



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 7 April 2009**

**8083/09**

**LIMITE**

**CRIMORG 48  
ENFOPOL 64  
ENFOCUSTOM 35  
COMIX 261**

**NOTE**

---

from :            Presidency  
to :                delegations

---

No. prev. doc.    16780/08 CRIMORG 212 ENFOPOL 253 ENFOCUSTOM 109 COMIX 888

---

Subject :         Guidelines on the implementation of Council Framework Decision 2006/960/JHA  
of 18 December 2006 on simplifying the exchange of information and intelligence  
between law enforcement authorities of the Member States of the European Union

---

Delegations will find enclosed the guidelines on the "Swedish Framework Decision", endorsed by the Council on 27-28 November 2008 and adapted to take account of the results of the road test and additional contributions of delegations to the Annexes.

This latest version includes the new chapters 2.3 and 2.4, following the discussion of the Ad Hoc Working Group on 19 February 2009. For information, an annex has been added containing the references of the Member States' notifications of bilateral agreements.

**FRAMEWORK DECISION (2006/960/JHA) OF 18 DECEMBER 2006 ON SIMPLIFYING  
THE EXCHANGE OF INFORMATION AND INTELLIGENCE BETWEEN LAW  
ENFORCEMENT AUTHORITIES OF THE MEMBER STATES OF THE  
EUROPEAN UNION**

**CONTENTS<sup>1</sup>**

- 0. Introduction
- 1. Implementation of the Framework Decision
  - 1.1 Competent law enforcement authorities
  - 1.2 List of information that can be transmitted pursuant to the Framework Decision
  - 1.3 Contacts in the case of urgency
- 2. Use of the Framework Decision
  - 2.1 Channel of communication
  - 2.2 Requests in cases of urgency
  - 2.3 Exchange with Europol
- 3. Links to more information

**Annexes**

- I. Text of Framework Decision 2006/960/JHA as published in OJ L 386 of 29.12.2006, p. 89
- II. National fact sheets
- III. List of competent authorities
- IV. List of contact details in case of urgency

---

<sup>1</sup> The comments contained here are not binding and do not affect domestic legislation implementing the Framework Decision. Comments are merely recommendations. Authorities are, however, reminded of their obligation to interpret their national law in conformity with the Framework Decision (see the Pupino case in the European Court of Justice C-105/03).

## 0. Introduction

- The aim of this publication is to provide guidelines for the implementation of *Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union* and should be adapted in the light of experience acquired, while supplying the competent authorities with specific information on how the forms attached to the Council Framework Decision should ideally be filled in.
- The Framework Decision aims to enhance the effective and expeditious exchange of information and intelligence between law enforcement authorities, which was too often hampered by formal procedures, administrative structures and legal obstacles.
- The Framework Decision does **not** purport to change the Member States' systems of investigation and intelligence gathering and does **not** aim to centralise all exchange of information and intelligence. However, the Decision implies an improvement of the existing ways of exchanging information and intelligence by setting rules on procedures, time limits and grounds for refusal, with the aim of simplifying the exchange.
- The Framework Decision should be used by law enforcement authorities for exchanging existing information and intelligence effectively and expeditiously **for the purpose of conducting criminal investigations or criminal intelligence operations**.
- In that context, Member States shall ensure that the **conditions for** providing information and intelligence to competent law enforcement authorities of **other Member States are not stricter than the conditions applicable at national level** for providing and requesting information and intelligence.
- These guidelines may be updated in future as necessary in the light of practical experience and/or amendments to the Framework Decision.

## **1. Implementation of the Framework Decision in the EU Member States**

### **1.1. Competent law enforcement authorities**

In accordance with Article 2(a) of the Framework Decision, a “competent law enforcement authority” covers

- a national police customs or other authority
- that is authorised by national law
- to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities.

Agencies or units dealing especially with national security issues are **not** covered.

Member States shall state in a declaration which authorities are covered by the concept of "competent law enforcement authority".

The list of these authorities is set out in Annex III.

### **1.2. List of information that can be transmitted pursuant to the Framework Decision**

According to Article 2(d), “information and/or intelligence” covers the following two categories:

- any type of information or data which is held by law enforcement authorities
- any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures.

Since the content of these categories depends on national legislation, some practical guidance is set out in the national fact sheets in Annex II. Without being limitative, these lists set out the type of information available to the Member States' authorities that can generally be provided pursuant to the Framework Decision.

With a view to a clear understanding of Article 1(5), it should be taken into account that "coercive measures" can be understood differently by Member States. Where appropriate, indications are given in the national fact sheets (see Annex II).

### **1.3 Contacts in the case of urgency**

In accordance with Article 6(1) of the Framework Decision, exchange of information and intelligence applying the rules of the Framework Decision may take place via any existing channel of international law enforcement cooperation.

However, it was felt useful to draw up a list of contacts that can be used in case of urgency.

The details provided by Member States about these contacts are set out in Annex IV.

## **2. Use of the Framework Decision**

### **2.1 Channel of communication**

Pursuant to Article 6 of the Framework Decision, the requesting Member State may choose between any of the existing channel for international law enforcement cooperation, the most important ones being currently:

- SIRENE
- ENU/EUROPOL Liaison Officer
- INTERPOL NCB
- Liaison officers
- Mutual administrative international customs assistance ("Naples II Convention")
- Bilateral cooperation channels (including Police and Customs Cooperation Centres)

The requested Member State normally replies through the same channel used for the request. Where the requested Member State must for legitimate reasons reply through another channel, the requesting authority is informed of this change.

The choice of channel will be guided by the following criteria:

- subject
- requested country
- level of security/confidentiality required
- urgency

The *Manual of Good Practices concerning the International Police Cooperation Units at National Level* (document 7968/08 ENFOPOL 63 + COR 1), as approved by the Police Chiefs, includes the following proposed criteria for use of channels:

a) *geographical approach:*

- *nationality/residence/origin of person or object concerned is known and request concerns establishing details (address, phone number, fingerprints, DNA, registration, ...)*
- *nationality/residence/origin of person or object concerned is not known*

b) *thematic approach:*

- *Europol (organised crime, at least 2 MS, connection to AWF, need for joint approach)*
- *confidentiality / sensitivity*
- *channel used for previous related request*

c) *technical approach:*

- *IT-criteria: need of secure channels (BDL for intelligence and terrorism-related information) or technical compatibility (SIRPIT for fingerprints)*

d) *urgency*

- *urgency / proven speed of channel (in particular immediate risk for person's physical integrity, immediate loss of evidence, request for urgent cross border operation or surveillances)*
- *priority*

## 2.2. Requests in cases of urgency

As the notion of urgency is not defined in Framework Decision 2006/960/JHA, it seems advisable for all Member States to have a convergent approach to urgent requests so that this procedure, which places heavy demands on the requested State, is used in a balanced and reasonable manner. Also, Member States will ensure that the notion of “urgency” is interpreted in a restricted manner.

The following guidance is therefore offered to provide help in determining what circumstances may be deemed as “urgent”, but is not to be regarded as definitive. In any case, the question of whether a request is urgent shall be evaluated on a case-by-case basis, avoiding that it becomes a trite indication.

"Urgent" cases as referred to in Article 4 of Framework Decision 2006/960 can be understood to mean any situation during which the fact of obtaining information will:

- prevent a risk of death or harm to persons or serious damage to property;
- result in, or terminate, a decision involving deprivation of liberty (where such a decision has to be taken within a short period of time);
- prevent the loss of information that is important for the further stages of an investigation.

Examples of such situations would be:

- abductions and hostage-takings;
- the risk that a serious offence will be committed or repeated;
- the disappearance of minors, and the disappearance of adults giving cause for concern;
- decisions relating to the keeping a person in police custody, or remanding a suspect in custody or releasing a person;
- the possible escape of a suspect in a serious case;
- the need to obtain information at risk of imminent destruction.

## 2.3. Disproportionate requests or requests concerning "minor offences"

Article 1 of the Framework Decision clearly explains that it concerns the exchange of information "for the purpose of conducting criminal investigations or criminal intelligence operations" and that it "does not impose any obligation (...) to provide information and intelligence to be used as evidence (...)".

Because resources are by definition limited in each Member State, they should be maximised and be used in the most relevant and efficient way.

That is why Article 10 provides that information can be withheld when replying to a request would clearly be disproportionate or irrelevant with regard to the purposes for which it has been requested. The same reasoning underlies the rule that where an offence is punishable by one year of imprisonment or less, the requested Member State is not obliged to reply.

Obviously, these provisions do not prevent one Member State from asking requests related to "minor" offences, nor do they prevent the other Member State from replying. If the requesting Member State provides a sound explanation of the reasons for its request, even if it is about a minor offence, it will be easier for the requested Member State to consider whether resources can be spent on it.

However, the time limits set out in the Framework Decision would not mandatorily apply to such requests.

#### **2.4. Incomplete requests**

Where the request does not contain all information necessary to reply, the requested Member State should as soon as possible inform the requesting authorities thereof. The time limits for replying only start running if and once the requesting Member State has completed the request.

If the request is not completed, the request Member State has obviously no obligation to reply.

#### **2.5. Exchange with Europol**

Care should be taken to copy Europol each time a request falls within Europol's mandate. In addition, the answer provided by the requested Member State should also be copied to Europol.

This principle has to be applied whatever the channel is chosen, including the Europol channel.

In this respect, a difference has to be made between, on the one hand, the use of the Europol channel as a means of information exchange between Member States, using their liaison officers and, on the other hand, the direct communication to Europol, as an organisation, for any intelligence falling within its mandate.



