

The logo features the word "EUROPOL" in a bold, blue, sans-serif font. The letters are arranged horizontally, with the "O" in the middle being slightly larger and containing a white dot. Behind the text is a stylized graphic consisting of a central blue circle with several yellow lightning bolts radiating outwards, creating a sense of energy and global reach.

E U R O P O L

Europol Information Management

Products and Services

Europol is the European Union law enforcement organisation that handles criminal intelligence. Its aim is to improve the effectiveness and cooperation between the competent authorities of the member states in preventing and combating serious international organised crime and terrorism. The mission of Europol is to make a significant contribution to the European Union's law enforcement action against organised crime and terrorism, with an emphasis on targeting criminal organisations.

Europol supports the law enforcement activities of the member states mainly against:

- illicit drug trafficking;
- illicit immigration networks;
- terrorism;
- forgery of money (counterfeiting of the Euro) and other means of payment;
- trafficking in human beings (including child abuse);
- illicit vehicle trafficking;
- money laundering.

In addition, other main priorities for Europol include crimes against persons, financial crime and cybercrime. This applies where an organised criminal structure is involved and two or more member states are affected.

Europol provides support by:

- facilitating the exchange of information between member states via their liaison officers assigned to Europol as representatives of their national law enforcement agencies;
- providing operational analysis in support of operations;
- generating strategic reports (e.g. threat assessments) and crime analysis on the basis of information and intelligence supplied by member states and third parties ;
- providing expertise and technical support for investigations and operations carried out within the EU, under the supervision and the legal responsibility of the member states concerned.

Europol is also active in promoting crime analysis and harmonisation of investigative techniques within the member states.

Contents

INTRODUCTION	3
Representation at Europol.....	3
EUROPOL INFORMATION MANAGEMENT	6
Europol's Information Management Process.....	7
Evaluation and Handling Codes	7
Data Protection and Confidentiality	10
INFORMATION MANAGEMENT PRODUCTS AND SERVICES.....	12
Sharing of Information	12
Operational Analysis	13
Strategic Analysis.....	14
Operational Support	14
EUROPOL COMPUTER SYSTEMS.....	17
Information Exchange System (InfoEx)	17
Information System (IS).....	18
Europol Analysis System (EAS)	20
Index System (IxS)	21

Introduction

The Europol information management model describes the information flow at Europol level. Developed in co-operation with the member states and agreed by heads of Europol national units, it defines the practical business of information handling and exchange between Europol and its partners. It also ensures adherence to strict data security regulations.

This booklet gives answers to questions about the role of Europol, the information management process and the use and dissemination of data supplied to Europol. Explanations of the main Europol products in the area of sharing of information, operational and strategic analysis as well as operational support can also be found.

Practical examples appear in the text to expand on the explanations in order to help law enforcement personnel better understand the extent of the activities that take place at Europol.

Representation at Europol

Liaison officers

All EU member states have at least one liaison officer at Europol. The member state liaison officers represent their country of origin and operate under the responsibility of their own member state. Third parties (i.e. non-EU states and international bodies) having a co-operation agreement with Europol may also host liaison officers at Europol, subject to an agreement.

Europol has established and maintains its own liaison offices in Washington (USA) and at the headquarters of Interpol in Lyon (France).

Member state liaison officers are authorised to exchange information between their national unit, Europol and other member states. Furthermore they are authorised to consult the various Europol computer systems, in order to fulfil their role. The liaison officers assist in the exchange of information between their national unit and Europol in particular by:

- providing Europol with information from the seconding national unit;
- forwarding information from Europol to the seconding national unit;
- co-operating with the officials of Europol by providing information and giving advice as regards analysis of the information concerning the seconding member state.

Third party liaison officers have in principle the same tasks and facilities as the member state liaison officers, with the exception of access to the Europol computer systems.



Figure 1: Europol building.

Europol National Units

The Europol national units (ENUs) are situated within each member state and are staffed by a mixture of law enforcement staff and customs officials as well as civilian members of staff. The Europol national unit is the only liaison body between Europol and the member states; all information is exchanged through this unit. The national units have access to relevant national data and to the Information System of Europol (IS).

