, where public records data and national identification systems are limited. The WAPIS programme therefore needs to set up Automated Fingerprint Identification Systems (AFIS) in countries where AFIS is not yet up and running and do not have the capacity to maintain it.

The WAPIS national system is installed in a Data collection and registration centre (DACORE) on the premises of a designated law enforcement agency.

The creation of a DACORE constitutes a major event that will have a considerable influence on progress in setting up the WAPIS system for the beneficiary State, and especially for the administration in charge of creating it. The DACORE will be the regulatory body managing the system, and should therefore be set up with particular care by the supervisory authority.

This creation should be made official by means of a statutory text, which will stipulate how it is organized and how it operates. The DACORE should be an administrative, technical and operational support service capable of bringing together the representatives of all the law enforcement agencies involved in the programme.

The term “DACORE” is the generic name of an entity which will take a name specific to each State, as decided by each of the authorities concerned.

A DACORE should have its own budget heading to ensure that its operation, development and that of the overall system is permanent. It will be important for the beneficiary State to set up this arrangement as soon as possible in order to be prepared when the programme ends.
The responsible authorities need to be aware that it is up to them to roll out the WAPIS system throughout the territory for the benefit of the services using the system, and to keep it operational.

The first step, for the administration in charge of creating a DACORE, consists of making premises available that are suitable for the functions to be performed by this new service.

The second step consists of selecting and assigning the staff who will work in the DACORE. This is a very important step, during which particular care must be taken since the diversity of tasks performed by this service requires a high level of professionalism, or even specialist technical, legal, financial management or administrative skills.

A DACORE is not simply a building housing computer equipment, but an entirely separate entity, with specific missions, its own hierarchy and rule book, that operates 24 hours a day.

The WAPIS National Committee constitutes the decision-making body in terms of implementing and operating the West African police information system, and the DACORE, irrespective of what it is called, becomes its executive and functional body. It will be the nerve centre linking all the components, and on which they depend.

The DACORE needs to perform four essential functions to ensure that the WAPIS system works properly:

- Administrative and financial management
- Operational support
- Technical maintenance
- Training

Each of these functions involves specific missions and requires the DACORE to have its own organization and infrastructures.
LEGAL CONTEXT

The statutory text establishing the DACORE sets out its organization and structures, and defines its functions. A single text can establish the DACORE and the system.

QUALIFICATION

The minimum qualification level required of every DACORE member shall be defined in the centre’s rule book, which shall be drawn up by the director in close collaboration with the Single Point of Contact and the Interpol Country officer responsible for setting up the system in the beneficiary country. This rule book shall be submitted for approval and validation by a plenary session of the WAPIS National Committee.
GENERAL MISSION

The DACORE’s general mission is to execute the WAPIS National Committee’s instructions defining the strategic and tactical objectives, and to oversee and run the WAPIS system.

To do this, it needs to identify and perform the actions to be undertaken and monitor their enforcement.

ADMINISTRATIVE MISSIONS

The administrative function’s missions are to:

› Manage human resources;
› Organize and run the DACORE;
› Undertake the DACORE’s administrative and financial management;
› Ensure enforcement of personal data protection and data security regulations;
› Provide situation reports and statistics to the relevant authorities.

TECHNICAL MISSIONS

The DACORE needs to conduct several missions of a technical nature.

ADMINISTERING THE SYSTEM

A DACORE shall have a chief administrator and a deputy administrator capable of standing in for the former. Under the authority of the DACORE director, the system administrator grants rights of access to the database, checks the legitimacy of the records and lookups, and monitors the system in conjunction with the technical team.
CHECKING LEGALITY AND QUALITY

The DACORE makes a final check of the legality and quality of the data recorded in draft form by the data entry operators. These checks should normally be made upstream by the user services, and the DACORE’s mission is to ensure that they have been done properly.

For this purpose, the DACORE shall have “validators”, experienced officers with extensive knowledge of criminal law, court proceedings and police practice.

The number of validators in a DACORE depends on the amount of data being entered in the database.

COLLECTING DATA

The DACORE’s management is responsible for drawing up a strategy for collecting criminal proceedings instigated by services not yet equipped with WAPIS terminals, and redirecting them to the DACORE where the data will be entered by operators.