All information received from the Member States has to be routed via the national units in accordance with Art. 4(2) of the Europol Convention, i.e. from the national units via the Europol liaison officers to Europol. For the communication between the liaison officers and Europol the only tool to be used to transmit the forms is InfoEx.<sup>2</sup>

There are 4 options to provide the information and intelligence exchanged in accordance with Framework Decision 2006/960/JHA,

- to *transmit the form to a specific analysis workfile (AWF)* if the offence or criminal activity is addressed by the AWF in question; such information and intelligence will be processed in compliance with the applicable legal provisions, processes, policies and procedures; this includes existing cross-matching functionalities and the subsequent notification of matches subject to the handling codes that apply;
- to *send the form to the Serious Crime Unit* specialised in the specific crime type; in these units knowledge and expertise is available to support law enforcement efforts of Member States and cooperation partners, like non-EU States;
- to *insert the information or intelligence into the Europol Information System*, provided the conditions for insertion are met; this can be done directly both by the national units and the Europol liaison officers; such information and intelligence will be processed in compliance with the applicable legal provisions, processes, policies and procedures; this includes existing cross-matching functionalities and the subsequent notification of matches subject to the handling codes that apply;

---

<sup>2</sup> The existing InfoEx tool will be replaced by the Secure Information Exchange Network Application (SIENA). In the first release, expected by 30 June 2009, the national units will be able to exchange information directly with and via Europol without the necessity to transmit the information via their Europol liaison officers.

- *to send the form without specific destination to Europol*; in that case, Europol's Serious Crime Department<sup>3</sup> will assess the information and forward it to the relevant unit or AWF, the latter upon consent of the Member State that sent the information; in addition, Europol can advise the Member State to insert the information into the Europol Information System; the general principles of the processing of data received without specific destination at Europol are 1) that any decision to contribute information or intelligence to an AWF or to the Europol Information System is made by the Member State and 2) that the Member State receives feedback on the processing, including on matches that were found.

The first three options can be combined.

In the cooperation with Europol specific handling codes are used that differ from the conditions for use mentioned in the forms for the Swedish FWD. The Europol handling codes can be filled in when using the InfoEx and when inserting data into the Europol Information System. Information and intelligence received by Europol will be processed in accordance with the specific Europol handling codes in addition to the conditions on the use expressed by the sender of the form.

### **3. Links to more information**

See also Manual of good practices concerning the International Police Cooperation Units at National Level (doc. 7968/08 ENFOPOL 63 + COR 1), as adopted by the Police Chiefs meeting on 19 March 2008).

---

<sup>3</sup> Via its [future] front office.

(Acts adopted under Title VI of the Treaty on European Union)

COUNCIL FRAMEWORK DECISION 2006/960/JHA

of 18 December 2006

on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 30(1)(a) and (b) and 34(2)(b) thereof,

Having regard to the initiative of the Kingdom of Sweden,

Having regard to the opinion of the European Parliament,

Whereas:

- (1) One of the core objectives of the European Union is to provide its citizens with a high level of security within an area of freedom, security and justice.
- (2) That objective is to be achieved by preventing and combating crime through closer cooperation between law enforcement authorities in the Member States, while respecting the principles and rules relating to human rights, fundamental freedoms and the rule of law on which the Union is founded and which are common to the Member States.
- (3) Exchange of information and intelligence on crime and criminal activities is the basis for law enforcement cooperation in the Union serving the overall objective of improving the safety of the Union's citizens.
- (4) The timely access to accurate and up to date information and intelligence is a crucial element for the possibility of law enforcement authorities to successfully detect, prevent and investigate crime or criminal activity, in particular within an area where internal border controls have been abolished. As the activities of criminals are carried out clandestinely, they need to be controlled, and information relating to them needs to be exchanged particularly expeditiously.
- (5) It is important that the possibilities for law enforcement authorities to obtain information and intelligence concerning serious crime and terrorist acts from other Member States be viewed horizontally and not in terms of differences with regard to type of crime or division of competencies between law enforcement or judicial authorities.

(6) Currently, effective and expeditious exchange of information and intelligence between law enforcement authorities is seriously hampered by formal procedures, administrative structures and legal obstacles laid down in Member States' legislation; such a state of affairs is unacceptable to the citizens of the European Union and it therefore calls for greater security and more efficient law enforcement while protecting human rights.

(7) It is necessary for law enforcement authorities to be able to request and obtain information and intelligence from other Member States at different stages of investigation, from the phase of gathering criminal intelligence to the phase of criminal investigation. The Member State's systems are different in that respect, but this Framework Decision does not purport to change these systems. However, it seeks, as regards certain types of information and intelligence, to ensure that certain information vital for law enforcement authorities is exchanged expeditiously within the Union.

(8) The absence of a common legal framework for the effective and expeditious exchange of information and intelligence between the law enforcement authorities of the Member States is a deficiency that will have to be remedied; the Council of the European Union therefore deems it necessary to adopt a legally binding instrument on simplifying the exchange of information and intelligence. This Framework Decision should not affect existing or future instruments which allow the objectives of this Framework Decision to be extended or which facilitate the procedures for exchanging information and intelligence, such as the Convention of 18 December 1997 drawn up on the basis of Article K.3 of the Treaty on European Union on Mutual Assistance and Cooperation between Customs Administrations<sup>(1)</sup>.

(9) As regards the exchange of information, this Framework Decision is without prejudice to essential national security interests, the jeopardizing of the success of a current investigation or the safety of individuals, or specific intelligence activities in the field of State security.

(1) OJ C 24, 23.1.1998, p. 2.

- (10) It is important to promote the exchange of information as widely as possible, in particular in relation to offences linked directly or indirectly to organised crime and terrorism, and in a way which does not detract from the required level of cooperation between Member States under existing arrangements.
- (11) The common interest of Member States in fighting crime of a cross-border nature must strike the appropriate balance between fast and efficient law enforcement cooperation and agreed principles and rules on data protection, fundamental freedoms, human rights and individual liberties.
- (12) In the Declaration on combating terrorism as adopted by the European Council at its meeting on 25 March 2004, the European Council instructed the Council to examine measures for simplifying the exchange of information and intelligence between law enforcement authorities of the Member States.
- (13) As regards Iceland and Norway, this Framework Decision constitutes a development of the provisions of the Schengen acquis which fall within the area referred to in Article 1 of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis<sup>(1)</sup>. The procedures set out in that Agreement have been followed in respect of this Framework Decision.
- (14) As regards Switzerland, this Framework Decision constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement signed between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis, which fall within the area referred to in Article 1(4) of Decision 1999/437/EC read in conjunction with Article 4(1) of Decision 2004/860/EC<sup>(2)</sup> on the signing on behalf of the European Community and on the provisional application of certain provisions of that Agreement, and with Article 4(1) of Decision 2004/849/EC<sup>(3)</sup> on the signing on behalf of the European Union, and on the provisional application of certain provisions of that Agreement.

<sup>(1)</sup> OJ L 176, 10.7.1999, p. 31.

<sup>(2)</sup> OJ L 370, 17.12.2004, p. 78.

<sup>(3)</sup> OJ L 368, 15.12.2004, p. 26.

HAS ADOPTED THIS FRAMEWORK DECISION:

## TITLE I

### SCOPE AND DEFINITIONS

#### Article 1

##### Objective and scope

1. The purpose of this Framework Decision is to establish the rules under which Member States' law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.

2. This Framework Decision shall be without prejudice to bilateral or multilateral agreements or arrangements between Member States and third countries and to instruments of the European Union on mutual legal assistance or mutual recognition of decisions regarding criminal matters, including any conditions set by third countries concerning the use of information once supplied.

3. This Framework Decision covers all information and/or intelligence as defined in Article 2(d). It does not impose any obligation on the part of the Member States to gather and store information and intelligence for the purpose of providing it to the competent law enforcement authorities of other Member States.

4. This Framework Decision does not impose any obligation on the part of the Member States to provide information and intelligence to be used as evidence before a judicial authority nor does it give any right to use such information or intelligence for that purpose. Where a Member State has obtained information or intelligence in accordance with this Framework Decision, and wishes to use it as evidence before a judicial authority, it has to obtain consent of the Member State that provided the information or intelligence, where necessary under the national law of the Member State that provided the information or intelligence, through the use of instruments regarding judicial cooperation in force between the Member States. Such consent is not required where the requested Member State has already given its consent for the use of information or intelligence as evidence at the time of transmittal of the information or intelligence.

5. This Framework Decision does not impose any obligation to obtain any information or intelligence by means of coercive measures, defined in accordance with national law, in the Member State receiving the request for information or intelligence.

6. Member States shall, where permitted by and in accordance with their national law, provide information or intelligence previously obtained by means of coercive measures.

7. This Framework Decision shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union and any obligations incumbent on law enforcement authorities in this respect shall remain unaffected.

(ii) any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures, in accordance with Article 1(5).

(e) 'offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA on the European arrest warrant' ('offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA'); offences under national law which correspond to or are equivalent to those referred to in that provision.

## Article 2

### Definitions

For the purposes of this Framework Decision:

(a) 'competent law enforcement authority': a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. Agencies or units dealing especially with national security issues are not covered by the concept of competent law enforcement authority. Every Member State shall, by 18 December 2007, state in a declaration deposited with the General Secretariat of the Council which authorities are covered by the concept of 'competent law enforcement authority'. Such a declaration may be modified at any time.

(b) 'criminal investigation': a procedural stage within which measures are taken by competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts;

(c) 'criminal intelligence operation': a procedural stage, not yet having reached the stage of a criminal investigation, within which a competent law enforcement authority is entitled by national law to collect, process and analyse information about crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future;

(d) 'information and/or intelligence':

(i) any type of information or data which is held by law enforcement authorities;

and

## TITLE II

### EXCHANGE OF INFORMATION AND INTELLIGENCE

## Article 3

### Provision of information and intelligence

1. Member States shall ensure that information and intelligence can be provided to the competent law enforcement authorities of other Member States in accordance with this Framework Decision.

2. Information and intelligence shall be provided at the request of a competent law enforcement authority, acting in accordance with the powers conferred upon it by national law, conducting a criminal investigation or a criminal intelligence operation.

