COUNCIL OF THE EUROPEAN UNION

Brussels, 3 June 2014 (OR. en)

6721/3/14 REV 3

DAPIX 24 ENFOPOL 45

NOTE

From:	Presidency
To:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	7968/08
Subject:	Draft SPOC Guidelines for international law enforcement information exchange

In June 2013, the European Council mandated the future Presidencies to start discussions on the future strategic guidelines in the area of freedom, security and justice with a view to its June 2014 meeting.

In particular with regard to strengthening the cooperation of MS' law enforcement authorities, MS stressed that the exchange and management of information should be considered in a systematic manner. Full advantage should be taken of all opportunities, at technical and organisational level, created over the past years for gathering, analysing and exchanging information. In this context, some MS mentioned the merits of a single point of operational contact (SPOC) in order to cope with the increase of cross-border information exchange.

The methodology of setting up a SPOC has been discussed within DAPIX over the last years. The Presidency suggests to take stock of the recent evolutions and, in particular in the light of experience with the operational function of SPOCs in Member States, to update the "Manual of Good Practices concerning International Police Cooperation Units at National Level" (see doc. 7968/08 ENFOPOL) with a view to setting up SPOC Guidelines.

The draft Guidelines, in particular, keep in mind the use and implementation at national level of SIENA for the purpose of a secure cross-border data exchange, case management and operational cooperation within one single secure environment.

The Presidency recommends to thoroughly examine the use of SIENA III as the prime tool for exchanging operational and strategic intra-EU crime related information and intelligence, both with regard to the Europol mandate and to bilateral information exchange between Member States. Europol currently aims at a further enhanced interoperability between the national case management system and SIENA by expanding the interaction between both interfaces allowing more SIENA actions to be performed directly from the case management system such as searches, task assignment and national workflow definition of incoming and outgoing SIENA messages.

The Presidency invites Member States

- to regularly check and update the national fact sheets on structures for international law enforcement cooperation set out in the addendum to this note, and

- to take note of the draft SPOC Guidelines set out in this note and agreed by DAPIX on 2 June 2014 with a view to submitting it to COSI and the Council for endorsement.

Draft SPOC Guidelines for international law enforcement information exchange

Introduction

The current Guidelines are meant for those units within the Member States' law enforcement authorities that are responsible for international law enforcement cooperation.

There are many different forms and channels of international law enforcement cooperation, each with its own purpose, needs, specific characteristics, ways of communication etc.

It requires a lot of Member States' resources to service all these channels in the best possible way. Member States, both as a requested or a requesting State, had to set up efficient structures, or improve existing national platforms in order to cope with the increased international information exchange since the entry into force of the Council Framework Decision on simplification of information exchange (the so-called Swedish Framework Decision), the "Prüm Decision" and any further implementation of the principle of availability and the principle of equivalent access[1].

The "one stop shop" strategy has to be, as far as possible, recommended.

This document aims to provide guidelines and examples for the above-mentioned units to maximise the use of their resources, avoid overlaps and make cooperation with other Member States more efficient, expedient and transparent.

The characteristics of an ideal international unit (or platform) are hereafter expressed. The Guidelines for a Single Point of Contact (SPOC) should be applied whenever possible and useful but always taking into account national legislation and regulations, structures and organisations.

[1] According to Art. 3 (3) of Council Framework Decision 2006/960/JHA, conditions applicable for cross-border exchange of information or intelligence shall not be stricter than those applied at national level.

Given the differences between Member States' legal situation (central/federal states), their law enforcement structures and powers (federal/regional/local levels, number of police forces, mandates of agencies, statutory responsibilities, etc.), not all guidelines, recommendations or examples will be useful or even applicable in every Member State.

Among the guidelines Member States should select the solution appropriate for their situation in view of the common and agreed aim of enhancing international cooperation and consider appropriate ways of informing other Member States about the selected solutions in view of the exchange of best practices.

The current Guidelines contain, next to this introduction, the following chapters:

- structure and composition of a SPOC for international cooperation
- national information exchange and availability of national databases and networks at the SPOC
- international information exchange: criteria for the use of cooperation channels / use of European and international databases
- staff training.

The national sheets on existing Member States' structures for international law enforcement cooperation are set out in the addendum to this document (see doc. 6721/2/REV 2 ADD 1 DAPIX 24 ENFOPOL 45).