The formal tasks of the Europol national units as described in the Europol Convention are outlined below:

- to supply Europol through their own initiative with information necessary for it to carry out its tasks;
- to respond to Europol's requests for information and advice;
- to keep information up to date;
- to evaluate the information in accordance with national law for the competent authorities and transmit this material to them;
- to issue requests for advice, information and analysis to Europol;
- to insert data in the computerised systems;
- to ensure legal compliance in every exchange of information between themselves and Europol.

National Contact Points

The same principles and responsibilities applicable to the member states' Europol national units apply equally to the units designated in each of the third parties as the point of contact with Europol for the exchange of information within the frame of the co-operation agreement. These units are called National Contact Points (NCPs) and they operate as a Europol national unit except they have no access to the Information System of Europol. They may

be linked to Europol with electronic dedicated lines equipped with encryption devices for enhanced protection.

The communication of information is realised via the third party liaison desk at Europol or where a liaison desk does not exist directly via Europol's Information Management Operations Unit. This is the unit responsible for receiving and transmitting data to third parties . This ensures a controlled and structured way of exchanging information between Europol and non-EU states and co-operating international bodies.

Europol Information Management

The vision of Europol is to become a world-class centre of excellence to support the EU member states' fight against organised crime and terrorism. It can only do this in full cooperation with the member states on which it depends for information contribution.

$$E=mc^2$$

Europol = member states contributions²

Information management is a general framework for Europol. It is a reference for information related business and a guide for law enforcement investigators. It can be used for the prioritisation of resources at Europol. Information handling and standardised procedures contribute to quality control of the products and services of Europol through co-ordination of work of the Europol units, Europol liaison officers and through awareness of Europol throughout the member states.

Europol established the Strategic Information Management Committee (SIM) being a horizontal working group composed of senior Europol officials with authority in the domain of information management (IM). It acts as a focal point for information and questions in the area of Europol IM. Supporting the operational side of IM at Europol, the SIM brings together constraints of technology and politics and recommends actions to respond to organisational IM needs.

The operational work at Europol ensures the maximum value of the use of information received from member states, through utilisation of the information management cycle. This cycle is the process of collection of information, evaluation, collation, analysis and subsequent dissemination of an enhanced (information) product for investigative use within the member states. Enhanced information is the key with which to identify future deployment and direction of resources in the fight against serious organised crime.

One of the main benefits of information handling will be the ability to prioritise work. A well-defined process of the flow of information will facilitate all the activities from the collection of relevant data towards a Europol product required by its final users. All the steps in the information management process facilitate the tasking and co-ordination at all levels. Information channelling occurs amongst the member states and between member states and Europol using the information exchange system. It also occurs between member states, Europol and non-EU States and international bodies.

The information management process has to be seen as something ongoing which needs to be adopted to new challenges and changing environment. All Europol's partners are invited to continue their contribution.

Europol's Information Management Process

Information management is a process based on raw information, which can be about a crime, perpetrator, suspected person, etc. Information management's objective is the enhancement of the basic information which provides additional knowledge about the activities of criminals. Proper information management provides a clearer picture, which is normally unknown to the investigating authorities and is intended to be used to enhance the efforts of law enforcement investigators.

The result focussed on is '**information designed for action**'. The exchange of enhanced information is the core business of Europol; it provides support to law enforcement efforts and is a fundamental tool in the investigation and eradication of organised criminality.



Figure 2: Information management process.

As the diagram shows, raw information is evaluated and collated with other information received from various sources. The information may then be examined or analysed to identify patterns or trends of criminal activity and finally disseminated to the member state(s) that it affects. The security of information and data received at Europol is of paramount importance, it is therefore Europol's position that all data is evaluated and assigned a handling code before transmission to Europol. The product disseminated from Europol to the respective member states will be coded accordingly.

Evaluation and Handling Codes

Evaluation codes

Evaluation codes are based on the 4x4 system used in the member states to establish the authenticity and accuracy of the supplied information. Evaluation codes consist of source codes and information codes.

Source Codes

- A** where there is **no doubt** of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be **reliable in all instances**;
- B** source from whom information received has **in most instances proved to be reliable**;
- C** source from whom information received has **in most instances proved to be unreliable**;
- X** the reliability of the source **cannot be assessed**.

Information Codes

- 1** information whose **accuracy is not in doubt**;
- 2** information **known personally** to the source but not known personally to the official passing it on;
- 3** information **not known personally** to the source but **corroborated** by other information already recorded;
- 4** information which is **not known personally** to the source and **cannot be corroborated**.