3. Member States shall ensure that conditions not stricter than those applicable at national level for providing and requesting information and intelligence are applied for providing information and intelligence to competent law enforcement authorities of other Member States. In particular, a Member State shall not subject the exchange, by its competent law enforcement authority with a competent law enforcement authority of another Member State, of information or intelligence which in an internal procedure may be accessed by the requested competent law enforcement authority without a judicial agreement or authorisation, to such an agreement or authorisation.

4. Where the information or intelligence sought may, under the national law of the requested Member State, be accessed by the requested competent law enforcement authority only pursuant to an agreement or authorisation of a judicial authority, the requested competent law enforcement authority shall be obliged to ask the competent judicial authority for an agreement or authorisation to access and exchange the information sought. The competent judicial authority of the requested Member State shall apply the same rules for its decision, without prejudice to Article 10(1) and (2), as in a purely internal case.

(1) OJ L 190, 18.7.2002, p. 1.

5. Where the information or intelligence sought has been obtained from another Member State or from a third country and is subject to the rule of speciality, its transmission to the competent law enforcement authority of another Member State may only take place with the consent of the Member State or third country that provided the information or intelligence.

#### Article 4

##### Time limits for provision of information and intelligence

1. Member States shall ensure that they have procedures in place so that they can respond within at most eight hours to urgent requests for information and intelligence regarding offences referred to in Article 2(2) of Framework Decision 2002/584/JHA, when the requested information or intelligence is held in a database directly accessible by a law enforcement authority.

2. If the requested competent law enforcement authority is unable to respond within eight hours, it shall provide reasons for that on the form set out in Annex A. Where the provision of the information or intelligence requested within the period of eight hours would put a disproportionate burden on the requested law enforcement authority, it may postpone the provision of the information or intelligence. In that case the requested law enforcement authority shall immediately inform the requesting law enforcement authority of this postponement and shall provide the requested information or intelligence as soon as possible, but not later than within three days. The use made of the provisions under this paragraph shall be reviewed by 19 December 2009.

3. Member States shall ensure that for non-urgent cases, requests for information and intelligence regarding offences referred to in Article 2(2) of Framework Decision 2002/584/JHA should be responded to within one week if the requested information or intelligence is held in a database directly accessible by a law enforcement authority. If the requested competent law enforcement authority is unable to respond within one week, it shall provide reasons for that on the form set out in Annex A.

4. In all other cases, Member States shall ensure that the information sought is communicated to the requesting competent law enforcement authority within 14 days. If the requested competent law enforcement authority is unable to respond within 14 days, it shall provide reasons for that on the form set out in Annex A.

#### Article 5

##### Requests for information and intelligence

1. Information and intelligence may be requested for the purpose of detection, prevention or investigation of an offence where there are factual reasons to believe that relevant information and intelligence is available in another Member State. The request shall set out those factual reasons and explain the purpose for which the information and intelligence is sought and the connection between the purpose and the person who is the subject of the information and intelligence.

2. The requesting competent law enforcement authority shall refrain from requesting more information or intelligence or setting narrower time frames than necessary for the purpose of the request.

3. Requests for information or intelligence shall contain at least the information set out in Annex B.

#### Article 6

##### Communication channels and language

1. Exchange of information and intelligence under this Framework Decision may take place via any existing channels for international law enforcement cooperation. The language used for the request and the exchange of information shall be the one applicable for the channel used. Member States shall, when making their declarations in accordance with Article 2(a), also provide the General Secretariat of the Council with details of the contacts to which requests may be sent in cases of urgency. These details may be modified at any time. The General Secretariat of the Council shall communicate to the Member States and the Commission the declarations received.

2. Information or intelligence shall also be exchanged with Europol in accordance with the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) <sup>(1)</sup> and with Eurojust in accordance with the Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime <sup>(2)</sup>, insofar as the exchange refers to an offence or criminal activity within their mandate.

<sup>(1)</sup> OJ C 316, 27.11.1995, p. 2. Convention as last amended by the Protocol drawn up on the basis of Article 43(1) of the Europol Convention (OJ C 2, 6.1.2004, p. 3).

<sup>(2)</sup> OJ L 63, 6.3.2002, p. 1. Decision as last amended by Decision 2003/659/JHA (OJ L 245, 29.9.2003, p. 44).

*Article 7***Spontaneous exchange of information and intelligence**

1. Without prejudice to Article 10, the competent law enforcement authorities shall, without any prior request being necessary, provide to the competent law enforcement authorities of other Member States concerned information and intelligence in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA. The modalities of such spontaneous exchange shall be regulated by the national law of the Member States providing the information.

2. The provision of information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question.

*Article 8***Data protection**

1. Each Member State shall ensure that the established rules on data protection provided for when using the communication channels referred to in Article 6(1) are applied also within the procedure on exchange of information and intelligence provided for by this Framework Decision.

2. The use of information and intelligence which has been exchanged directly or bilaterally under this Framework Decision shall be subject to the national data protection provisions of the receiving Member State, where the information and intelligence shall be subject to the same data protection rules as if they had been gathered in the receiving Member State. The personal data processed in the context of the implementation of this Framework Decision shall be protected in accordance with the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and, for those Member States which have ratified it, the Additional Protocol of 8 November 2001 to that Convention, regarding Supervisory Authorities and Transborder Data Flows. The principles of Recommendation No. R(87) 15 of the Council of Europe Regulating the Use of Personal Data in the Police Sector should also be taken into account when law enforcement authorities handle personal data obtained under this Framework Decision.

3. Information and intelligence provided under this Framework Decision may be used by the competent law enforcement authorities of the Member State to which it has been provided solely for the purposes for which it has been supplied in accordance with this Framework Decision or for preventing an immediate and serious threat to public security; processing for other purposes shall be permitted solely with the prior authorisation of the communicating Member State and subject to the national law of the receiving Member State. The authorisation may be granted insofar as the national law of the communicating Member State permits.

4. When providing information and intelligence in accordance with this Framework Decision, the providing competent law enforcement authority may pursuant to its national law impose conditions on the use of the information and intelligence by the receiving competent law enforcement authority. Conditions may also be imposed on reporting the result of the criminal investigation or criminal intelligence operation within which the exchange of information and intelligence has taken place. The receiving competent law enforcement authority shall be bound by such conditions, except in the specific case where national law lays down that the restrictions on use be waived for judicial authorities, legislative bodies or any other independent body set up under the law and made responsible for supervising the competent law enforcement authorities. In such cases, the information and intelligence may only be used after prior consultation with the communicating Member State whose interests and opinions must be taken into account as far as possible. The receiving Member State may, in specific cases, be requested by the communicating Member State to give information about the use and further processing of the transmitted information and intelligence.

*Article 9***Confidentiality**

The competent law enforcement authorities shall take due account, in each specific case of exchange of information or intelligence, of the requirements of investigation secrecy. To that end the competent law enforcement authorities shall, in accordance with their national law, guarantee the confidentiality of all provided information and intelligence determined as confidential.

*Article 10***Reasons to withhold information or intelligence**

1. Without prejudice to Article 3(3), a competent law enforcement authority may refuse to provide information or intelligence only if there are factual reasons to assume that the provision of the information or intelligence would:

(a) harm essential national security interests of the requested Member State;

or

(b) jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals;

or

(c) clearly be disproportionate or irrelevant with regard to the purposes for which it has been requested.

2. Where the request pertains to an offence punishable by a term of imprisonment of one year or less under the law of the requested Member State, the competent law enforcement authority may refuse to provide the requested information or intelligence.

3. The competent law enforcement authority shall refuse to provide information or intelligence if the competent judicial authority has not authorised the access and exchange of the information requested pursuant to Article 3(4).

### TITLE III

#### FINAL PROVISIONS

#### Article 11

##### Implementation

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision before 19 December 2006.

2. Member States shall transmit to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national laws the obligations imposed on them under this Framework Decision. On the basis of this and other information provided by the Member States on request, the Commission shall, before 19 December 2006, submit a report to the Council on the operation of this Framework Decision. The Council shall before 19 December 2006 assess the extent to which Member States have complied with the provisions of this Framework Decision.

#### Article 12

##### Relation to other instruments

1. The provisions of Article 39(1), (2) and (3) and of Article 46 of the Convention Implementing the Schengen Agreement <sup>(1)</sup>, in as far as they relate to exchange of information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations as provided for by this Framework Decision, shall be replaced by the provisions of this Framework Decision.

2. The Decision of the Schengen Executive Committee of 16 December 1998 on cross-border police cooperation in the area of crime prevention and detection (SCH/Com-ex (98) 51 rev 3) <sup>(2)</sup> and the Decision of the Schengen Executive Committee of 28 April 1999 on the improvement of police cooperation in preventing and detecting criminal offences (SCH/Com-ex (99) 18) <sup>(3)</sup> are hereby repealed.

3. Member States may continue to apply bilateral or multilateral agreements or arrangements in force when this Framework Decision is adopted in so far as such agreements or arrangements allow the objectives of this Framework Decision to be extended and help to simplify or facilitate further the procedures for exchanging information and intelligence falling within the scope of this Framework Decision.

4. Member States may conclude or bring into force bilateral or multilateral agreements or arrangements after this Framework Decision has come into force in so far as such agreements or arrangements allow the objectives of this Framework Decision to be extended and help to simplify or facilitate further the procedures for exchanging information and intelligence falling within the scope of this Framework Decision.

5. The agreements and arrangements referred to in paragraphs 3 and 4 may in no case affect relations with Member States which are not parties to them.

<sup>(1)</sup> OJ L 239, 22.9.2000, p. 19. Convention as last amended by Regulation (EC) No 1160/2005 of the European Parliament and of the Council (OJ L 191, 22.7.2005, p. 18).

<sup>(2)</sup> OJ L 239, 22.9.2000, p. 407.

<sup>(3)</sup> OJ L 239, 22.9.2000, p. 421.



6. Member States shall no later than 19 December 2006, notify the Council and the Commission of the existing agreements and arrangements referred to in paragraph 3 which they wish to continue applying.

7. Member States shall also notify the Council and the Commission of any new agreement or arrangement as referred to in paragraph 4, within three months of their signature or, for those instruments which had already been signed before the adoption of this Framework Decision, their entry into force.