This strategy shall be submitted for approval by the WAPIS National Committee and implemented in accordance with their instructions.

REGISTERING DATA

A DACORE shall have a group of “data entry operators”, the number of whom depends on the amount of data being entered. They are responsible for entering data arising from criminal proceedings that will be sent to them.

The importance of data entry operators should not be underestimated, and they should have a great deal of experience in court and police proceedings.

A data entry operator cannot also work as a validator.

MAINTAINING AND MONITORING THE NETWORK

The DACORE shall have a technical team whose missions will consist of monitoring operation of the network. They must work around the clock and be able to respond quickly in case of a technical problem. They will also be responsible for equipment maintenance and providing support to territorial services.
The number of members in this team should take into account the fact that it needs to operate 24 hours a day, and have enough material resources to undertake its missions.

**TRAINING**

The Training of the users of the system must be a priority task for the DACORE.

A number of DACORE staff members should therefore be appointed to perform this training according to their level of teaching skill.

The training function’s missions are to:

- Support skills development in the areas where the WAPIS system is used, personal data protection and information security;
- Plan, organize and run basic and advanced training sessions;
- Update the training material.

**ORGANISATION**

The training should be aimed at law enforcement officers, system super-users, and also any judges who may need to use it. Law enforcement officers are authorized to receive this training so that they can update the database with the results of their investigations.

A training programme must be drawn up and put on the curriculum in training schools for the police, gendarmerie, and judges, etc.

**INFRASTRUCTURES**

To conduct its training mission successfully, the DACORE should have the following infrastructures:

**Training room**

In order to train users of the WAPIS system, whether police officers, gendarmes, judges or other law enforcement officers, who play a major part in the programme to set up the system, a DACORE must have a training room with around fifteen terminals and the necessary equipment for this type of room (video projector, screen, whiteboard, flip chart, etc.).
As soon as the staff training phase begins, the room should be used at least one week a month, if not more. This means that the WAPIS training room should primarily be reserved for use by staff using the system.

Ideally, the training room should be located within the premises of the DACORE and can also serve as a meeting room, but if this is impossible for practical reasons, the training room can be installed on a different site with the required security measures.
Organization defines the components of the service, in other words the design and management level, the line management level and the application level.

### DESIGN AND MANAGEMENT

Management is the responsibility of the director, assisted by their deputy and supported by the administrative secretariat.

The director shall be appointed by a statutory text emanating from the supervisory authority.

The deputy director can come from another law enforcement agency involved in using the system and made available to DACORE by their administration.

The director and his deputy should come from the senior management ranks of law enforcement agencies.

The management is responsible for administrative management of human resources, the centre and the overall system. It ensures enforcement of the decisions taken by the National Committee relating to the centre and all the missions that come under the latter’s remit. Moreover, it organizes and manages the advanced training programme for users of the WAPIS system.

The management reports on its activities to the National Committee.

The DACORE management shall have an administrative secretariat to which an administrator can be assigned by the Finance Ministry to run the budget for the service and its material needs.

### LINE MANAGEMENT

The line management of the DACORE working groups must consist of officers of inspector grade or higher and/or with a high level of IT training.
ENFORCEMENT

MANAGING THE SYSTEM

Under the authority of the DACORE director, this function is dedicated to administrators who assign duties to the various system users (data entry operator, validator, checker, investigating officer) and define rights of access to the database.

They permanently monitor and check the system, ensuring that the operating and security regulations are adhered to.

They coordinate interventions by technical teams in external services and deal with problems that may occur on the network.

On request, they can provide accurate statistical reports based on a number of search criteria.

The system is managed by:
  › an IT administrator responsible for managing the system and overseeing its use
  › at least one deputy administrator reporting to the system management supervisor.

The two administrators must come from two different services.

MONITORING THE NETWORK

The DACORE technicians monitor the network via an oversight system and can make a site visit if there is a problem falling within their remit. This monitoring is part of the priorities covered 24/7.

MAINTENANCE

The WAPIS programme will maintain the entire system for a period of two years from installation of the equipment.

