EUROPEAN
COMMISSION

Brussels, 7.12.2012
COM(2012) 735 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)

1. INTRODUCTION

Ensuring a high level of security within the EU and Schengen area requires that criminal networks be tackled by concerted European action[1]. This is needed to address not just serious and organised crime, such as trafficking in human beings, illicit drugs or firearms, but also less serious offences committed on a large scale by mobile organised crime groups and crimes committed by individual offenders across Member State borders.

Exchanging information between Member States is in this context an essential tool for law enforcement authorities. International and bilateral arrangements have therefore been supplemented by EU instruments and systems, such as the Schengen Information System and the Europol Information System, with in-built safeguards to protect privacy and personal data in line with the Charter of Fundamental Rights. This Communication takes stock of **how** the resulting **cross-border information exchange in the EU works today**, and makes recommendations for how to improve it.

It concludes that information exchange generally works well, and examples of successful results are given below to illustrate this. **No new EU-level law enforcement databases or information exchange instruments are therefore needed at this stage**. However, the existing EU instruments could and should be better implemented, and the exchanges should be organised more consistently.

This Communication accordingly sets out recommendations to Member States for how to **improve the implementation of existing instruments** and **streamline the communication channels used**. It emphasises the need to **ensure high data quality, security and protection**. It also explains how the Commission will provide support, including **funding and training**, for Member States. In this way, it provides a Model for guiding EU and Member State activity.

This Communication responds to the invitation in the *Stockholm Programme* for the Commission to assess the need for a European Information Exchange Model based on an evaluation of existing instruments. It builds on the Commission's Communication of 2010 giving an overview of information management in the area of freedom, security and justice ('2010 Overview Communication')[2] and on the *EU Information Management Strategy* for internal security agreed in 2009[3], along with actions undertaken by Member States, the Commission and Europol to implement it ('IMS Actions'). It further draws on a mapping exercise of EU information exchange involving national and other (EDPS, EU agencies,

[1] The EU Internal Security Strategy in Action, COM(2010) 673.
[2] COM(2010) 385.
[3] Council Conclusions 30 November 2009, 16637/09.

Interpol) experts, a study on information exchange among law enforcement authorities[4], and discussions with stakeholders, including data protection authorities.

2. THE CURRENT SITUATION

Law enforcement authorities exchange information for different purposes: for criminal investigation, for preventing crime, for detecting crime (e.g. using criminal intelligence operations) and for ensuring public order and security. As to the scale of cross-border exchanges, the above-mentioned study from 2010 reported responses by national-level agencies in Member States that in about ¼ of their investigations and criminal intelligence operations requests were sent to other EU or Schengen Member States.

2.1. Instruments

The 2010 Overview Communication described all EU-level measures regulating the collection, storage or cross-border exchange of personal information for the purpose of law enforcement or migration management. This Communication focuses on **instruments used for cross-border exchanges between Member States**. Examples of how the instruments are used have been provided by Member States.

The **Swedish Initiative**[5] establishes rules, including deadlines, for exchange of information and intelligence between Member State law enforcement authorities for the purpose of conducting criminal investigations or criminal intelligence operations. It applies the principle of 'equivalent access': information must be provided to requesting Member States under conditions no stricter than that applicable at national level. The information must also be exchanged with Europol and Eurojust insofar as the exchange refers to offences within their mandate.

In 2012 a Swedish company was tricked by a known Italian fraudster into paying €65 000 to an Italian account. The Swedish SPOC (see 3.2 below) received a request from Italy, via the SIRENE channel (see below), to contact the company's director to check if payment had been made, in which case Italy would freeze the money. Sweden took action and replied under the Swedish Initiative in less than 24 hours. Due to this quick action, the Swedish police received information that a company was a fraud victim and the Italian authorities obtained information needed to take action and the money will probably be recovered.