*Article 13*

**Entry into force**

This Framework Decision shall enter into force on the day following its publication in the *Official Journal of the European Union*.

Done at Brussels, 18 December 2006.

For the Council  
The President  
J.-E. ENESTAM

## ANNEX A

## INFORMATION EXCHANGE UNDER COUNCIL FRAMEWORK DECISION 2006/960/JHA FORM TO BE USED BY THE REQUESTED MEMBER STATE IN CASE OF TRANSMISSION/DELAY/REFUSAL OF INFORMATION

This form shall be used to transmit the requested information and/or intelligence, to inform the requesting authority of the impossibility of meeting the normal deadline, of the necessity of submitting the request to a judicial authority for an authorisation, or of the refusal to transmit the information.

This form may be used more than once during the procedure (e.g. if the request has first to be submitted to a judicial authority and it later transpires that the execution of the request has to be refused).

<b>Requested authority (name, address, telephone, fax, e-mail, Member State)</b>	
<b>Details of the handling agent (optional):</b>	
<b>Reference number of this answer</b>	
<b>Date and reference number of previous answer</b>	
<b>Answering to the following requesting authority</b>	
<b>Date and time of the request</b>	
<b>Reference number of the request</b>	

Normal time limit under Article 4 of Framework Decision 2006/960/JHA	
The offence falls under Article 2(2) of Framework Decision 2002/584/JHA and the requested information or intelligence is held in a database directly accessible by a law enforcement authority in the requested Member State	Urgency requested → <input type="checkbox"/> 8 hours
	Urgency not requested → <input type="checkbox"/> 1 week
Other cases	→ <input type="checkbox"/> 14 days

Information transmitted under Framework Decision 2006/960/JHA: information and intelligence provided
<p>1. Use of transmitted information or intelligence</p> <p><input type="checkbox"/> may be used solely for the purposes for which it has been supplied or for preventing an immediate and serious threat to public security;</p> <p><input type="checkbox"/> is authorised also for other purposes, subject to the following conditions (optional):</p>
<p>2. Reliability of the source</p> <p><input type="checkbox"/> Reliable</p> <p><input type="checkbox"/> Mostly reliable</p> <p><input type="checkbox"/> Not reliable</p> <p><input type="checkbox"/> Cannot be assessed</p>
<p>3. Accuracy of the information or intelligence</p> <p><input type="checkbox"/> Certain</p> <p><input type="checkbox"/> Established by the source</p> <p><input type="checkbox"/> Hearsay-confirmed</p> <p><input type="checkbox"/> Hearsay- not confirmed</p>

4. The result of the criminal investigation or criminal intelligence operation within which the exchange of information has taken place has to be reported to the transmitting authority

- No  
 Yes

5. In case of spontaneous exchange, reasons for believing that the information or intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA:

**DELAY – It is not possible to respond within the applicable time limit under Article 4 of Framework Decision 2006/960/JHA**

The information or intelligence cannot be provided within the given time-limit for the following reasons:

It is likely to be given within:

- 1 day     2 days     3 days  
 .... weeks  
 1 month

- The authorisation of a judicial authority has been requested.  
The procedure leading up to the granting/refusal of the authorisation is expected to last ... weeks

**REFUSAL — The information or intelligence:**

- could not be provided and requested at national level; or  
 cannot be provided, for one or more of the following reasons:

A — Reason related to judicial control which prevents the transmission or requires the use of mutual legal assistance

- the competent judicial authority has not authorised the access and exchange of the information or intelligence
- the requested information or intelligence has previously been obtained by means of coercive measures and its provision is not permitted under the national law
- the information or intelligence is not held
- by law enforcement authorities; or
  - by public authorities or by private entities in a way which makes it available to law enforcement authorities without the taking of coercive measures

- B — The provision of the requested information or intelligence would harm essential national security interests or would jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals or would clearly be disproportionate or irrelevant with regard to the purposes for which it has been requested.

If case A or B is used, provide, if deemed necessary, additional information or reasons for refusal (optional):

- D — The requested authority decides to refuse execution because the request pertains, under the law of the requested Member State, to the following offence (nature of the offence and its legal qualification to be specified) ..... which is punishable by one year or less of imprisonment

- E — The requested information or intelligence is not available

- F — The requested information or intelligence has been obtained from another Member State or from a third country and is subject to the rule of speciality and that Member State or third country has not given its consent to the transmission of the information or intelligence.

## ANNEX B

## INFORMATION EXCHANGE UNDER COUNCIL FRAMEWORK DECISION 2006/960/JHA REQUEST FORM FOR INFORMATION AND INTELLIGENCE TO BE USED BY THE REQUESTING MEMBER STATE

This form shall be used when requesting information and intelligence under Framework Decision 2006/960/JHA

## I — Administrative information

Requesting authority (name, address, telephone, fax, e-mail, Member State):	
Details of the handling agent (optional):	
To the following Member State:	
Date and time of this request:	
Reference number of this request:	

Previous requests				
<input type="checkbox"/> This is the first request on this case				
<input type="checkbox"/> This request follows previous requests in the same case				
Previous request(s)			Answer(s)	
	Date	Reference number (in the requesting Member State)	Date	Reference number (in the requested Member State)
1.				
2.				
3.				
4.				

If the request is sent to more than one authority in the requested Member State, please specify each of the channels used:	
<input type="checkbox"/> ENU/Europol Liaison Officer	<input type="checkbox"/> For information <input type="checkbox"/> For execution
<input type="checkbox"/> Interpol NCB	<input type="checkbox"/> For information <input type="checkbox"/> For execution
<input type="checkbox"/> Sirene	<input type="checkbox"/> For information <input type="checkbox"/> For execution
<input type="checkbox"/> Liaison Officer	<input type="checkbox"/> For information <input type="checkbox"/> For execution
<input type="checkbox"/> Other (please specify):	<input type="checkbox"/> For information <input type="checkbox"/> For execution
If the same request is sent to other Member States, please specify the other Member States and the channel used (optional)	

II — Time limits

Reminder: time limits under Article 4 of Framework Decision 2006/960/JHA

A — The offence falls under Article 2(2) of Framework Decision 2002/584/JHA

and

the requested information or intelligence is held in a database directly accessible by a law enforcement authority

→ The request is urgent → Time limit: 8 hours with possibility to postpone

→ The request is not urgent → Time limit: 1 week

B — Other cases: time limit: 14 days

<input type="checkbox"/> Urgency IS requested
<input type="checkbox"/> Urgency is NOT requested
Grounds for urgency (e.g.: suspects are being held in custody, the case has to go to court before a specific date):
<b>Information or intelligence requested</b>

<b>Type of crime(s) or criminal activity(ies) being investigated</b>
Description of the circumstances in which the offence(s) was (were) committed, including the time, place and degree of participation in the offence(s) by the person who is the subject of the request for information or intelligence:

Nature of the offence(s)																																
<p>A — Application of Article 4(1) or 4(3) of the Framework Decision 2006/960/JHA</p> <p><input type="checkbox"/> A.1. The offence is punishable by a maximum term of imprisonment of at least three years in the requesting Member State AND</p> <p>A.2. The offence is one (or more) of the following:</p> <table border="0"> <tr> <td><input type="checkbox"/> Participation in a criminal organisation</td> <td><input type="checkbox"/> Laundering of the proceeds of crime</td> </tr> <tr> <td><input type="checkbox"/> Terrorism</td> <td><input type="checkbox"/> Counterfeiting of currency, including the euro</td> </tr> <tr> <td><input type="checkbox"/> Trafficking in human beings</td> <td><input type="checkbox"/> Computer-related crime</td> </tr> <tr> <td><input type="checkbox"/> Sexual exploitation of children and child pornography</td> <td><input type="checkbox"/> Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties</td> </tr> <tr> <td><input type="checkbox"/> Illicit trafficking in narcotic drugs and psychotropic substances</td> <td><input type="checkbox"/> Facilitation of unauthorised entry and residence</td> </tr> <tr> <td><input type="checkbox"/> Illicit trafficking in weapons, munitions and explosives</td> <td><input type="checkbox"/> Murder, grievous bodily injury</td> </tr> <tr> <td><input type="checkbox"/> Corruption</td> <td><input type="checkbox"/> Illicit trade in human organs and tissue</td> </tr> <tr> <td><input type="checkbox"/> Fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests</td> <td><input type="checkbox"/> Kidnapping, illegal restraint and hostage-taking</td> </tr> <tr> <td><input type="checkbox"/> Organised or armed robbery</td> <td><input type="checkbox"/> Racism and xenophobia</td> </tr> <tr> <td><input type="checkbox"/> Illicit trafficking in cultural goods, including antiques and works of art</td> <td><input type="checkbox"/> Illicit trafficking in nuclear or radioactive materials</td> </tr> <tr> <td><input type="checkbox"/> Swindling</td> <td><input type="checkbox"/> Trafficking in stolen vehicles</td> </tr> <tr> <td><input type="checkbox"/> Racketeering and extortion</td> <td><input type="checkbox"/> Rape</td> </tr> <tr> <td><input type="checkbox"/> Counterfeiting and piracy of products</td> <td><input type="checkbox"/> Arson</td> </tr> <tr> <td><input type="checkbox"/> Forgery of administrative documents and trafficking therein</td> <td><input type="checkbox"/> Crimes within the jurisdiction of the International Criminal Court</td> </tr> <tr> <td><input type="checkbox"/> Forgery of means of payment</td> <td><input type="checkbox"/> Unlawful seizure of aircraft/ships</td> </tr> <tr> <td><input type="checkbox"/> Illicit trafficking in hormonal substances and other growth promoters</td> <td><input type="checkbox"/> Sabotage</td> </tr> </table> <p>→ The offence therefore falls under Article 2(2) of Framework Decision 2002/584/JHA → Article 4(1) (urgent cases) and 4(3) (non urgent cases) of Framework Decision 2006/960/JHA are therefore applicable as regards time limits for responding to this request</p>	<input type="checkbox"/> Participation in a criminal organisation	<input type="checkbox"/> Laundering of the proceeds of crime	<input type="checkbox"/> Terrorism	<input type="checkbox"/> Counterfeiting of currency, including the euro	<input type="checkbox"/> Trafficking in human beings	<input type="checkbox"/> Computer-related crime	<input type="checkbox"/> Sexual exploitation of children and child pornography	<input type="checkbox"/> Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties	<input type="checkbox"/> Illicit trafficking in narcotic drugs and psychotropic substances	<input type="checkbox"/> Facilitation of unauthorised entry and residence	<input type="checkbox"/> Illicit trafficking in weapons, munitions and explosives	<input type="checkbox"/> Murder, grievous bodily injury	<input type="checkbox"/> Corruption	<input type="checkbox"/> Illicit trade in human organs and tissue	<input type="checkbox"/> Fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests	<input type="checkbox"/> Kidnapping, illegal restraint and hostage-taking	<input type="checkbox"/> Organised or armed robbery	<input type="checkbox"/> Racism and xenophobia	<input type="checkbox"/> Illicit trafficking in cultural goods, including antiques and works of art	<input type="checkbox"/> Illicit trafficking in nuclear or radioactive materials	<input type="checkbox"/> Swindling	<input type="checkbox"/> Trafficking in stolen vehicles	<input type="checkbox"/> Racketeering and extortion	<input type="checkbox"/> Rape	<input type="checkbox"/> Counterfeiting and piracy of products	<input type="checkbox"/> Arson	<input type="checkbox"/> Forgery of administrative documents and trafficking therein	<input type="checkbox"/> Crimes within the jurisdiction of the International Criminal Court	<input type="checkbox"/> Forgery of means of payment	<input type="checkbox"/> Unlawful seizure of aircraft/ships	<input type="checkbox"/> Illicit trafficking in hormonal substances and other growth promoters	<input type="checkbox"/> Sabotage
<input type="checkbox"/> Participation in a criminal organisation	<input type="checkbox"/> Laundering of the proceeds of crime																															
<input type="checkbox"/> Terrorism	<input type="checkbox"/> Counterfeiting of currency, including the euro																															
<input type="checkbox"/> Trafficking in human beings	<input type="checkbox"/> Computer-related crime																															
<input type="checkbox"/> Sexual exploitation of children and child pornography	<input type="checkbox"/> Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties																															
<input type="checkbox"/> Illicit trafficking in narcotic drugs and psychotropic substances	<input type="checkbox"/> Facilitation of unauthorised entry and residence																															
<input type="checkbox"/> Illicit trafficking in weapons, munitions and explosives	<input type="checkbox"/> Murder, grievous bodily injury																															
<input type="checkbox"/> Corruption	<input type="checkbox"/> Illicit trade in human organs and tissue																															
<input type="checkbox"/> Fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests	<input type="checkbox"/> Kidnapping, illegal restraint and hostage-taking																															
<input type="checkbox"/> Organised or armed robbery	<input type="checkbox"/> Racism and xenophobia																															
<input type="checkbox"/> Illicit trafficking in cultural goods, including antiques and works of art	<input type="checkbox"/> Illicit trafficking in nuclear or radioactive materials																															
<input type="checkbox"/> Swindling	<input type="checkbox"/> Trafficking in stolen vehicles																															
<input type="checkbox"/> Racketeering and extortion	<input type="checkbox"/> Rape																															
<input type="checkbox"/> Counterfeiting and piracy of products	<input type="checkbox"/> Arson																															
<input type="checkbox"/> Forgery of administrative documents and trafficking therein	<input type="checkbox"/> Crimes within the jurisdiction of the International Criminal Court																															
<input type="checkbox"/> Forgery of means of payment	<input type="checkbox"/> Unlawful seizure of aircraft/ships																															
<input type="checkbox"/> Illicit trafficking in hormonal substances and other growth promoters	<input type="checkbox"/> Sabotage																															
<p>Or</p> <p><input type="checkbox"/> B — The offence(s) is(are) not covered under A. In this case, description of the offence(s):</p>																																
Purpose for which the information or intelligence is requested																																
Connection between the purpose for which the information or intelligence is requested and the person who is the subject of the information or intelligence																																
Identity(ies) (as far as known) of the person(s) being the main subject(s) of the criminal investigation or criminal intelligence operation underlying the request for information or intelligence																																
Reasons for believing that the information or intelligence is in the requested Member State																																
Restrictions on the use of information contained in this request for purposes other than those for which it has been supplied or for preventing an immediate and serious threat to public security																																
<p><input type="checkbox"/> use granted</p> <p><input type="checkbox"/> use granted, but do not mention the information provider</p> <p><input type="checkbox"/> do not use without authorisation of the information provider</p> <p><input type="checkbox"/> do not use</p>																																

## ANNEX II

## NATIONAL FACT SHEETS

<u>Belgium</u>
<u>Bulgaria</u>
<u>Czech Republic</u>
<u>Denmark</u>
<u>Germany</u>
<u>Estonia</u>
<u>Greece</u>
<u>Spain</u>
<u>France</u>
<u>Ireland</u>
<u>Italy</u>
<u>Cyprus</u>
<u>Latvia</u>
<u>Lithuania</u>
<u>Luxembourg</u>
<u>Hungary</u>
<u>Malta</u>
<u>Netherlands</u>
<u>Austria</u>
<u>Poland</u>
<u>Portugal</u>
<u>Romania</u>
<u>Slovenia</u>
<u>Slovakia</u>
<u>Finland</u>
<u>Sweden</u>
<u>United Kingdom</u>
<u>Iceland</u>
<u>Norway</u>
<u>Switzerland</u>

## **BELGIUM**

1. **INFORMATION AVAILABLE**
2. **LANGUAGES USED IN CASE OF URGENCY**
3. **PREFERRED CHANNEL**

### 1. **INFORMATION AVAILABLE**

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- AFIS/FIT: Automated Fingerprint Identification System/Fingerprint Image Transmission (Ten Prints and Latent Prints)
- ANG /BNG Control: This application has been designed for searches by Belgian police officers in the police's general national database (*Algemene Nationale Gegevensbank/Banque de données générale*), and focuses on persons, objects and means of transportation subject to a measure to be taken. Searching this database automatically implies searching the Schengen Information System (SIS).
- ANG / BNG Consultation: This database holds information on:
  - Specific and non-specific facts
  - Persons (suspects – convicted offenders – missing persons)
  - Organisations
  - Means of transportation
  - Objects
  - Numbers
  - Locations
  - Relations between different entities
  - Information on ongoing inquiries
- Phototheque: In addition to the ANG/ BNG, this application contains pictures of persons that are known in this database.



- CWR (Central Weapons' Register): This database holds information on:
  - Owners of firearms
  - Firearms they legally possess
  - Arms dealers
  - Certain documents, such as firearms licenses, firearms depository permits and European cards.
  - Shooting ranges

In addition, this database also makes information on firearms' seizures, restitutions after seizure, thefts, losses, destruction and confiscations available.

*Is this information always considered as non coercive according to your national law ?*

This information is considered non-coercive information.

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- DIV (National Vehicle Registration Authority): Vehicle Registration Data
- LDL: Information relating to driving licenses
- National Register: Administrative information on natural persons, identity cards and addresses.

NOTE: under *current* Belgian legislation, the actual national registration number can only be transferred internationally after prior judicial authorisation.

- SIDIS (National Criminal Record Information System): Personal data on current and former imprisoned persons and information (length, location, ...) on their imprisonment.

*Is this information always considered as non coercive according to your national law ?*

This information is considered non-coercive information.

**Information/databases accessible by law enforcement authorities but managed by private entities**

---

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

Access to information (including personal data) held by telecom operators (*i.e.* non-published information) requires prior judicial authorisation.

*Is this information always considered as non coercive according to your national law ?*

This information is not always considered non-coercive information.

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

From Belgium to another country:

- 1) French (most used)
- 2) English
- 3) Spanish (not outside office hours)
- 4) German (not outside office hours)
- 5) Dutch

**Replies to urgent requests can be provided in the following languages:**

From another country to Belgium:

- 1) French
- 2) English
- 3) Spanish (not outside office hours)
- 4) German (not outside office hours)
- 5) Dutch

Answers can be provided to urgent requests written in the following languages :

Within office hours

- 1) French
- 2) English
- 3) Spanish
- 4) German
- 5) Dutch

Outside office hours

- 1) French
- 2) English
- 3) Dutch

3. **PREFERRED CHANNEL**

## **BULGARIA**

1. **INFORMATION AVAILABLE**
2. **LANGUAGES USED IN CASE OF URGENCY**
3. **PREFERRED CHANNEL**

### 1. **INFORMATION AVAILABLE**

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- *identification of persons*
- *identification of vehicle owners and drivers*
- *drivers licence enquiries*
- *police records from police databases or files*
- *reports on crimes committed*
- *persons convicted of crime (criminal records)*
- *persons suspected of concrete crime*
- *persons suspected of criminal activities (criminal intelligence)*
- *decisions prohibiting entry to country or restraining orders*
- *wanted/missing persons*
- *photographs*
- *modus operandi*
- *stolen vehicles or stolen goods*
- *ascertaining individuals' whereabouts and place of residence*
- *firearms tracing*
- *fingerprints*
- *DNA*

***Is this information always considered as non coercive according to your national law ? Yes***

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- *administrative registers on persons (census)*
- *information from official records accessible to the public*
- *unusual or suspicious (money) transactions*
- *information about companies*
- *company board of directors, operations, share capital etc*
- *information, concerning prison inmates*

***Is this information always considered as non coercive according to your national law ? Yes***

**Information/databases accessible by law enforcement authorities but managed by private entities**

- *ascertaining the identity of telephone subscribers and subscribers to other telecommunications services, where publicly accessible*
- *information held by credit cards companies*

***Is this information always considered as non coercive according to your national law ? Yes***

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- *information held by banks*
- *documentation of search of premises, seizures, forfeited property or frozen assets*
- *documented questioning of suspects, witnesses, plaintiffs, experts etc.*
- *documentation of telephone tapping and video surveillance*
- *statements provided by under-cover agents*
- *questioning or other records of conversations with persons who co-operate with crime-fighting authorities*
- *compilations that contain appraised or non-appraised information on crime or criminal activities*

***Is this information always considered as non coercive according to your national law ?***

## 2. LANGUAGES USED IN CASE OF URGENCY

**The following languages will/can be used for sending a request in case of urgency:**

*Bulgarian ; English*

**Replies to urgent requests can be provided in the following languages:**

*Bulgarian ; English*

**Answers can be provided to urgent requests written in the following languages :**

*Bulgarian ; English*

## 3. PREFERRED CHANNEL

Police cooperation: The Republic of Bulgaria cannot use the Schengen channel for information exchange since the SIRENE bureau is not operational yet.