The use of the 4x4 evaluation system is embodied in the analysis regulations as well as in the operational agreements Europol has signed with third parties

		EVALUATION OF THE SOURCE				
		A	B	C	X	
		where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances	source from whom information received has in most instances proved to be reliable	source from whom information received has in most instances proved to be unreliable	the reliability of the source cannot be assessed	
EVALUATION OF THE INFORMATION	1	information whose accuracy is not in doubt	A1	B1	C1	X1
	confirmed information					
	2	information known personally to the source but not known personally to the official passing it on	A2	B2	C2	X2
	3	information not known personally to the source but corroborated by other information already recorded	A3	B3	C3	X3
unconfirmed information						
4	information which is not known personally to the source and cannot be corroborated	A4	B4	C4	X4	

Figure 3: Evaluation codes used in the information exchange via Europol.



Handling Codes

Handling codes are both a complementary and necessary addition to evaluation codes in respect of information exchanged via Europol. Handling codes protect the information source, ensure future security of the information, and ensure that the information is processed in accordance with the wishes of the owner of the information.

The codes H1 and H2 are applied when the most common restrictions on the use of the information are applicable. H3 may be used to include additional restrictions, permissions and/or purpose of the transmission of the data.

The Handling Codes read as follows:

- H1** This information must not be used as evidence in judicial proceedings without the permission of the provider.
- H2** This information must not be disseminated without the permission of the provider.
- H3** Other restrictions apply.
The other restrictions, permissions and/or purpose of the transmission of the data should be described in free text.

	Europol Information Exchange		
IE	164417_001	Refers to IE	
ENU ID		Request ENU ID	
REQUEST from	IMT4 - Operational Exchange		
Sent to	Czech Republic (CZ); Germany (DE); Romania (RO); Spain (ES); Norway (NO) via Europol; LO Europol (Washington);		
Main Subject	Drugs		
Creation	2008-11-10 T 09:43 +01:00	Submission	
		Deadline	

Handling Codes	
This information may be transmitted or utilised only by Europol and the competent authorities of the Member States in order to prevent and combat crimes falling within the competence of Europol and to prevent and combat other serious forms of crime.	
This information will be deleted on <input type="text"/> unless new information is added that requires continued storage.	
<i>Additional restrictions/permissions (optional):</i>	
<input checked="" type="checkbox"/>	H-1 This information must not be used as evidence in judicial proceedings without the permission of the provider.
<input type="checkbox"/>	H-2 This information must not be disseminated without the permission of the provider.
<input type="checkbox"/>	H-3 Other restrictions apply: <input type="text"/>

Figure 4: Example of an information exchange message (InfoEx request) showing the usage of Handling Codes.

Data Protection and Confidentiality

The purpose of data protection is to afford protection to the individual about whom data are processed. This is typically achieved through a combination of rights for the data subject and conditions for those who process data. Data protection within Europol is about creating a framework for Europol's information handling that appropriately takes care of the interests of the individual on whom law enforcement data are processed.

The level of protection of Europol information is a standardised format that indicates the protection measures that need to be applied to this information.

In this respect, three types of information can be identified:

- **(Europol) public information** = information which is marked or is clearly recognisable as being public information. The decision to allocate the public status to information can only be taken by head of unit or department within Europol, or a person under his authority, where the information originates;
- **Europol BPL information** = Basic Protection Level information (BPL);
- **Europol classified information** = information subject to a special security regime and marked with one of the classification levels:

The Europol Classification Levels

Europol Restricted
This level is applicable to information and material the unauthorised disclosure of which could be disadvantageous to the interests of Europol or of one or more member states.
Europol Confidential
This level is applicable to information and material the unauthorised disclosure of which could harm the essential interests of Europol or of one or more member states.
Europol Secret
This level is applicable only to information and material the unauthorised disclosure of which could seriously harm the essential interests of Europol or of one or more member states.
Europol Top Secret
This level is applicable only to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of Europol or of one or more member states.

A table of equivalence with Europol has been established for all classification levels in each member state. Tables of equivalence exist also for third parties having a co-operation agreement with Europol.

Information which is subject to the Basic Protection Level and to which no classification level has been assigned are marked as “Europol Unclassified not for public dissemination”.

Special attention is paid to handling of information classified as Europol Confidential and above.