In 2012 in the emergency department of a hospital near Paris, a Belgian-born man gave confused accounts of how he had received a serious gunshot wound. His companion's statements pointed investigators towards possible acts in Belgium. First enquiries showed that the man was known in BE, including for murder. The French authorities immediately under the Swedish Initiative sent spontaneous information to the Belgium police who rapidly made a link with events two days previously in Belgium when four armed men had kidnapped a jewellery shop employee. Police intervention had put the men to flight; the men escaped, but one was shot in an exchange of fire with police. This information led the French authorities to put the man under surveillance pending a European Arrest Warrant (EAW), which was issued the same day in Belgium and transmitted to France via SIRENE.

[4] http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm

[5] Council Framework Decision 2006/960/JHA.

The **Prüm** Decision[6] provides for automated exchange of DNA profiles, fingerprint (FP) data and vehicle registration data (VRD) for investigating criminal offences (for DNA, FP, VRD), preventing criminal offences (FP, VRD) and maintaining public security (VRD). Comparison of biometric data (DNA, FP) operates on a 'hit/no-hit' basis: an automated comparison produces an anonymous 'hit' if the DNA or FP data held by the requesting Member State match data held by another Member State. The related personal or case data are only provided in response to a separate follow-up request.

A man was found stabbed to death in an apartment in a German city. A fingerprint was found on a doorframe. An automated Prüm search led to a hit in the Bulgarian database. Follow-up information requested from Bulgaria the next day was submitted within 3 hours and immediately entered into the Schengen Information System (SIS – see below). The next day the individual concerned was arrested in Austria.

In 2007, at the start of Prüm exchanges, equipment was stolen from a police car in Vienna. A DNA trace from the car was matched in the Austrian database with a trace from a similar case, but it was a Prüm hit in the German database that led to the identification of a Polish serial burglar. An EAW was issued in Austria. The suspect was arrested in Poland (due to a hit on an SIS alert) and was later convicted in Austria.

Europol supports Member States' action and cooperation in preventing and combating organised crime, terrorism and other forms of serious crime (as listed in the Annex to the Europol Council Decision[7]) affecting two or more Member States. It provides a platform for Member States — through Europol National Units ('ENUs') — to exchange criminal intelligence and information. The Europol Information System is a database of information (183 000 items) supplied by Member States on cross-border crime within Europol's mandate, the individuals involved (41 000) and other related data. Europol uses it for its analyses and Member States can use it for investigations. Since 2011 Member States may designate law enforcement authorities other than ENUs to be granted access to make searches on a hit/no-hit basis. Analysis work files allow Europol to provide operational analyses to support cross-border investigations.

Counterfeit payment cards were used to withdraw large sums of money from cash machines throughout Slovenia. Two Bulgarian citizens were being investigated; use of the Europol Information System (EIS) led to a hit showing that one of them had committed similar acts in France and Italy. France provided detailed information to the EIS. Due to a swift reply from France via SIENA (see below), followed by a fingerprint check and the lifting of a handling restriction, authorities in Slovenia could use the data as evidence before the courts. The Europol analysis work file revealed links between cases in SI, BG, FR, IE, IT and NO.

The **Schengen Information System (SIS)** contains alerts on persons and objects. As a compensatory measure for the lifting of internal border controls, it is used both within the Schengen area and at its external frontiers with the aim of maintaining a high level of security within the area. It is a large-scale system (over 43 million alerts) accessible on a hit/no-hit basis to frontline officers. Following a hit (i.e. details of a person or object match an alert), supplementary information can be obtained via the SIRENE Bureaux (see below). SIS will be replaced by **SIS II**, which will bring improvements such as the possibility to link related alerts (e.g. alert on a person and a vehicle), new categories of alerts, and a facility to store

[6] Council Decision 2008/615/JHA.
[7] 2009/371/JHA.

fingerprints, photographs and copies of European Arrest Warrants. The SIS II Council Decision[8] defines categories of alerts to support cooperation between police and judicial authorities in criminal matters. For these, all EU Member States will participate in SIS II, while Europol and Eurojust will continue to have access. Management of central parts of SIS II will be transferred to the IT Agency[9].