Urgent requests should be sent through the Interpol channel which operates 24/7.

Any other request could be sent through the Europol channel, if it falls within its mandate or through the Interpol channel.

Customs cooperation: Non urgent requests should be sent directly to the Customs through the Naples II Convention channel. Urgent requests should be sent through the Interpol channel.

## CZECH REPUBLIC

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

1. INFORMATION AVAILABLE

**Information/databases managed and directly accessible by law enforcement authorities:**

- Persons suspected of (concrete) crime
- Persons suspected of criminal activities (criminal intelligence)
- Wanted/Missing persons
- Photographs (on condition that photographs have been already collected)
- Fingerprints (non directly accessible by LEA)
- DNA (non directly accessible by LEA)
- Identification distinguishing marks or dental record (in same cases the record of the distinguishing marks or dental record could be obtain using coercive measures, non directly accessible by LEA)
- Modus operandi
- Others registers that describe crimes committed or types of crime
- Stolen vehicles or stolen goods
- Stolen works of art
- Database of firearms
- Film or video recordings
- Information concerning foreign nationals (permits residence, issuing visa etc.)
- Decisions prohibiting entry and staying in the Czech republic concerning foreign nationals
- Database of permit residence of the foreign persons
- Information system Check person or vehicles (suspicious person or vehicles on the unusual places)
- Reports (complaints) on crime committed
- Customs authorities' information on import and export of goods
- Documented questioning of suspect, witnesses, plaintiffs etc.

- Documentation of search of premises including search for communication data seizures, fortified property or frozen assets
- Documentation of crime scene investigations (non directly accessible by LEA)
- Documentation of medico-legal investigations (non directly accessible by LEA)

*Is this information always considered as non coercive according to your national law ?*

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Persons convicted of crime (criminal records)
- Decision prohibiting entry to premises or restraining orders
- Photographs
- Firearms tracing
- Driving licences
- Passports
- National identity cards
- Information (held by Prison Administration Services) concerning prison inmates
- Vehicle data and vehicle owner
- Data concerning aircraft and owner of aircraft
- Vessel data and owner of vessel or boat
- Administrative registers on persons
- Address and accommodation
- Ownership of real property
- Register of Companies
- Film or video recordings
- Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, e-mail or website subscriptions or addresses

*Is this information always considered as non coercive according to your national law ?*

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Identification (distinguishing marks or dental record)
- Firearms tracing



- Film or video recordings
- Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, e-mail or website subscriptions or addresses

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- Reports (complaints) on crime committed
- Documented interrogations of suspect, witnesses, plaintiffs, experts etc.
- Documentation of search of premises including search for communication data seizures, fortified property or frozen assets
- Documentation of crime scene investigations
- Documentation of medico-legal investigations

*Is this information always considered as non coercive according to your national law ?*

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

English, Czech

**Replies to urgent requests can be provided in the following languages:**

English, Czech

**Answers can be provided to urgent requests written in the following languages :**

English, Czech

**3. PREFERRED CHANNEL**

## DENMARK

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- *Information on persons convicted of crime (criminal records)*
- *Information on persons suspected of (concrete) crime*
- *Information on persons suspected of criminal activities (criminal intelligence)*
- *Decisions prohibiting entry to premises or restraining orders*
- *Information on wanted/missing persons*
- *Photographs of suspected/convicted persons etc.*
- *Fingerprints*
- *DNA*
- *Information on identification (distinguishing marks or dental records)*
- *Information on modus operandi*
- *Information on stolen vehicles or stolen goods*
- *Firearms tracing (IBIS)*
- *Information on firearms (permits etc.)*
- *Reports (complaints) on crimes committed*
- *Observations or observation reports*
- *Photographs, film or video recordings etc.*
- *Operational analyses*
- *Counterfeit travel documents, money etc.*

*Is this information always considered as non coercive according to your national law ?*

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- *Driving licence information*
- *Passport information*
- *Information (held by Prison and Probation Service) concerning prison inmates*
- *Decisions, permits etc. concerning foreign nationals*
- *Vehicle data and information on vehicle owner (cars)*
- *Data concerning aircraft and owner of aircraft*
- *Vessel data*
- *Customs authorities' information on import and export of goods*
- *Administrative registers on persons (census)*
- *Information on address and accommodation*
- *Information on company board of directors, operations, share capital etc.*
- *Information on ownership of real property*
- *Income and wealth information*
- *Registered debts such as taxes, maintenance, fines, debts to individual guarantors etc.*

*Is this information always considered as non coercive according to your national law ?*

**Information/databases accessible by law enforcement authorities but managed by private entities**

- *Information on holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex*

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- *Transport companies' passenger and freight lists*
- *Telecommunication traffic (communication data) stored and produced by telecommunication operators and Internet Service Providers*
- *Information held by banks, financial institutions and insurance companies on balances, transactions, holding of credit cards or insurance policies*
- *Information on unusual or suspicious (money) transactions*

*Is this information always considered as non coercive according to your national law ?*

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

Danish or English

**Replies to urgent requests can be provided in the following languages:**

*24/7-service: Danish and English.*

*During working hours (Monday to Friday 08:00 – 16:00): French, German and Spanish. English is preferred.*

**Answers can be provided to urgent requests written in the following languages :**

*Same as above. English is preferred.*

**3. PREFERRED CHANNEL**

## GERMANY

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- identification of persons
- police intelligence from police databases or files
- preparation of plans and coordination of search measures and the initiation of emergency searches
- tracing the origins of goods, particularly weapons
- issuing urgent alerts concerning arms and explosives and alerts concerning currency counterfeiting and securities fraud
- information on practical implementation of cross-border surveillance, cross-border hot pursuit and controlled deliveries
- persons convicted of crime (criminal records)
- persons suspected of crime
- persons suspected of criminal activities (criminal intelligence)
- decisions prohibiting entry to premises or restraining orders
- wanted / missing persons
- photographs of persons convicted or suspected of crime, missing persons, unidentified bodies, unknown helpless persons, crime scene traces and other objects
- fingerprints of persons convicted or suspected of crime, missing persons, unidentified bodies, unknown helpless persons as well as unidentified traces
- DNA profiles of persons convicted or suspected of crime, missing persons, unidentified bodies, unknown helpless persons as well as unidentified traces
- other registers that describe crimes committed or types of crime [ViCLAS]
- stolen vehicles or stolen goods
- information concerning prison inmates
- permits, fingerprints etc concerning foreign nationals
- unusual or suspicious money transactions

*Is this information always considered as non coercive according to your national law ?*

In principle yes.

*Comment: The purpose of the question seems not clear. If the requested information needed to be obtained by means of coercive measures, the framework decision is not be applicable (see Article 1 para. 5 Council Framework Decision 2006/960/JHA). As regards information that had previously been obtained by means of coercive measures, the Council Framework Decision 2006/960/JHA provides that Member States shall provide this kind of information or intelligence where permitted by and in accordance with their national law. This kind of information should therefore only be included in the above mentioned list, if the national law in principle allows for the provision of this kind of information under the Council Framework Decision 2006/960/JHA. Hence, it seems irrelevant for the purposes of this fact sheet whether the information in the above list has previously been obtained by means of coercive measures.*

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- drivers licence enquiries
- tracing whereabouts and residence
- identification of telecommunications subscribers
- identification of vehicle owners and drivers
- passports
- national identity cards

*Is this information always considered as non coercive according to your national law?*

In principle yes.

*See comment above.*

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Investigating the origin of German motor vehicles and the data of vessels registered in Germany.

*Is this information always considered as non coercive according to your national law ?*

In principle yes.

*See comment above.*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- ...

*Is this information always considered as non coercive according to your national law ?*

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

German and English in a 24/7-service by the Bundeskriminalamt (BKA) and Zollkriminalamt (ZKA).

Alternatively, regarding requests sent to the BKA: all Interpol working languages during office working hours (Monday 09:00 to 15:00, Tuesday to Thursday 08:30 to 15:00, Friday 08:30 to 14:30) and additional languages depending on capacities of the BKA translation service.

**Replies to urgent requests can be provided in the following languages:**

Same as above

**Answers can be provided to urgent requests written in the following languages:**

*The difference between this question and the question before is not clear.*

**3. PREFERRED CHANNEL**

## **ESTONIA**

1. **INFORMATION AVAILABLE**
2. **LANGUAGES USED IN CASE OF URGENCY**
3. **PREFERRED CHANNEL**

### 1. **INFORMATION AVAILABLE**

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- Persons suspected of criminal activities ( criminal intelligence)
- Wanted and missing persons
- DNA
- Fingerprints
- Photographs
- Criminal records
- Firearm licenses, firearm classification
- Stolen vehicles and stolen goods
- Reports on crimes committed
- Information gathered during criminal proceedings obtained by coercive measures  
(documentation of telephone tapping, house search etc.)
- Information of customs authorities
- Information of border guard
- Land register
- Information concerning imprisoned persons
- Company board of directors, operations, share capital etc, bankruptcy and reorganization proceedings.