Information Management Products and Services

Example:

The National Police in Spain commenced an investigation into a criminal organisation suspected of being involved in drugs trafficking, money laundering and illegal immigration activities across a number of EU member states and Norway.

What is the added value of Europol to this scenario?

Other countries in or outside the EU may already have information on the persons identified in Spain and investigations may already be ongoing with possible links to the Spanish investigation. The Europol national unit in Spain and the Spanish liaison officers at Europol may consult the Europol computer systems for possible hits. In addition to information on the identified persons, other details may also be known within the Europol systems, such as means of communication, means of transportation, bank accounts, modus operandi, money laundering techniques etc. This additional information could assist Spain and the other countries concerned to exchange information via Europol thus enhancing the investigation efforts.

In addition, member states may request Europol to conduct searches in open source material and expert databases, such as company registers and the Ecstasy logo system, in order to provide any available additional intelligence.

Non-EU States and international bodies, with which Europol has concluded a co-operation agreement, can also submit requests to Europol, subject to the terms and conditions of the relevant agreements.

Sharing of Information

There are two main tools at Europol to support the sharing of information: the Information System and the Information Exchange System.

Information System

The main objective of the Information System of Europol (IS) is to support EU member states and Europol in fighting against all forms of serious international crime and terrorism. The IS provides capabilities for storing, searching, visualising and linking information related to trans-national crimes, allowing law enforcement agencies across Europe to co-operate efficiently in their investigations. The system supports automatic detection of possible hits between different investigations and facilitates the sharing of sensitive information in a secure and reliable way. More information on the IS can be found in the section *Europol Computer Systems*.

Information Exchange System

The Information Exchange System (InfoEx) is used to manage the exchange of operational information between member states and Europol. Also third parties Europol has a co-operation agreement with are part of this communication channel. More information on the InfoEx can be found in the section *Europol Computer Systems*.

Operational Analysis

Analysis Work Files (AWF)

The Analysis Work File (AWF) is an instrument unique to Europol. It is the means by which Europol provides support to investigations being carried out in member states. As such, AWF support is often closely linked with a Joint Investigation Team (JIT). The Europol support consists of intelligence analysis, expert advice and assistance. It can be provided remotely from the Europol premises, or in the field.

The principle of the AWF is relatively simple. Investigations being carried out in different national jurisdictions often show significant linkages between them. This is due to the common involvement of international criminal structures in cross-border crime. These national investigations produce information which is supplied via secure communication channels to the Europol Analysis Unit. This information is centralised and processed within the Europol Analysis System. This is a secure system, accessible only to the analysts who work on the AWF.

The analysts initially look for simple cross-matches within the data. Subsequently, more detailed analysis will be performed in line with the objectives of the AWF, and the main targets of the investigations. The aim of all analysis is to provide direction to investigators to assist the progress of their investigations, following new leads and filling intelligence gaps. Accordingly, a circular flow of data is created such that the AWF and the investigations feed each other with new information. In this way, the AWF acts as the central point allowing national investigations to benefit from information obtained in other jurisdictions. The overall aim of increasing the efficiency and effectiveness of the competent authorities of the member states is thus achieved.

All work within an AWF has to comply with the regime imposed by the Europol Convention, and the Rules for Analysis Work Files. These establish the basic pre-conditions for an AWF: It must be a Europol mandated crime area, affecting two or more member states and involving an organised crime structure.

Index System (IxS)

The index system provides a search function, which refers to the contents of the Europol Analysis System. It enables member states and Europol to determine if a subject of interest exists in any of the AWFs. More information on the Index System can be found in the section *Europol Computer Systems*.

Strategic Analysis

The **EU Organised Crime Threat Assessment (OCTA)** is one of the core products of Europol. As its name suggests, it develops a threat assessment of current and expected new trends in organised crime across the EU. The assessment is based upon existing knowledge and expertise and it is drawn up in order to enable the decision makers to take the appropriate action to counter the anticipated threat.

The OCTA marks a new approach to the way in which Europol, the European institutions and the member states will think and operate in the future and in so far, it is a first step into a change of paradigm in policing. It also fits in firmly with the aim of The Hague Programme to provide a forward looking approach to fight organised crime in a more pro-active than in a re-active manner.

A **threat assessment** contains the analysis and evaluation of the character, scope and impact of criminality (for example, the impact of money laundering on the EU; the impact of South American drug cartels on the EU).