Other EU instruments or IT systems provide for exchange of law enforcement information between customs authorities (Naples II Convention; Customs Information System as part of the Anti-Fraud Information System databases operated by the European Anti-Fraud Office – OLAF), Financial Intelligence Units, Asset Recovery Offices and Cybercrime Alert Platforms[10]. Law enforcement access to other large-scale EU systems is provided for (Visa Information System) or is proposed (EURODAC[11]) for preventing, detecting and investigating terrorism and other serious crime. The question of granting law enforcement access and, if so, under what conditions, is also part of the preparatory work currently being undertaken in view of the proposal for an Entry/Exit System that is to be presented soon.

A European Border Surveillance System (EUROSUR) is being developed for information exchange and operational cooperation between National Coordination Centres and with Frontex to improve situational awareness and reaction capability for preventing irregular migration and cross-border crime at the EU's external borders. A Common Information Sharing Environment (CISE) for surveillance of the EU maritime domain aiming inter alia at enhancing maritime situational awareness is being developed to enable exchanges of information across public authorities of seven relevant sectors (including general law enforcement) and across borders while establishing interoperability between existing and future surveillance systems such as EUROSUR.

Member States also exchange information under national laws and bilateral agreements. They are also all members of Interpol, through which information can be exchanged with countries across the world either through Interpol notices and databases (e.g. Stolen and Lost Travel Documents) or bilaterally using the Interpol channel.

2.2. Channels and communication tools

Three main channels are used for cross-border information exchange, each based on national units in each Member State that use a related communication tool:

(1) **SIRENE**[12] Bureaux can, following a hit on an alert in SIS, obtain supplementary information from the Member State that issued the alert. They operate 24/7 and follow the procedures in the SIRENE Manual. Currently, they exchange information using a system called SISNET, which will be replaced by the SIS II communication network by the end of March 2013.

(2) **Europol** National Units (ENUs) exchange information with Europol. They may also exchange information bilaterally on crime outside Europol's mandate and without

---

8 2007/533/JHA.

9 European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

10 The forthcoming European Cyber-Security Strategy will provide an opportunity to assess future information exchange needs between the network and information security authorities and law enforcement, e.g. via the European Cybercrime Centre.

11 EU database of fingerprints of asylum applicants and those crossing borders irregularly.

12 **S**upplementary **I**nformation **RE**quest at the **N**ational **E**ntry.

involving Europol. ENUs can exchange information directly or through Europol Liaison Officers, who are part of an ENU but stationed at Europol headquarters. A secure communications tool, **SIENA**[13], has been developed by Europol for exchanges with Europol and between Member States. In 2011, Member States used SIENA to exchange 222 000 messages; in 53% of those the information in the message was shared with Europol.

(3) **Interpol** National Central Bureaux, operating 24/7, exchange information with Interpol as well as bilaterally without involving Interpol. National Central Bureaux use the I-24/7 communication tool developed by Interpol.

Other channels include bilateral Liaison Officers (stationed in other Member States and typically used in more complex cases) and Police and Customs Cooperation Centres (set up by neighbouring Member States to support information exchange and operational cooperation in border areas).

The **choice of channel** is partly regulated by EU law: SIS requests for post-hit supplementary information must be via SIRENE Bureaux, and information exchange with Europol via ENUs. Otherwise the choice is up to Member States.

2.3. Interaction of the different instruments, channels and tools

There is a diversity of instruments, channels and tools, each designed for particular purposes. A criminal investigation can involve parallel or sequential use of more than one instrument. In a cross-border case of serious or organised crime, a person or object could be checked against both the Europol Information System and SIS, and where there are 'hits' follow-up requests could be made via Europol or SIRENE channels, respectively. A biometric trace could be the subject of a Prüm exchange followed by a post-hit Swedish Initiative request using the SIENA tool.

Whatever the combination or sequence, the rules of each instrument must be respected. These include rules on data protection, on data security and quality, and on the purpose for which the instruments may be used. National processing of data for cross-border exchanges must also comply with EU legislation on protection of personal data[14]. Proportionality must be respected, e.g. requests may be refused under the Swedish Initiative if providing information would be clearly disproportionate to the request's purpose. Respecting these rules requires that requests and replies be validated by well-qualified staff working with appropriate information tools.