An extension to this period may be considered by the WAPIS Programme Steering Committee at the appropriate time.
**INFRASTRUCTURES**

To conduct these missions successfully, the DACORE shall comprise several technical infrastructures.

To perform the administrative function, the DACORE shall be provided with a number of structures:

---

**OFFICES**

- Director’s office
- Deputy director’s office
- Secretarial office
- Finance/accounts manager’s office
- IT administrator’s office
- Deputy IT administrator’s office
- Validators’ office
- IT technicians’ equipment room
- Data entry operators’ room

---

**EQUIPMENT ROOM**

This houses the main server and must meet specific technical criteria:

- Minimum surface area 8 m²;
- Located on the premises of a law enforcement agency with full security measures. Access to the DACORE must be controlled;
- Allowing installation of a computer cabinet 800 mm wide and 120 mm deep;
- Powered via UPSs with protection from 32 A to 30 mA;
- Equipped with air conditioning units that will maintain the room temperature between 19° and 27°C;
- With enough energy self-sufficiency to cope with a prolonged power outage;
- Secured by an access control mechanism and reserved for people with authorization to enter.

NB: The DACORE does not need to have an equipment room. This can be installed in separate premises, provided they are sufficiently close to the DACORE for IT technicians to be able to respond quickly if necessary.

A second server called a “mirror server” should be installed in a location away from the main server, but in a room that meets the same technical criteria. Linked directly to the main server, it simultaneously records the data entered and will back up this data if the main server fails. For obvious security reasons, the location of this second server should be a matter of maximum discretion.
In order to make the system operational at the national level, a procedure will have to be put in place to ensure collection, registration, validation of data in the system as well as to carry out research and control.

"DATA ENTRY" FUNCTION

This is an essential element which affects the overall usage and utility of the system. For data to be usable, it must be correctly, accurately and meticulously recorded in the database, in accordance with the rule of law and the legislation in force.

This means that the operators who will be recording the data must have sufficient knowledge and skills in the area of criminal law, special criminal law and court proceedings to be able to make entries that can be validated without the need for correction.

The best-placed staff to record criminal data are law enforcement officers, since they are the most familiar with the content of their investigations.

There are two likely scenarios:

For territorial services equipped with WAPIS terminals, it is the law enforcement officers who will write their own reports, since they are best placed to appreciate the quality and legality of cases handled.

- **A**: For services not yet equipped with WAPIS terminals, LEOs should fill in a data collection form which will be sent to the DACORE or the nearest point with a WAPIS terminal, where data entry operators will then record it. The collection form must always be accompanied by a copy of the court proceedings for digitization and use at a later date.

- **B**: At least two operators (a manager and their deputy) should be asked to organize collection and recording of data from external services not equipped with WAPIS terminals. This service should also be charged with organizing and implementing digitization of the criminal archives from the various administrations (police, gendarmerie, customs, etc.). The number of data entry operators is likely to change according to the amount of incoming data from external services not equipped with WAPIS terminals.
Data entry and digitization of procedures already archived in the various services’ central files should be started as soon as possible, since this work will take several years.

It is up to the National Committee to schedule implementation of “quality control” in all the services concerned.

A guide to setting up “quality control” is attached as an appendix to this document (see Appendix 1).

**“DATA VALIDATION” FUNCTION**

All data entered in the system remains in “draft” status until it is approved by the validator. It is only after this validation that the data becomes usable and viewable.

A strict rule must apply to validation of data: **IN NO CASE CAN THE DATA ENTRY OPERATOR BE A VALIDATOR.**

The validator’s role will therefore be to check the quality of the entry, its legality and its compliance with the rules laid down.

This means that the validator has sufficient knowledge and skills in the area of criminal law, special criminal law, court proceedings and personal data protection to perform this check.

If there is an error or missing information, the validator returns the entry to the initial service, accompanied by comments allowing the necessary corrections. Once these alterations have been made, the entry is resubmitted for approval by the validator.