A **risk assessment** identifies and examines vulnerable areas of society that are, or could be, criminally exploited; this type of report offers recommendations on potential counter measures.

A **general situation report** describes current crime situations in general or specific areas (for example, drug situation in the EU; the amount of money laundered in the EU; the situation on terrorism in the EU).

Operational Support

Joint Investigation Teams (JIT)

A Joint Investigation Team is an investigation team set up on the basis of an agreement between two or more member states, for a specific purpose, which will be carried out for the benefit of the participating countries, with a possible participation of third parties and Europol. It is meant to support criminal investigations, not affecting, overlapping or replacing existing means for international law enforcement cooperation.

JITs offer a legal and operational framework for a multinational and multi-agency approach to criminal investigations, providing the possibility for seconded members to take certain investigative measures and to facilitate mutual legal assistance. These measures may be executed within the territory of any member state participating to a JIT agreement, subject to national legislation. Also, JIT members may carry out investigative measures without the need for further requests under the traditional mutual legal assistance regime.

Europol officials may participate in a support capacity, by assisting in all activities. This may relate to the exchange of information and the co-ordination of information flows as well as the provision of analytical, investigative, forensic or financial support and general support such as meeting facilities or language support.

Knowledge Management Platform

It is widely accepted that efficient cross-border co-operation is essential to the fight against serious international organised crime, and knowledge management is a key concept in that co-operation. Europol puts efforts in improving knowledge management within the EU. One of the services used for this purpose is called the **Knowledge Management Centre (KMC)**, a database which stores uncommon and rarely used forms of investigative expertise e.g. high tech crime, witness protection, negotiation techniques, and reliable interpreters in rare and uncommon languages/dialects etc.

Europol currently provides an indirect search facility to the KMC to Europol staff, all member states and third parties with a co-operation agreement with Europol.

The KMC will be developed into a web portal able to provide a unique repository for member states' Law Enforcement Authorities (LEA) and their partners in a range of key operational support areas, such as witness protection, informants handling, controlled deliveries, hostage taking and advice on tactical planning for operations. The new Knowledge Management Platform will be accessible directly to LEA via a secure website.

Member states and third parties are provided by Europol with the **Ecstasy and Cocaine Logo Catalogues**, both products with a view to identifying links between seizures and initiating information exchange, investigations and forensic profiling for the targeting of criminal groups. Both products are part of Europol's Ecstasy and Cocaine Logo Systems (EELS and ECLS).

Terrorism Related Information

Europol provides the member states and third parties with periodic special briefing papers where all available information in the area of terrorism is collected, compiled and analysed with a view to demonstrating certain developments in that area and updating the competent agencies accordingly. The main product in this area is the yearly **Terrorism Situation and Trend Report (TE-SAT)**.

Within the same frame Europol launched the **Check the Web** electronic portal, which store information regarding Islamist extremist websites and statements of terrorist organisations published on the Internet, with the objective of putting that information at the disposal of Europol staff and member states law enforcement authorities, via a secure connection to the Europol National Unit.

Consultation of Schengen Information System

Europol has been granted access to the Schengen Information System (**SIS**) where information, provided to Europol from Non-EU States and international bodies with which Europol is co-operating, can be cross-checked. This service is also available for those member states that do not yet have access to the SIS.

Other Information Services

Europol offers other services to member state law enforcement authorities and third parties such as searches in open source material and company registers. Specific searches for diverse information are available to the member states through their Europol national units and Europol liaison officers.

Training

As part of Europol's main responsibilities, training can be provided on request or on Europol's own initiative, to the law enforcement agencies in the member states, and to Europol's co-operation partners in one or more of the following areas:

- cyber crime;
- informant handling;
- illicit synthetic drugs laboratories;
- forgery of money;
- non-cash payment fraud;
- strategic analysis;
- crime intelligence analysis;
- operational analysis;
- awareness training.

Europol Computer Systems

Information Exchange System (InfoEx)

The Information Exchange System (InfoEx) is used to manage the exchange of operational information between member states and Europol. Also third parties with which Europol has a co-operation agreement with are part of this communication channel.

The InfoEx is available at the Europol Headquarters for member state liaison officers and duly authorised Europol officials. The exchange of information with Europol national units in the member states is secured via encrypted point-to-point lines. The third parties have an indirect access to this system through Europol's Information Management Operations Unit.