2.4. Interface with judicial cooperation

The criminal justice process involves both law enforcement and judicial authorities, but differences between Member States include the extent to which criminal investigation is directed or supervised by judicial authorities (including prosecutors). Where judicial authorities are in the lead, as well as where information is needed as evidence, judicial cooperation procedures of mutual legal assistance (MLA) are typically required.

Furthermore, information directly accessible to law enforcement in one Member State may require judicial authorisation in another. The Swedish Initiative requires that where requested

[13] **S**ecure **I**nformation **E**xchange **N**etwork **A**pplication.

[14] Council Framework Decision 2008/977.

information requires judicial authorisation, then the requested law enforcement authority must make a request to the judicial authority which must apply the same rules as in a purely internal case.

The mapping exercise found, however, that law enforcement experts perceive the differing rules as a source of delay in cross-border investigations. Although outside the scope of this Communication, it can be noted that Eurojust is available to facilitate judicial cooperation. Also relevant would be the European Investigation Order, currently being discussed, which could replace existing rules for cross-border obtaining of evidence implementing the principle of mutual recognition. It would be required to be recognised and executed with the same celerity as for a similar national case, and, in any case, within stipulated deadlines.

2.5. Principles

In its 2010 Overview Communication the Commission set out substantive and process-oriented principles for developing new initiatives and evaluating current instruments.

The substantive principles are:

(1) *Safeguarding fundamental rights, in particular the right to privacy and data protection.* These are rights under Articles 7 and 8 of the Charter and Article 16 of the Treaty on the Functioning of the EU.

(2) *Necessity.* A restriction of the right to privacy may be justified only if it is lawful, pursuing a legitimate aim and necessary in a democratic society.

(3) *Subsidiarity*.

(4) *Accurate risk management.* Necessity tests and purpose limitations are essential.

The process-oriented principles are:

(1) *Cost-effectiveness.* This requires taking existing solutions into account and assessing whether a proposal's objectives could be achieved through better use of existing instruments.

(2) *Bottom-up policy design.* An example of this is the mapping exercise involving law enforcement experts when preparing this Communication.

(3) *Clear allocation of responsibilities.* The 2010 Overview Communication noted that Member States had no project leader to turn to for advice on Prüm implementation. The Commission's Prüm Report notes how this deficit is now in part filled by support at Europol. As to the idea in the 2010 Overview Communication that the IT Agency may be able to provide technical advice, the Agency's current priorities lie elsewhere. An occasion for reconsidering this will be the 3-year evaluation due by the end of 2015.

(4) *Review and sunset clauses.* The Commission has issued reports on the Swedish Initiative and Prüm. This Communication takes account of those.

3. ASSESSMENT AND RECOMMENDATIONS

This section focuses on the Swedish Initiative, Prüm and the Europol channel. Although SIS and the SIRENE channel account for a high volume of information exchange, recommendations are not presented on these because extensive changes are already underway notably the forthcoming move to SIS II.

3.1. Improve the use of existing instruments

Other than the forthcoming Europol reform, the Commission does not intend in the short-term to propose amendments to the above-mentioned EU instruments. Nor are new instruments currently needed. First of all, **existing instruments need to be implemented**.

This applies particularly to Prüm. The Commission's Prüm Report accompanying this Communication finds that Prüm data exchange is highly appreciated for investigations, but that implementation is seriously lagging. **Many Member States are not yet exchanging data under Prüm even though the deadline for transposition was 26 August 2011**[15]. The main reasons are of a technical nature and due to a lack of human and financial resources in Member States. However, given the possibilities of EU support (funding, Mobile Competence Team, helpdesk), what seems to be needed above all is political will to implement. As stated in the Report, the Commission will continue to assist by offering EU funding. However, the context will change in December 2014 when the Commission will be able to bring infringement proceedings. Rules for control of national implementation do not apply until then, since Prüm, like the Swedish Initiative, was adopted under the former third pillar.