1. STRUCTURE AND COMPOSITION OF A UNIT FOR INTERNATIONAL COOPERATION

1.1 Structure

– The SPOC is a "one stop shop" for international law enforcement cooperation: it has one phone number and one e-mail address (and other communication means, fax, etc.) for all international law enforcement cooperation requests dealt with at national level.

– It gathers under the same management structure the different national offices or contact points such as

  - the Europol National Unit (ENU)
  - the Interpol National Central Bureau (NCB)
  - the SIRENE Bureau
  - the contact point for national liaison officers posted abroad and foreign liaison officers posted in the Member State
  - the contact points designated pursuant to the "Swedish Framework Decision" and the "Prüm Decisions" (step 2 – exchange of additional information following a hit for DNA, fingerprints and VRD)
  - if any: the contact point for the regional and bilateral offices

– A front desk at the SPOC determines which office/contact point will deal with the request.

– Ideally, the SPOC houses these offices and contact points in the same building.

– The SPOC is set up through its own national legislative or regulation identity, to empower them to meet their large-scale responsibilities and duties. This is particularly useful in the light of the multi-agencies composition of the SPOC**.** The platform is placed under the responsibility of a leading Ministry (usually the Ministry of Interior) and a leading Department (usually the national criminal police).

– The relationship between the SPOC and all competent law enforcement and other concerned authorities is established through national law and regulated in written agreements, in particular with those authorities represented in the SPOC but not belonging to the "leading Ministry".

– These agreements or regulations lay down the necessary legal aspects but also practical working procedures.

– The SPOC operates 24/7 (see 3.1.2)

– The SPOC comprises the most comprehensive national competence, covering the broadest geographical and material scope as possible, to be able to handle the full range of possible requests related to law enforcement cooperation.

– The SPOC has the competence to direct any request that would be wrongly addressed to the appropriate requested authority, without returning the request to the requesting country.

– The SPOC is set up in a secure working environment, including high level of security and safety of the premises and is equipped with back up power systems.

1.2 Resources

– The SPOC is a multi-agency organisation, composed of staff coming from/belonging to different services and / or Ministries including criminal police, public order police, border guards, customs, and judicial authorities.

– In Member States where judicial authorities supervise criminal investigations, the presence of these authorities in the SPOC is very useful for

  - a quicker response to requests related to criminal investigations, especially where the transmission of information by law enforcement channels requires a clearance by the judicial authorities
  - the "flagging" procedure related to a European/International Arrest Warrant (EAW / IAW)
  - the transmission of rogatory letters to the relevant investigating judge or prosecutor office
  - legal advice to police/customs staff of the SPOC or help to solve possible conflict between national law and the object of the request sent by another Member State (see 3.3.5)
  - the permission "on the spot" of urgent surveillances within national territory, as defined by the provisions of Article 40 of the Schengen Convention (or to forward such requests to another Member State).

– The SPOC is sufficiently and adequately staffed, including interpretation or translation capacities, to function on a 24/7 basis.

– In as far as possible, all staff is trained and equipped/mandated to deal with all kinds of tasks within the SPOC. Where this is not possible, it is ensured that all tasks can be dealt with through on-call duty officers 24/7.

– The ICT capacities are state of the art, including secure and back-up communication lines (phone, fax, e-mail), an efficient and effective electronic case management system, and appropriate and timely (helpline) IT support.

1.3 Publicity

– The SPOC is adequately known by the national police officers, and officers from other law enforcement agencies. Apart from its contact details (phone, fax numbers, e-mail addresses), every investigating police officer knows the basic services provided by the SPOC, and the main channels to be used depending on the type of the request concerned.

– For that purpose, a national "quality manual for international law enforcement cooperation" is drafted and published, both on Intranet and through booklets. It includes summary information on:

  - legal framework and international instruments (under national law, EU, United Nations, bilateral agreements on crime prevention and legal assistance)
  - standard of quality and required data for request for law enforcement cooperation and legal assistance
  - the various international channels and the national rules of how to use them
  - necessity, appropriateness and proportionality of the request
  - limits and restrictions to information exchange.

2. NATIONAL INFORMATION EXCHANGE AND AVAILABILITY OF NATIONAL DATABASES AND NETWORKS

There is a close correlation between the way in which information and data bases are shared internally and the proper sharing of information at international level (Chapter 3.3).

Ability to answer correctly and quickly to other MS requests is dependent on the present Chapter.