#### ***Is this information always considered as non coercive according to your national law ?***

Yes. Certain restrictions may be provided by Estonian State Secrets and Classified Information of Foreign States Act in a context of forwarding intelligence information to a foreign state.



**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Population information - personal data: name, date of birth, gender etc, place of residence, passports and national identity cards
- Records of Citizenship and Migration Board ( passports and national identification cards, applications for passports and national identification cards, foreign passports, certificate of record of service on Estonian ships and its application data, seafarer's discharge book and its application data, residence permit data, working permit data, visa information, entry ban
- Driving licenses, data on vehicles and vehicle owners, traffic licenses
- Data on vessels and their owners
- Health fund information

***Is this information always considered as non coercive according to your national law ?***

Yes. Certain restrictions may be provided by Estonian State Secrets and Classified Information of Foreign States Act in a context of forwarding intelligence information to a foreign state.

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Credit information
- Information held by banks, financial institutions and insurance companies
- Passenger register (accommodation information)
- Passenger and freight lists of transport companies
- Holders of telephone, cell-phone, fax, e-mail or website address

***Is this information always considered as non coercive according to your national law ?***

Yes. Certain restrictions may be provided by Estonian State Secrets and Classified Information of Foreign States Act in a context of forwarding intelligence information to a foreign state.

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- Information obtained using coercive measures

***Is this information always considered as non coercive according to your national law ?***

2. **LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

Estonian, English

**Replies to urgent requests can be provided in the following languages:**

Estonian, English

**Answers can be provided to urgent requests written in the following languages :**

Estonian, English

3. **PREFERRED CHANNEL**

Interpol or Sirene

## GREECE

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases directly accessible by law enforcement authorities but managed by other authorities

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases accessible by law enforcement authorities but managed by private entities

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

## **2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

....

**Replies to urgent requests can be provided in the following languages:**

.....

**Answers can be provided to urgent requests written in the following languages :**

.....

## **3. PREFERRED CHANNEL**

## SPAIN

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases directly accessible by law enforcement authorities but managed by other authorities

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases accessible by law enforcement authorities but managed by private entities

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

## **2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

....

**Replies to urgent requests can be provided in the following languages:**

.....

**Answers can be provided to urgent requests written in the following languages :**

.....

## **3. PREFERRED CHANNEL**

## FRANCE

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### A. Informations disponibles dans le cadre d'une enquête administrative ou judiciaire française en cours ou close :

Toutes les informations sont disponibles et peuvent être transmises dans la mesure où elles correspondent à la finalité de la demande.

A noter que pour les enquêtes judiciaires en cours les informations ne peuvent être transmises qu'après autorisation du juge.

#### B. Informations disponibles hors des enquêtes administratives ou judiciaires françaises :

##### Information/databases managed and directly accessible by law enforcement authorities:

- Individus condamnés (fichier police)
  - Individus mis en cause dans le cadre d'une enquête pénale
  - Individus soupçonnés d'activité criminelle (renseignement pénal)
  - Interdictions de fréquenter certains lieux, et autres formes d'interdiction
  - Individus recherchés et disparus
  - Photographies
  - Empreintes digitales
  - ADN
  - Biens et les véhicules volés
  - Armes à feu (balistique/traçabilité)
  - Propriétaires de bateaux
  - Importations/exportation de biens (douanes)
  - Antécédents des personnes physiques et morales ayant fait l'objet d'une infraction douanière
- Etc....

*Is this information always considered as non coercive according to your national law ?*

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Permis de conduire
  - Passeports
  - Cartes nationales d'identité
  - Détenus
  - Véhicules et les propriétaires de véhicules
  - Propriétaires d'aéronefs
  - Armes à feu (identification du propriétaire)
  - Base de données européennes relatives aux antécédents des personnes physiques et morales ayant fait l'objet d'une infraction douanière.
  - Comptes bancaires détenus par les personnes physiques et morales.
- Etc....

*Is this information always considered as non coercive according to your national law ?*

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Conseils d'administration, les parts de capital des entreprises (etc....), lorsque ces informations détenues par des entités privées sont publiques
- Etc....

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

*Is this information always considered as non coercive according to your national law ?*



2. **LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

....

**Replies to urgent requests can be provided in the following languages:**

French, English

**Answers can be provided to urgent requests written in the following languages :**

French, English

3. **PREFERRED CHANNEL**

## **IRELAND**

1. **INFORMATION AVAILABLE**
2. **LANGUAGES USED IN CASE OF URGENCY**
3. **PREFERRED CHANNEL**

### 1. **INFORMATION AVAILABLE**

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- PULSE General Garda Information System
- All Revenue and Customs databases

*Is this information always considered as non coercive according to your national law ?*

Yes

#### **Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- National Vehicle File
- Companies Registration Office Database
- Social Welfare Database

*Is this information always considered as non coercive according to your national law ?*

Yes

#### **Information/databases accessible by law enforcement authorities but managed by private entities**

- Telecommunications Service Providers (call related data, email data)

*Is this information always considered as non coercive according to your national law ?*

No. Warrant issued pursuant to Interception of Postal Packets and Telecommunications Messages (Regulations) Act, 1993 by the Minister for Justice, Equality and Law Reform

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- N/A

*Is this information always considered as non coercive according to your national law ?*

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

English

**Replies to urgent requests can be provided in the following languages:**

English

**Answers can be provided to urgent requests written in the following languages :**

English

**3. PREFERRED CHANNEL**

- (i) For police cooperation: Interpol
  
- (ii) For customs cooperation: Naples II

## ITALY

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- Individuals checked during services by police forces
- Individuals subject of judicial measures or responsible for an administrative violation
- Individuals subject of measures issued in order to prevent the commission of crimes
- Third nationals subject of an expulsion order or ED citizens ordered to leave the national territory
- Individuals reporting crime and victim of crime
- Individuals owners of vehicles, documents, securities subject of crimes, lost or found
- Individuals holding, buying, selling or moving weapons on or from the national territory
- Individuals suspected of having committed crimes
- Individuals that must be traced on the national territory because subject of a judicial/administrative measure
- Individuals that must be traced following an alert from police forces
- Individuals that must be traced for various urgent communications
- Foreign individuals holding permit of stay
- Missing persons and individuals who reported the event
- Individuals holding a position within the contracting or sub-contracting firm
- Individual who are the subject of foreign arrest warrant
- Individuals banned from sporting events
- Spouse of individuals involved in crimes or administrative violation or subject of communications
- Persons found dead

- Transferor or transferee of buildings on the national territory
- Legal person
- Vehicle, licence plates stolen, lost, misappropriated or found. Searched because subject of judicial/administrative measures
- Documents, issued or blank, stolen, lost, misappropriated. Subject of judicial/administrative measures (for driving licence only)
- Weapons stolen, lost, misappropriated or found. Judicial/administrative measures for weapons operated on the national territory
- Securities stolen, lost, misappropriated or found
- Notes, stolen, lost, misappropriated or found
- Tenders called on the national territory for an amount equal or superior of € 100,000.00

*Is this information always considered as non coercive according to your national law ?*

Yes

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Public vehicle register
- National Institute for social security
- Tax register
- Jail information system
- State Printing Office and Mint database

*Is this information always considered as non coercive according to your national law ?*

Yes

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Mobile phones (now only Vodaphone and TIM)

*Is this information always considered as non coercive according to your national law ?*

No

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

## **2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

Italian and English

**Replies to urgent requests can be provided in the following languages:**

Italian and English

**Answers can be provided to urgent requests written in the following languages :**

Italian and English

## **3. PREFERRED CHANNEL**

## CYPRUS

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

**Note:** The categorization below provides an indication as to how information is obtained and/or released and by which authority. Ultimately, each request will be decided on a case-by case basis, that is, according to the facts and special circumstances of the case, if there are any (i.e confidentiality reasons). Nevertheless, no stricter rules will apply for the release of information to the law enforcement authorities of the Member States than those imposed to other national authorities.

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- Persons convicted of crime (criminal records)
- Persons suspected of (concrete) crime
- Persons suspected of criminal activities (criminal intelligence)
- Decisions prohibiting entry to premises or restraining orders
- Wanted/missing persons
- Photographs\*
- Fingerprints
- DNA (The DNA Personal Data Controller is the Cyprus Police but the Data Processor is the Cyprus Institute of Neurology & Genetics.)
- Modus operandi
- Other registers that describe crimes committed or types of crime
- Stolen vehicles or stolen goods
- Firearms tracing
- Reports (complaints) on crimes committed
- Firearms \*

- Decisions, permits, fingerprints etc concerning foreign nationals\*
- Customs authorities' information on import and export of goods
- Address and accommodation \*
- Film or video recordings \*
- Questioning or other records of conversations with persons who co-operate with crime-fighting authorities
- Statements provided by under-cover agents
- Other compilations that contain appraised or non-appraised information on crime or criminal activities
- Operational analyses
- Documented questioning of suspects, witnesses, plaintiffs, experts etc.
- Documentation of search of premises including search for communication data, seizures, forfeited property or frozen assets
- Documentation of crime scene investigations

*- Is this information always considered as non coercive according to your national law?*

*In most cases the above types of information could be obtained without the use of coercive measures (see note above).*

**Information/databases directly accessible by law enforcement authorities but managed by other authorities.**

- Photographs \*
- Driving licenses
- Passports
- National identity cards
- Firearms\*
- Information (held by Prison Administration Services) concerning prison inmates
- Decisions, permits, fingerprints etc concerning foreign nationals\*
- Vehicle data and vehicle owner (cars)
- Data concerning aircraft and owner of aircraft\*
- Vessel data and owner of vessel or boat\*
- Administrative registers on persons (census)
- Address and accommodation\*
- Company board of directors, operations, share capital etc



- Ownership of real property
- Income and wealth information
- Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, e-mail or website subscriptions or addresses\* (If information is publicly available)

***- Is this information always considered as non coercive according to your national law?***

*In respect to some types of information in the above category, Law Enforcement Authorities have direct electronic access. In order to obtain information which is not directly accessible by electronic means, the Law Enforcement Authorities may need to file an application to the other authority. In most cases such an application is not considered as coercive.*

**Information / databases accessible by law enforcement authorities but managed by private entities**

- Data concerning aircraft and owner of aircraft\*
- Vessel data and owner of vessel or boat\*
- Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, email or website subscriptions or addresses\* (If information is publicly available)

***- Is this information always considered as non coercive according to your national law?***

*A private entity may refuse to give access to a Law Enforcement Authority, to any of the information mentioned above. In such a case, coercive measures need to be taken, in order to collect the information.*

**Information / databases that always require a judicial authorization to be accessed by law enforcement authorities.**

- Identification (distinguishing marks or dental records)
- Transport companies' passenger and freight lists (The Custom and Excise Department has direct access to information in freight lists but not to information in passenger lists.)
- Registered debts such as taxes, maintenance, fines, debts to individual guarantors etc
- Film or video recordings\*
- Documentation of medico-legal investigations
- Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, email or website subscriptions or addresses (If information is not publicly available)

- Storage and production of telecom traffic (communication data) generated by various information technology systems and handled by telecom operators and Internet Service Providers.
- Unusual or suspicious (money) transactions
- Information held by banks, financial institutions and insurance companies on balances, transactions, holding of credit cards or insurance policies.