As to **the Swedish Initiative**, the Commission reported in 2011 that the instrument had not yet reached its full potential but that its importance would increase[16]. That assessment remains valid; not all Member States have yet implemented[17]. Most Member States have informed that they have transposed it into their domestic legislation[18], while some have stated that they had no need to transpose it as their domestic legislation was already in line with it[19]. Nevertheless, despite its advantages including the equivalent access principle and deadlines, it is in practice still not widely used. Reasons given include that alternatives are considered to be adequate and that the request form is cumbersome (even in its 2010 simplified version[20]).

The Commission was asked to examine its usefulness for Prüm post-hit follow-up requests[21]. Where follow-up information is needed as evidence before a court, a judicial cooperation request will normally be required. However, where use as evidence is not or not yet needed, systematic use of the Swedish Initiative as legal basis and SIENA as communication tool should be promoted so as to make full use of the advantages of each and to align Member States with a single best practice.

---

15 The following Member States have implemented:
DNA: BG/CZ/DE/ES/EE/FR/CY/LV/LT/LU/HU/NL/AT/PT/RO/SI/SK/FI;
FP: BG/CZ/DE/EE/ES/FR/CY/LT/LU/HU/NL/AT/SI/SK;
VRD: BE/DE/ES/FR/LT/LU/NL/AT/PL/RO/SI/FI/SE.
For more details, see the Prüm Report.

16 SEC(2011) 593.

17 The following Member States are still to adopt implementing legislation: BE/EL/IT/LU.

18 BG/CZ/DK/DE/EE/ES/FR/CY/HU/LT/LV/NL/PL/PT/RO/SI/SK/FI/SE.

19 IE/MT/AT/UK.

20 9512/1/10.

21 Council Conclusions 27-28 October 2011, 15277/11.

As regards **Europol**, a 2012 evaluation[22] confirmed other findings that Member States do not adequately share information with Europol (and thereby with each other). The Commission will address this in a proposal to amend Europol's legal basis. For its part, Council has invited Member States to make increased use of the Europol Information System[23].

In line with the Stockholm Programme, the Commission ordered a study on a possible **European Police Records Index System**[24]. The idea is to respond to the perceived need, given the increased cross-border nature of crime, for a police officer in one Member State to know if a suspect is known to police in another. In line with the cost-effectiveness principle, the Commission considers that creating an EPRIS is **currently not justified** given that existing instruments and tools, which could serve this purpose partly or fully through better or intensified use, are not fully used. This concerns in particular the Europol Information System (uploading relevant data and extending access at national level), SIS II (increasing use of relevant alerts on persons or vehicles for checks for the purposes of prosecuting criminal offences and preventing threats to public security), SIENA (further developing access at national level, interlinking with national systems and automating tasks where appropriate), and Prüm (full implementation to improve identification of criminals acting in different Member States).

Member States are invited to:

- Implement fully the Swedish Initiative, including its principle of equivalent access.
- Implement fully the Prüm Decision, using the available EU support.
- For Prüm post-hit follow-up requests, use the Swedish Initiative and the SIENA tool.

The Commission will:

- Continue to provide EU funding to support implementation of Prüm.
- By December 2014: prepare for applying in this area the rules for ensuring national implementation of EU law.

3.2. Streamline and manage the channels

Choice of channel. One result of Member States having a free choice of channel (apart from the legal requirements relating to SIRENE Bureaux and ENUs) is that they use different channels to different extents. The Manual of Good Practices concerning International Police Cooperation Units at National Level ('2008 Manual')[25], drawn up under the aegis of the EU Police Chiefs, contains criteria[26], but they are not binding and have not led to convergence of national practices. Some Member States have moved towards more systematic use of the Europol channel. Others continue to rely a good deal on the Interpol channel, the attraction of which seems to lie partly in its traditional central role in international police cooperation and partly in its perceived ease of use. SISNET is used by some Member States for non-SIS matters e.g. Swedish Initiative requests.