Subject to data protection rules and the authorisation level of respective staff members, the SPOC has access, direct or at request from competent authorities, to the broadest range of relevant national databases and in any case to all those databases available to the authorities represented in the SPOC. This covers in particular law enforcement databases, identity documents database, vehicle registration, national visa database, immigration office database, prisoners database, DNA databases, fingerprint databases, information exchange with the national liaison officers, border control database, trade register, ANPR etc.

– Ideally, all members of the SPOC have access to all of these databases, if necessary on a hit/no hit only basis; if this is not possible, all databases are accessible to the unit on a 24/7 basis, where necessary via on-call duty officers.

– The SPOC has arrangements for indirect (e.g. on a hit/no hit basis) but quick, effective and efficient access to relevant databases of other authorities or bodies, where appropriate subject to judicial approval. This applies to records of companies providing electricity, water, phone and other communication supplies.

– The SPOC uses standard forms for transmitting international requests to and receiving the corresponding replies from the national authorities, which are independent from the law enforcement authority involved (at local level or in the SPOC).

– The SPOC shall respect all applicable data protection rules

  - condition for access to the data
  - designation of duly empowered officials according to the appropriate user profile
  - keeping of records (logging of checks and searches, date and time of access, type of data used for consultation, name of authorities having requested the check, records of the staff members -name or personal code- having consulted data, etc.)
  - conservation period of personal data
  - deletion of data
  - purpose limitation/ownership rights

– The data protection rules are implemented and reflected in internal business procedures and working instructions, which are subject to regular review and supervision by the national data protection authority.

– Access to the databases and communication with national authorities is via secure means.

– Access to the different databases is organised in a user-friendly way, where possible via a single workstation.

– SPOC shall respect the security rules for protection of classified information[2].

3. INTERNATIONAL INFORMATION EXCHANGE

3.1 Access to information

– The SPOC has direct access to European and international law enforcement databases (SIS, Europol databases, Interpol databases, CIS) and European databases, such as EURODAC, or software applications such as EUCARIS, to which law enforcement has been given access.

– The SPOC is connected to the Europol (SIENA), Interpol (I-24/7 communication system), and sTESTA network.

– Access to the databases and communication is achieved via secure means.

– Access to the different databases is organised in a user-friendly way, where possible via a single workstation and combined with access to national databases and systems.

3.2 General rules for international communications

– A request is sent through one channel only.

– If a request is, in exceptional cases, sent through different channels at the same time, this is clearly indicated on the request.

– If the request is sent to parties for information only, this is clearly indicated.

– The channel is NOT be changed during an on-going operation or during any phase unless it is absolutely necessary and the partner's choice of channel when replying to the requests is respected.

[2] see: National legislation, Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU), and concluded bilateral agreements on exchange and protection of classified information

– A change of channel is communicated to all parties, including the reason for the change.

– The requirements of the channel used (for example – usage of the handling and evaluation codes for Europol SIENA are respected.

– The purposes of and restrictions on the processing of information defined by the provider of the information are respected.

– Whenever possible, the SPOC replies directly to the international request, where appropriate with copy to the concerned national authority.

– Where the SPOC cannot reply directly, because it is beyond its mandate and/or because it cannot directly obtain the information, it forwards the request to the appropriate competent national authority, even if the original request was wrongly addressed to another authority.

– When a request is refused, the grounds for refusal have to be provided through the initial channel.

– When receiving a reply from the national authorities to an international request, the unit pro-actively verifies whether this information can be useful to another Member State, Europol or Eurojust[3] and if this is the case, requests and encourages the owner of the information to transmit the information further.

3.3 Specific rules for the choice of channel

– The front desk is crucial in choosing the most appropriate and relevant channel by gathering all requests ("in" or "out") dealt with by the SPOC, before dispatching them to the relevant desk (Europol, Interpol, SIRENE, bilateral liaison officers). In this context, the SPOC should acts on the basis of clear and specific national rules which build on the basis of the criteria below**.**

[3] See Art.6 (2) of Council Framework Decision 2006/960/JHA

– This helps to prevent overlaps or that a request is sent more than once through different channels and may even lead to the discovery that two different national services or departments are investigating the same case or are targeting the same suspect.