The InfoEx provides four main functionalities: creation of a **Request**, creation of an **Answer**, **Search** engine and finally a catalogue of **Groups** to which requests may be addressed.

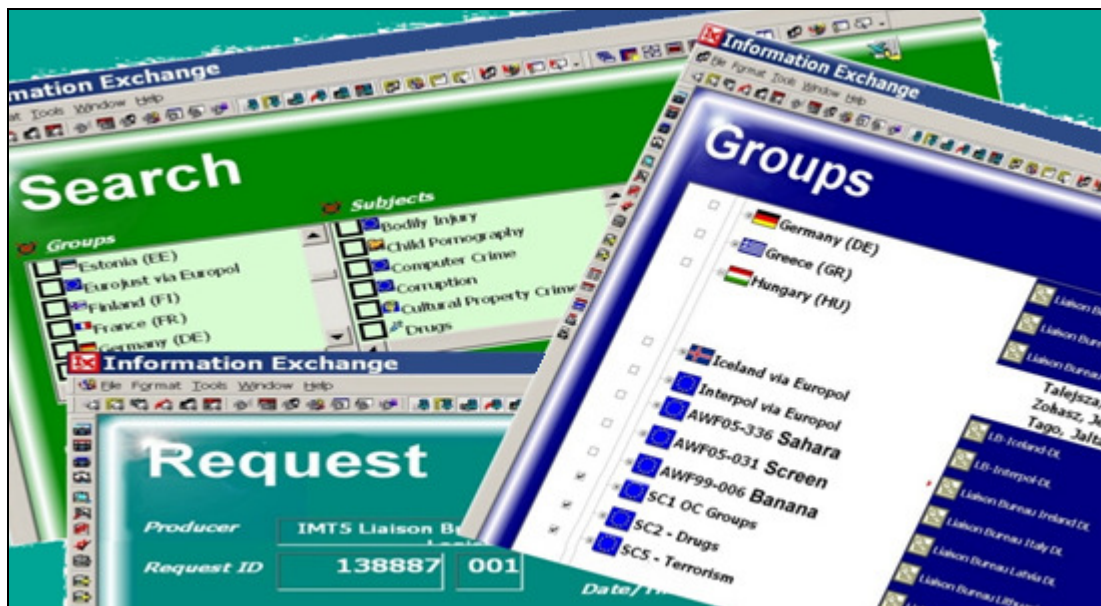


Figure 5: Information Exchange System.

Another feature of the InfoEx system is that exchanged information can be retrieved with the search engine and transferred for further use to the various operational Europol units.

Example:

The French national police have arrested persons suspected of transporting illegal immigrants from France to the United Kingdom. France subsequently initiates an exchange of relevant data with the UK. It appears that the smuggling method, the modus operandi, is as yet unknown to the authorities. As a result of the investigation is of interest to Europol, the information was transferred via the InfoEx system to the Europol experts within the Serious Crime Department. The investigation, in particular the identified modus

*operandi, is included by Europol in **information bulletins** that are disseminated to law enforcement agencies in the member states via the Europol National Units.*

In addition, an in-depth analysis of this and other related cases may result in specific bulletins, threat/risk assessments and possible operational activities.

A project is ongoing to replace the InfoEx with a modern information exchange tool (SIENA) in 2009. In addition to the Europol Headquarters, the SIENA will be directly accessible for authorised users in the member states' Europol National Units.

Information System (IS)

The purpose of the Information System of Europol (IS) as an intelligence database is to support member states, Europol and Europol's co-operation partners in fighting all forms of serious international crime and terrorism. member states may also use the data stored in the IS to combat other serious forms of crime.

The IS supports all operational activities within the Europol framework. It provides a rapid reference to information available to law enforcement agencies in the EU member states and to Europol on suspected and/or convicted persons, criminal structures/organisations, criminal offences and means used to commit them.

The IS provides capabilities for storing, searching, visualising and linking information related to trans-national crimes, allowing law enforcement agencies across Europe to co-operate efficiently in their investigations. The system supports automatic detection of possible hits between different investigations and facilitates the sharing of sensitive information in a secure and reliable way.

The IS is a shared advantage and responsibility of the EU member states and Europol. Each member state and Europol can be considered as having an account in the IS for which they are responsible. Information deposited therein is made available to other EU investigators and is automatically compared with information in the IS deposited by other member states. The purpose of this is to look for matches with a view to enhancing intelligence and providing new leads for further investigation.