22 https://www.europol.europa.eu/sites/default/files/publications/rand_evaluation_report.pdf
23 Council Conclusions 7-8 June 2012.
24 http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm
25 7968/08.
26 Repeated in Guidelines on the implementation of the Swedish Initiative, 9512/1/10.

The Commission believes the time has come within the EU for a more coherent approach, one giving the Europol channel a central role. Under this approach, where the channel is not legally defined **the Europol channel using the SIENA tool should become the default channel** unless there are specific reasons to use another. Thus, for example, police cooperation requests currently made using SISNET (which will close when SIS II goes live[27]) should in future be made using SIENA.

Some Member States favour an approach that leaves wide flexibility to use different channels. The Commission disagrees. The development by all Member States of national rules on the choice of channel and their convergence towards a single shared approach would be better than the current dispersed approach. The choice of the Europol channel is justified by its advantages. Europol Liaison Officers can be asked to intervene where necessary. SIENA can be used for direct bilateral exchanges, but also facilitates sharing of information with Europol in line with legal requirements of the Europol Decision and the Swedish Initiative. SIENA messages are structured, can handle large data volumes and are exchanged with a high level of security. Data protection is enhanced by exchanging information in a structured format e.g. by using SIENA. The suggested approach is fully in line with the Commission's forthcoming proposal for Europol reform and with the European Council's strategic guidelines in the Stockholm Programme, which state that 'Europol should become a hub for information exchange between the law enforcement authorities of the Member States, a service provider and a platform for law enforcement services'.

Managing the channels. A Single Point of Contact (SPOC) is a 'one-stop shop' for international police cooperation, operating 24/7, in which a Member State brings together its SIRENE Bureau, ENU and Interpol National Central Bureaux, and contact points for other channels. The creation by each Member State of a SPOC (even if that term was not always used) was in 2007 a conclusion of the third round of mutual evaluation visits[28] and recommended by the 2008 Manual. Most Member States have international police cooperation departments, but only some of these have the characteristics of fully fledged SPOCs. In 2012, the Council invited Member States 'to explore the possibilities of establishing' a SPOC[29]. The Commission would go further: to improve EU law enforcement information exchange as a whole, **all Member States should set up SPOCs** with certain minimum features.

For requests to another Member State, bringing together the different channels into a single organisational structure that follows national choice of channel rules will ensure the correct and consistent choice of channel as well as the quality of requests. Quality is ensured by SPOCs validating requests to confirm that they are necessary and appropriate. Where information is not exchanged through a SPOC itself (e.g. via Police and Customs Cooperation Centres (PCCCs) or via national agencies making direct exchanges using SIENA), a SPOC can ensure national coordination. For incoming requests, SPOCs should where legally permissible have direct access to national databases to answer requests quickly, particularly under Swedish Initiative deadlines. SIRENE Manual rules (e.g. on security, workflow systems, data quality and staffing) could be a basis for organising all channels in a consistent way. Sharing resources such as staff and infrastructure can contribute to cost savings or at least better use of resources.

---

27 The SIS II communication network is legally limited to SIS II data and supplementary information.

28 13321/3/07.

29 Council Conclusions 7-8 June 2012, 10333/12.

SPOCs should include all law enforcement agencies including customs. Cooperation should be established between SPOCs and National Coordination Centres (NCCs) for border surveillance. Where compatible with national legal systems, links should be created with judicial authorities, in particular where they supervise criminal investigations.

A growing number of PCCCs[30] successfully exchange information at local and regional level. Annual conferences at EU level enable experiences to be shared and common approaches to be discussed. Although the generally high number of exchanges mostly do not concern the most serious and organised crime, one challenge is to ensure that information in relevant cases is passed up to national (SPOC) level and, where appropriate, to Europol. In this context, the Commission looks forward to the results of an on-going pilot project (under an IMS Action) using SIENA at a PCCC.