Possible cooperation channels:

– bilateral and regional liaison officers

– SIRENE Bureau

– Europol **(**ENU, liaison officers at Europol)

– Interpol (NCB, liaison officers at Interpol)

– jointly staffed units in border regions, in particular PCCCs

– direct contacts between concerned authorities

– coordination units for Naples II/ Anti-Fraud Information System (AFIS)/CIS/FIDE/FIU

Proposed criteria for use of channels:

– Europol

  – EU reach and its mandate (terrorism, serious and organised crime, 2 or more MS concerned)

  – Contributions to AWF, EMPACT projects, analysis, JITs

  – Exchange of classified information (up to EU RESTRICTED)

  – Exchange under Swedish Framework Decision (SIENA form/ UMF)

  – Urgency

- Interpol
  - Exchange of information with EU Member States and third countries
  - Alerts (wanted/missing persons, arrest warrants, extraditions)
  - Verification of persons identity / documents
  - 24/7 availability and urgency
- SIRENE
  - SIS alerts
  - Cross border surveillance
  - 24/7 availability and urgency
- Bilateral/regional channels
  - Exchange of classified information (depends of concluded bilateral agreements)
  - Urgency, trust
- PCCC
  - Local reach and exchange of information about crimes committed in the border area
- Naples II/AFIS/CIS/FIDE/FIU
  - Specific information exchange/ legal assistance

3.4 Case Management System

Dealing with law enforcement information exchange, the SPOC should follow the “circle of criminal intelligence”, *i.e.* it receives a request, evaluates it according to the importance, replies directly (when possible) and disseminates it to the competent authority that is most suitable for the operational handling and, finally, supplies the information requested.

With a view to making this procedure more efficient at each SPOC, access to a “case management system", that evaluates, classifies and disseminates the information originating from all cooperation channels and national authorities, is considered of crucial importance.

The prioritisation of the incoming information should be among the core functions of the SPOC. To support this, the system that is dealing with the reception-evaluation-distribution of the incoming data should also have the ability of prioritisation. A built-in capability of automated characterisation of the importance level of the incoming information would be ideal, so that this data could be handled with the appropriate concern and urgency. The characterisation could be as following:

- Level 1 (Urgent)
- Level 2 (Normal / Non-urgent)

Every case should automatically be attributed to a single registration number, unique for the involved cooperation channels such as SIRENE, INTERPOL, EUROPOL, etc. This could make the handling of each case more speedy and help avoiding any confusion during the course of the above described “circle of criminal intelligence”. Besides, following the attribution of a single registration number, the creation of a related folder would be ideal. The existence of such a folder would render the management of the cases more convenient and non-susceptible to mishandlings.

Before being distributed to the operating agencies the data contained in each request that arrives at the SPOC should undergo an automated cross-check against national and international databases available at the SPOC. The thorough “examination” of the incoming information can lead to reducing the correspondence between the SPOC and national law enforcement agencies.

Ideally, the national case management systems should be connected SIS/SIRENE and Interpol, as well as to SIENA.

4. STAFF COMPETENCE AND TRAINING

4.1 General recommendations

- Staff is experienced in dealing with international cases and main EU and international tools of police co-operation.
- Staff has knowledge of issues such as intelligence and criminal investigative techniques, as well as of the national legislation and data protection rules.
- Staff is able to communicate orally and to have good written skills in foreign languages. Basic knowledge of one or two languages other than the mother tongue is an asset, especially of those languages mostly used in the international cooperation cases of their Member State (based on geographical, economic or historical reasons or on criminal phenomena).
- Staff has enough computer skills to fulfil its desk duties.
- Staff receives regular training, both about EU and international cooperation mechanisms (*i.a.* via CEPOL) and about national developments.

4.2 Specific requirements for the management of the SPOC

- The management of the SPOC has a broad background in law enforcement.
- The management has a suitable ranking to require additional information from national competent authorities and / or to speed up and ensure the follow up of requests within the time frames.

– The management has good knowledge of national and international law (in particular of the Schengen, Europol and Interpol legal framework and standards) in order to advise staff members (and provide regular training on those matters).

– The management is empowered to settle a difference between / provide an assessment on different channels that may be used, using the criteria set out in Chapter 3.3.

– The management is able to assess and decide (in close cooperation with the authority that initially sent the request) about the most appropriate cooperation channel to be used, according to criteria set out in Chapter 3.3, and to convince the concerned authorities of this, as well as of the need and requirement to forward relevant information beyond the initial destination.