As with data entry, there are two scenarios for validation:

› **A:** For services equipped with WAPIS terminals, it is the heads of unit who will be responsible for this validation, since they are best placed to know the details and nature of cases handled by their employees. They should apply the quality and legality charter. Should the heads of unit not be able to perform this check and validation, these tasks will be the responsibility of the DACORE validators. They should monitor the system in order to make sure that the quality and legality instructions are followed by the heads of unit.
For services not yet equipped with WAPIS terminals:

For services not equipped with terminals, the head of unit will check drafting of the collection form, accompanied by a hard copy of the proceedings, before it is sent to the DACORE or chosen recording site. It is essential that this check is performed because the relevance of the data has an effect on use of the database.

At least two validators (a manager and their deputy) responsible for checking the quality and legality of the data entered should be assigned to the centre. The number of validators depends on the amount of incoming data entered that originates from external services not equipped with WAPIS terminals.

As concerns requests to register people who are “wanted persons”, these should be submitted for systematic validation by a competent authority, who will ensure that the request is legal and the additional instructions comply with the legislation and the procedure to be followed.

The same applies to requests to register stolen vehicles.

As regards the administrative police, registration requests coming from administrations should also be addressed to the DACORE, who will make the same checks before recording them.

For this type of request, the validators should ensure compliance with the provisions laid down in the national protocol for registering wanted persons before validating the request.

If wanted persons need to be de-registered, the requesting service should send the DACORE the appropriate form from the national protocol, and the validator, after checking, should change the status of the persons concerned.

The same process should be followed for registrations in the stolen vehicle database, except that it is the services who have found registered vehicles who will send the de-registration form to the DACORE to cancel the search, in accordance with the procedures laid down in the national protocol.

The same procedure will apply for lost or stolen administrative documents, stolen or reported weapons and generic found items.
"DATA VALIDATION" FUNCTION

The "search" function should mainly be used by law enforcement officers and investigating magistrates in the context of their enquiries, but it is not impossible for other duly authorized persons to perform these lookups.

Duly authorized named users can make searches in the criminal archives and look up established procedures, without making a previous request or visit, analyse offenders’ criminal record to see if there is anything that relates to their investigations, draw up a behavioural profile, identify accomplices, analyse modus operandi, make comparisons, etc.

 Judges will be able to consult the criminal archives for the needs of their cases.

During the transition period where numerous territorial services will still not be equipped with WAPIS terminals, the DACORE will need to respond to requests from services when investigators need to conduct investigations and searches in the database.

The DACORE’s management should therefore have a point of contact to whom requests can be addressed, a function which will need to use at least one dedicated WAPIS terminal running 24/7.

"CHECK" FUNCTION

This function should become a routine, mandatory operation, primarily for frontline agents.

It consists of verifying in the WAPIS database whether a person is “wanted”, whether a vehicle has been reported stolen, whether a weapon has been reported or stolen, whether an administrative document has been flagged up or whether found items have been used in previously-committed crimes or misdemeanours.

As a result, all types of identity check (cross-border, roadside checks, etc.) should also entail checking the WAPIS databases.

It is up to the heads of unit to ensure compliance with any instructions that have been circulated by their supervisory authority, after a decision by the National Committee.

During the same period and for the same reasons as for the “search” function,
the services should get in touch with the DACORE, if they are unable to get to a nearby service equipped with a WAPIS terminal, so they can make administrative checks concerning people, vehicles, administrative documents, weapons and generic items.

This function may or may not be combined with the “search” function, depending on the amount of incoming data.
Judges are directly involved in using the WAPIS system, for several reasons.

› **Looking up an individual’s criminal record**

Appointed magistrates will be able to use a WAPIS terminal to look up people’s criminal history.

› **Recording criminal evidence in the nominal database**

Judges will be able to record in the nominal database any criminal evidence concerning individuals wanted by examining judges who are the subject of conviction in absentia or failure to appear in court, or the subject of specific measures restricting their personal freedom.

The DACORE will be the single point of contact for the courts.

› **“Record of court proceedings”**

When filling in the “record of court proceedings”, competent magistrates (prosecutors, clerks of the court, sentence enforcement services, etc.) will update the final status of individuals who have been to court (e.g. convicted, case dismissed, pardoned, filed without further action).
In order to ensure the quality and exhaustiveness of national databases and, subsequently, of international, regional and INTERPOL systems, it is vital to determine the role and allocation of responsibilities of the various players in the criminal proceedings in terms of quality control.