The **Information Exchange Platform** is an IMS Action led by Europol to develop a common portal to access existing channels and systems, fully respecting their security and data protection rules. The Commission considers that there are benefits from facilitating use of existing channels and systems, but that further assessment is needed of the costs/benefits of an Information Exchange Platform, who would provide the funding, and how the project would be governed. This assessment should also involve the IT Agency[31].

Member States are invited to:

- Use, for exchanges where the channel is not legally defined, the Europol channel using the SIENA tool as the default channel, unless there are specific reasons to use another.
- Develop national instructions for choice of channel.
- In particular, after SIS II goes live and SISNET is closed, use the Europol channel and SIENA tool for police cooperation exchanges currently using SISNET.
- Create, if not already existing, a Single Point of Contact (SPOC) covering all main channels, available 24/7, bringing together all law enforcement authorities, with access to national databases.
- Ensure that information exchanged through Police and Customs Cooperation Centres is where appropriate passed up to national level, and where relevant to Europol.
- Establish cooperation between SPOCs and EUROSUR NCCs.

The Council is invited to:

- Amend EU-level guidance to reflect the choice of channel guidelines suggested above.

The Commission will:

- Participate in work to assess the feasibility of an Information Exchange Platform.

[30] 38 at end 2011.

[31] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

3.3. Ensure data quality, security and protection

Data protection safeguards in the existing instruments must be carefully observed. Under the Commission's proposal of 25 January 2012 for a Directive applying to the national processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences[32], the data protection rules in existing instruments will need to be reviewed to assess the need to align them with the Directive.

A **high level of data security** is necessary to protect the integrity of personal data that is exchanged and to ensure that Member States have confidence in exchanging information. A chain is only as strong as its weakest link: Member States and EU agencies must ensure data is exchanged over networks that are highly secure. The above-mentioned proposal for a Directive contains rules on data security[33], and at EU level there are detailed security rules for protecting EU classified information[34].

A **high level of data quality** is equally important. The 'business process', i.e. how information exchange is carried out in practice, is relevant in this context. One aspect of this is, where possible and appropriate, to **automate specific tasks**. For example, drawing up a request for information from another Member State requires re-entering data recorded in a national system into the communication tool used; doing this manually risks introducing errors and takes time. Automating such tasks will be enabled by **UMF II**[35], another IMS Action. This EU-funded project led by Europol aims to develop a standard for the format of messages used to request information and to provide replies. This would enable the automation of data transfer between different systems, e.g. national case management systems and SIENA. As well as potential cost savings or at least better use of resources, the benefits from eliminating manual re-entry of data are two-fold. It releases staff to be deployed on validation tasks. Further, by reducing copying errors and facilitating the exchange of information in structured formats, it improves the management and protection of data.

Automation of tasks does not imply that every police officer in the EU should have access to all police information in the EU. Exchanges must be limited to those that are necessary and appropriate, and need to be managed so as to ensure that they stay within those limits. **Automated searches, as a way to overcome capacity problems, therefore function under existing EU information exchange instruments on a hit/no-hit basis** (e.g. SIS, Prüm DNA and fingerprints), or else are limited to narrowly defined types of data (e.g. Prüm vehicle registration data). Certain tasks cannot and should not be automated, notably the validation of requests and replies. This is particularly important under the Swedish Initiative, which requires requests to be justified.

Finally, **interoperability** between different national systems and administrative structures can yield benefits in terms of consistent procedures, shorter response times, better data quality, and simplified design and development. The European Interoperability Framework[36] identifies four levels of interoperability: technical, semantic, organisational and legal. UMF II will develop the semantic level[37]. Aligning with shared practices (SPOCs, choice of channel)

---

32 COM(2012) 10.

33 Arts 27 to 29 of the proposal.

34 Council Decision 2011/292/EU.

35 **U**niversal **M**essage **F**ormat.

36 COM(2010) 744.

37 UMF II takes account of other work on semantics, such as common data models being developed under the EU programme on interoperability solutions for European public administrations.

will promote the organisational level. However, information may only ever be actually exchanged and used where legally permitted.