The IS was developed by Europol's in-house software development unit. Hosted at Europol's Headquarters in The Hague (The Netherlands), it is available in 21 languages to the law enforcement agencies of all EU member states.

Information Sharing

The Europol national units have direct access to the IS in order to run queries and to insert and maintain data in it. member states' liaison officers at Europol and duly empowered Europol officials also have direct access to the IS to perform these actions. In specific situations as described in the Europol Convention, third parties may also have indirect access to the information in the IS through Europol. They may also contribute data to the system.

Data Ownership

Data can be inserted into the IS in a manual or automated way. The data inserted into the IS remain under the full control of the inputting party (data owner); they cannot be altered in any way by Europol or another member state. The owner is responsible for data accuracy, reliability and verification of storage time limits, and ensuring that they are kept up-to-date.

Data stored in the IS may only be disseminated and/or used in accordance with the handling codes and Europol protection levels applied by the owner of the information.

What kind of data can be stored in the IS and how?

The data in the IS are stored in different objects (such as persons, cars, identity documents, etc.), which must be linked to each other to create a structured picture of a criminal case.

There are several ways of viewing data stored in the IS. One example is the Chart View, which gives a graphical overview of the stored information. It provides insight into links between data objects:

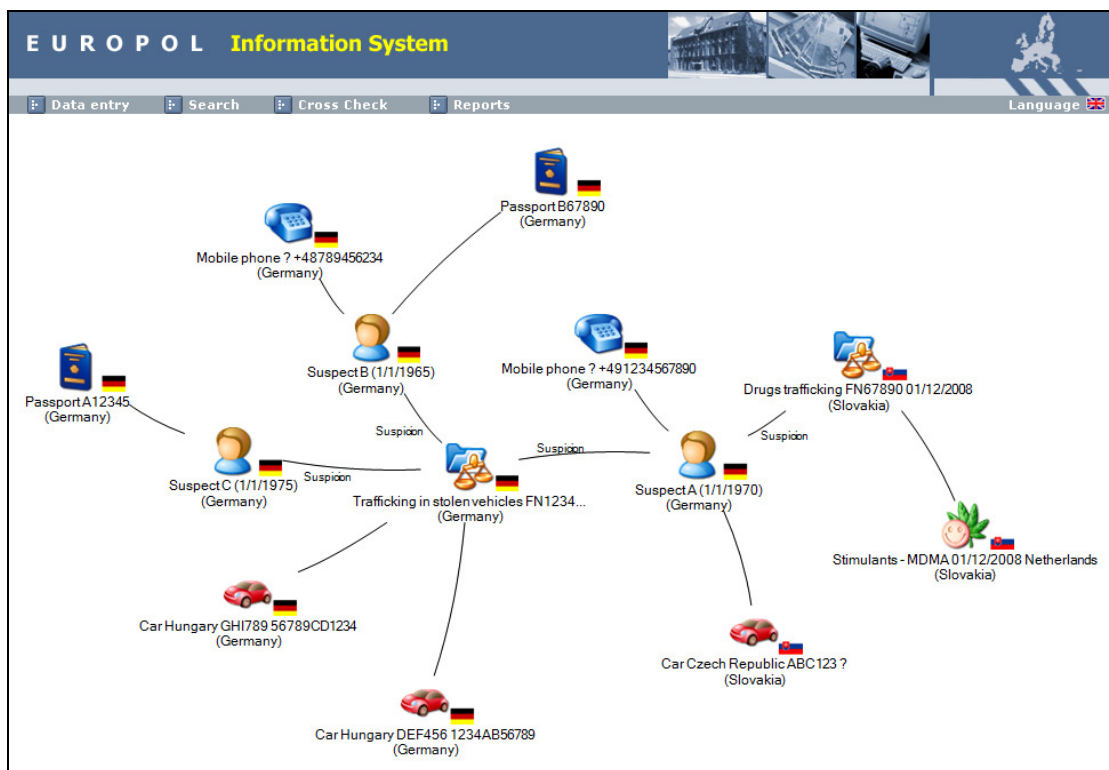


Figure 6: Example of the Information System Chart View.