**ALLOCATION OF ROLES AND RESPONSIBILITIES**

**IN THE LOCAL SERVICE**

- **Quality control of the proceedings from start to finish**
  As soon as criminal proceedings begin (whether legal, preliminary, crime or flagrante delicto, on letter of request), the local service should organize, according to the specific guidelines from its own management, a quality control process for data entered in the procedure so that the national databases can be updated in the most satisfactory manner possible, as soon as the first actions in the proceeding have been validated.

  This quality control process starts with the writer, and involves the whole chain of command right up to the unit commander, at the time of transmission.

  All elements in the procedure are important in terms of correctly entering information and operational or statistical use of national databases, and can lead to rejection if anything has been omitted. For example:

  - An incorrectly classified offence will bring up incorrect search results when searching the criminal record file.
  
  - The identity of a victim that is incorrectly entered, or not entered at all, using the screens provided, will distort the search in the criminal record file and prevent the fact being counted if the unit of account is the victim.
  
  - The same applies to the implicated party if something has been forgotten, with the same consequences as for the victim.
  
  - An incorrectly entered marital status will have repercussions on use of the information and could cause serious issues.
› Checks must be made that the links between the various offences indicated in the procedure and all the people who have been victims or implicated have been correctly managed. An offence is, in the majority of cases, attached to at least one person.

› Items that are incorrectly or not entered can give false search results in the generic file.

› **Specific checking of objects in order to update the generic lost or stolen property file**

The principle governing the generic lost or stolen property file establishes that management of addition to the file is the exclusive responsibility of local services according to how the management and quality control of their criminal proceedings is specifically organized.

Only the local service can confirm the normal character of a rejection from the file, for example when the victim is incapable of accurately describing the item concerned, or make the necessary corrections when there have been data entry errors.

› **Updating found items in the generic property file**

Updating the file with de-registrations (found items) is the exclusive responsibility of the local service that wrote the proceeding, stating that the lost or stolen item has been found, regardless of the service or institution that originated the theft procedure.

This internal manual update is essential in order to:

› Cancel the reporting form in the file and keep a record of it;

› Send, via the file, all the information relating to the item being found to the criminal record file (date and reference of the found item procedure). In fact, since finding a stolen item is not dealt with in a procedure by a specific statement of finding, the link between the lost or stolen item and the found item cannot be made automatically.

**AT NATIONAL LEVEL**

This level is handled by the DACORE, which is the supervisory body for the WAPIS system.

› **Registering “wanted persons” in the nominal database**
On the basis of the national protocol provided, the DACORE is responsible for checking the legality and lawfulness of requests to register “wanted persons” in the nominal database, which are sent to them by all the services concerned and sometimes also by administrations.

The requesting services should send the request to the DACORE, who will register it once it has been through quality control.

› Updating search forms in the nominal database
Whenever a person who is “wanted” in the nominal database is found, the service that has found them must always send as quickly as possible the de-registration form provided to the DACORE, who will cancel the entry after verification and checking.

The DACORE will make regular checks to confirm the validity of the search forms and will ask the services concerned for any updates.

› Updating found items in the lost or stolen vehicles file
The same as before for the generic property file, updating the lost or stolen vehicles file is the exclusive responsibility of the territorial service that wrote the proceeding, stating that the lost or stolen vehicle has been found, regardless of which service originated the complaint or the report.

The service that has found the vehicle will find in the vehicle search form all the information and instructions indicated by the requesting service that they need to execute. It will also be responsible for ensuring that the DACORE receive the de-registration form with a copy of the found item procedure, which will lead, after checking, to the search being cancelled.

› Importance of the collection file
As LEOs from local services do not have a computer terminal allowing them to enter data directly in the WAPIS database, they need to fill in the collection file that should routinely accompany the complaint or criminal proceedings file. This should allow the data entry operators to fill in the database without needing to analyse the original documents in depth.

From then on, the importance of exhaustive quality control, overseen at local service level, is essential before final transmission of the procedure.

The unit commanders or heads of unit, being aware of the importance of their role, must be particularly careful to comply with the instructions regarding quality control in order to prevent records being rejected from the database.