Europol and Member States are invited to:

- Continue development of the UMF II standard.

3.4. Improve training and awareness

To equip law enforcement officers with knowledge and skills needed to cooperate effectively, the Commission is preparing a European Law Enforcement Training Scheme. A mapping exercise showed that relevant EU information exchange instruments are covered in the initial training of law enforcement agencies, but it did not assess the quality of the training. Specialist officers such as those working in SPOCs need more in-depth training. Exchanges of such staff are also recognised[38] as beneficial and should be encouraged.

Member States are invited to:

- Ensure that all law enforcement officers receive appopriate training on cross-border information exchange.
- Organise exchanges of SPOC staff.

The Commission will:

- Ensure that the European Law Enforcement Training Scheme includes training on cross-border information exchange.

3.5. Funding

EU funding under the Prevention of and Fight against Crime Fund (ISEC) has been allocated to information exchange projects such as UMF II (€830 000) and implementation of Prüm (€11,9 million). The Fund will be replaced in 2014-20 by an EU Internal Security Fund, for which EU information exchange projects will also be eligible.

Part of the Internal Security Fund will be managed by Member States through so-called 'shared management' in accordance with **multiannual programmes. Those programmes should consider relevant national information exchange priorities** in line with the recommendations in this Communication. The Commission will in parallel consider how parts of the Internal Security Fund under its direct management can in particular support pilot projects, e.g. by further developing UMF II.

As regards Member States' own spending, other recommendations (on SPOCs, UMF II) could as indicated contribute to cost savings or at least better use of resources.

Member States are invited to:

- Consider relevant information exchange priorities in national multiannual programmes under the 2014-20 EU Internal Security Fund.

[38] 10333/12.

The Commission will:

- Include information exchange policies in ISF programming dialogues with Member States.
- Invite proposals for direct (Commission) funding of relevant pilot projects.

3.6. Statistics

Existing statistics, while good in some areas (e.g. SIS, SIENA), are not comprehensive. Better statistics would improve knowledge of the use of the Swedish Initiative (for which only numbers sent using SIENA are known) and Prüm.

Gathering statistics may however be resource-intensive, particularly if not embedded in normal workflow. Ad hoc exercises should be avoided. An evolutionary approach is best, building on processes already begun e.g., as described in the Prüm Report, identifying Prüm hits that helped investigations. Increased use of SIENA for Swedish Initiative requests, recommended above, will result in more such requests being reflected in SIENA statistics.

Member States are invited to:

- Improve Prüm statistics.

4. CONCLUSIONS

Improving cross-border information exchange is not an end in itself. The purpose is to tackle crime more effectively and thus to reduce harm to victims and to the EU economy.

Cross-border information exchange generally works well and, as illustrated by the examples given above, makes a highly valuable contribution in the fight against serious and cross-border crime in the EU. There is, however, scope for improvement. Legislation that has been agreed must be fully implemented, by all Member States. Looking to the future, Member States should in particular all converge towards more systematic use of the Europol channel and all develop comprehensive national Single Points of Contact (SPOCs).

The Commission for its part will continue to review how the instruments are implemented and used, to provide EU funding and to bring together the different aspects to ensure consistency. The Commission is not here proposing any new instrument. If it does in the future, it will follow the substantive principles in the 2010 Overview Communication: safeguarding fundamental rights, and ensuring necessity, subsidiarity and accurate risk management.

A strong effort is still needed to ensure relevant information is shared at Europol so as to create an EU-wide picture of cross-border criminality. The Commission's forthcoming proposal for Europol reform will address this need. However, the provision of information to Europol would already be facilitated by the recommendations in this Communication for more systematic use of the Europol channel and its secure communications tool SIENA.

To follow up on this Communication, the Commission will continue to work with Member States in the context of the EU Information Management Strategy for internal security, and it proposes that the Council should hold an annual debate in its Internal Security Committee.

The Commission also invites the European Parliament to debate its recommendations, including in its Special Committee on Organised Crime, Corruption and Money Laundering.