Example:

Germany has provided information to the IS on an organisation suspected of stealing expensive luxury vehicles that are transported to Poland via Austria and the Czech Republic. The information includes personal details on addresses, telephone numbers etc. Slovakia is conducting an investigation into a suspected money laundering activity in relation to drug trafficking, and

one of the suspects appears to have regular contact with a German telephone number. A search in the IS results in a possible hit; after further information exchange through the liaison officers at Europol it is established that both criminal organizations are connected and involved in money laundering activities.

Future

In the near future, the IS will reach an even larger user community as, in addition to the Europol National Units, other designated competent law enforcement authorities in the EU member states may also be connected to the IS to run queries.

Future versions of the system may provide facilities to match biometric data, such as DNA profiles, fingerprints and photographs. SIENA, the new platform for the exchange of operational information between Europol and its partners, will interface with the IS for further enrichment of police information.

The number of records in the IS has remarkably grown since the launch of the system. All member states have contributed data to it. It is foreseen that at least 16 member states will be able to connect their national databases to the IS and upload data automatically. This will increase the IS content and consequently the hit rate.

Europol Analysis System (EAS)

What is the function of the Europol Analysis System?

The Europol Analysis System (EAS) supports the work of Europol analysts. Direct access is permitted only to analysts working within specific analysis work files (AWFs). The system is dedicated to the analysis work files and has a number of specialist tools and software that facilitates a complete analysis of information supplied by the member states. The system is a vital tool in the processing and collation of information received from the member states.

The analysis work files contain clearly specified categories of persons (criminals, suspects, contacts, associates, victims, witnesses and informants) and data categories relevant to those persons, in accordance with the analysis work file regulations. The list of these categories is defined in a document known as the 'opening order'. Each analysis work file is unique in respect of the information that can be stored within it.

What does the analysis aim to achieve?

Analysis is a key element to Intelligence Led Policing. All analysis aims to "go beyond the facts". It takes incomplete and diverse data, collates it and tries to look at it in such a way that a new meaning can be seen from it, this can be to develop hypotheses or to identify intelligence gaps both of which allow the analyst to provide direction to the investigator. In this way it can be said that "added value" is given to the data.

To generalise, the analysis within an AWF is, according to the objectives and current focus, attempting to build up a picture of inter alia:

- group structures;
- individual roles;
- modus operandi;
- routes for commodities or money;
- sequences of events.

This is not to be seen merely as an academic exercise by which the crime problem can be described. That description is a vital element towards understanding the scale and nature of the problem, and in turn it contributes towards identifying areas of vulnerability. In the end this is the key issue as it provides the best law enforcement opportunity.

At a simpler level, by collecting diverse data from investigations throughout the EU, the AWF is often able to link together seemingly insignificant details like the same telephone number appearing in the diary of different criminals by which separate investigations in different member states can be linked together.

Index System (IxS)

The Index System (IxS) provides a search function, which refers to the contents of the Europol Analysis System. It enables member states and Europol to determine if a subject of interest exists in any of the AWFs.

Who can access the Index System?

The Europol Director, the Deputy Directors and duly empowered officials of Europol and the member states' liaison officers can access the system.

What data can be retrieved from the Index System?

The data that can be retrieved refers to the contents of the Europol Analysis System. Access is defined in such a way that it is possible to determine whether or not a subject of interest is available in any of the AWFs, but it is not possible to establish connections or further conclusions regarding the content of the files.

Example:

An Austrian investigation of a criminal organisation suspected of trafficking in human beings has indicated possible links with Germany. A person in Germany is suspected of being the middleman facilitating the international transfers.

Via the liaison officers from Austria and Germany information is exchanged using the InfoEx system. The Index System and the Information System are consulted in order to check known details of the suspected persons in Austria and Germany. The name of one of the suspected persons is identified by the Index System as being in a specific AWF.

This AWF contains data on organised transports of cocaine between South America and some EU countries. The participating member states in this analysis work file are the Netherlands, Belgium and Denmark. Belgium originally provided the information relating to the suspected person to the AWF. This leads to the exchange of information between Germany, Austria and Belgium via the respective liaison officers. The result of this exchange is the identification of possible links between two criminal organisations. Further analytical work and possible joint investigations may then lead to the successful dismantling of both criminal organisations.

For more information contact

EUROPOL

PO Box 90850

2509LW

The Hague

The Netherlands

www.europol.europa.eu