***- Is this information always considered as non coercive according to your national law?***

*No. In order to collect information from these databases, coercive measures need to be taken (e.g court order).*

**Additional comments concerning other types of information**

- Observations or observation reports: N/A
- Telecom monitoring : N/A
- Documentation of telephone tapping (including so-called surplus information)/  
Documentation of room bugging: N/A

**Note:** According to Article 17 of the Constitution of the Republic of Cyprus, interception of telecommunications or telephone tapping is not permitted, except only in very restricted circumstances, provided for by this Article and by the Protection of the Secrecy of Private Communications (Interception of Communications) Law of 1996 (L.92(I)/96). The interception permitted refers only to cases of convicted prisoners and/or of accused persons held in custody pending trial or where communication is conducted by unlawful means. Such interception may take place after a court order.

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

Greek, English

**Replies to urgent requests can be provided in the following languages:**

Greek, English

Answers can be provided to urgent requests written in the following languages :

Greek, English

### 3. PREFERRED CHANNEL

The channels and the way they are used in the Republic of Cyprus are as follows:

(i) for police cooperation: The Cyprus police cannot use the Schengen channel for information exchange since the Sirene bureau is not operational yet. Urgent requests should be sent through the Interpol channel which operates 24/7. Any other request could be sent through the Europol channel, if it falls within its mandate or through the Interpol channel.

(ii) for customs cooperation: Non urgent requests should be sent directly to the Customs and Excise Department through the Naples II Convention channel. Urgent requests should be sent through the Interpol channel because the Customs and Excise Department does not work 24/7.

(iii) for financial intelligence units' cooperation: Egmont Secure Web channel is used and FIU .Net channel will also be soon available for the FIU of Cyprus (MOKAS). Urgent requests should be sent through the Interpol channel.

## LATVIA

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### **General comment:**

In addition to information provided below, the following type of information/data bases are managed by law enforcement authorities, but are not directly accessible:

- a) national AFIS (Automated fingerprints identification system);
- b) national DNA data base;
- c) Electronic Criminal police intelligence information system.

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- the information system of the State police “Electronic Journal of Events” (records of every offence, including criminal offences and administrative violations, committed in the territory of whole state, and other cases within the competence of the State police (e.g., discovered unidentified bodies, detection of explosive items etc.). Available to all law enforcement authorities);
- Register of traffic regulations violations;
- Centralised customs information system (cargo declarations data base);
- State Revenue service data storage system (a number of interlinked data bases on specific issues, e.g., tax payers (VAT, real estate tax etc.), state officials annual income declarations, Customs auditing reports etc.);
- State Border guard register on border crossings;

#### ***Is this information always considered as non coercive according to your national law ?***

Information/data from above mentioned data bases usually is considered as non-coercive.

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

Integrated Information system, run and managed by the Information Centre of the Ministry of the Interior (which is not considered as a law enforcement authority). Consists of following data bases:

- “Wanted persons”;
  - “Register for invalid documents”;
  - “Register for dismissed criminal cases”;
  - “Wanted vehicles”;
  - “Contingent” (profiles of persons that have committed serious criminal offences, or are known as violent, drug users etc.);
  - “Wanted objects”;
  - “Register of firearms”;
  - “Register of criminal offences” (statistic data on committed crimes);
  - “Photo archive”;
  - “Persons, who have committed crimes”;
  - “Register of samples of documents”.
- 
- Register of citizens and residents;
  - Passport information system;
  - Visa and invitation register;
  - Permanent residence permit register;
  - Vehicles and driver`s licence register;
  - Register of heavy equipment, construction and agricultural machinery;
  - Real estate register;
  - Criminal records

***Is this information always considered as non coercive according to your national law ?***

Information/data from above mentioned data bases usually is considered as non-coercive.

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Commercial register (all companies, associations and enterprises, as well as foreign representations that are registered in Latvia);
- Phone subscribers (data bases of private entities on registered subscribers of landline, cell-phone, fax numbers);
- data on e-mail or website subscribers and other relevant information;

*Is this information always considered as non coercive according to your national law ?*

Information/data from above mentioned data bases usually is considered as non-coercive.

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- unusual or suspicious money transactions;
- information held by banks, financial institutions on bank accounts, transactions, holders of credit cards etc.
- documented questioning of suspects, witnesses, experts etc. within criminal case;
- documentation of search of premises, including search for communication data, seizures, forfeited property or frozen assets;
- documentation of phone tapping, room bugging, covert surveillance operations

*Is this information always considered as non coercive according to your national law ?*

Such information can be transmitted with permission (authorisation) of competent judicial authority.

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

ENGLISH

**Replies to urgent requests can be provided in the following languages:**

ENGLISH

**Answers can be provided to urgent requests written in the following languages :**

ENGLISH

**3. PREFERRED CHANNEL**

## LITHUANIA

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### **General comments:**

The primary investigation (*law enforcement*) authority in Lithuania is Police, but the same investigation powers have also Customs, State Border Guard Service, Finance Crime Investigation Service and other authorities.

According to the national legislation there are two types of investigations. First type of investigation is implemented according to the Law on Operational Activities (operational investigation). Another type of investigation is carried out according to the Criminal Procedure Code of the Republic of Lithuania (pre-trial investigation). All pre-trial investigation, according to the Lithuanian law, is under direction and supervision of Prosecutor Office of the Republic of Lithuania). The above mentioned difference between 2 types of investigation has impact on rules for the providing of information to requesting Member States when requested information is related to the national investigation.

In case of the operational investigation, it is usually police (or other law enforcement institutions) that decide which data can be provided to the authorities of the requesting countries.

In case of pre-trial investigation, providing of information to the requesting Member State requires authorization of Prosecutor Office of the Republic of Lithuania.

Information that is not yet gathered in the course of pre-trial or operational investigation as well as in databases of police could be obtained and transferred to the competent authority of the requesting state only via mutual assistance.

Defined rules for the exchange of information with foreign countries:

1. If intelligence information is received by operative actions, which require authorization of the judicial authority, this intelligence could be exchanged only with the consent of judicial authority, which authorized that action.



2. If the requested information is data of the pre-trial investigation, this information can be exchanged with the consent of prosecutor (part 1 of article 177 of the Criminal Procedure Code of the Republic of Lithuania).
3. If the requested information is from criminal case, which is passed to the court, this information can be exchanged with the consent of the judge.
4. If the requested information about private life has been obtained by coercive measures, it can be used in another case only with the consent of the pre-trial investigation judge or a court (article 162 of the Criminal Procedure Code of the Republic of Lithuania).

**Information/databases managed and directly accessible by law enforcement authorities:**

- Wanted persons register (information about missing persons, wanted suspects for criminal acts, wanted accused of criminal acts, wanted convicted persons, wanted with a view of extradition, debtors for child maintenance, wanted debtors pursuant to civil procedure; wanted avoiding administrative liability; witnesses summoned to appear before the judicial authorities, discreet surveillance, specific check);
- Register of suspected, accused and convicted persons (persons convicted of crime (criminal records), persons suspected or accused of (concrete) crime);
- Register of preventive measures (official warnings or Court Injunctions imposed by court according to Law on organized crime prevention);
- Register of events registered by police;
- Register of criminal activities;
- Criminal intelligence (persons suspected of criminal activities);
- Register of traffic regulation violation;
- Register of wanted motor vehicles;
- Register of wanted weapons;
- Register of wanted numeric objects;
- Database of external border crossing;
- Database of fingerprints;
- DNA database;
- Register of undesirable persons;
- National Cases Management and Intelligent system (NCMIS);
- Customs declaration data bases (MISC DB).

**Is this information always considered as non coercive according to your national law?**

Usually these kinds of information are not considered as coercive.

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Register of residents of Lithuania (personal data, place of residence, previous place of residence, photographs, issued passports and identity cards);
- Register of motor vehicles (vehicle data and vehicle owner);
- Register of driving licenses;
- Register of weapons existing in civil circulation;
- Social insurance database;
- Register of immovable property;
- Register of juridical person's.

**Is this information always considered as non coercive according to your national law?**

Usually these kinds of information are not considered as coercive.

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Database of telephone subscribers;
- Transport companies' passenger and freight lists;
- Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, e-mail or website subscriptions or addresses;
- Unusual or suspicious (money) transactions.

**Is this information always considered as non coercive according to your national law?**

Usually these kinds of information are not considered as coercive.

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- Storage and production of telecom traffic (communication data) generated by various information technology systems and handled by telecom operators and Internet Service Providers;

- Information held by banks, financial institutions and insurance companies on balances, transactions, holding of credit cards or insurance policies.
- Modus operandi if the requested information is data of the pre-trial investigation or criminal case;
- Documented questioning of suspects, witnesses, plaintiffs, experts, etc.;
- Documentation of search of premises including search for communication data, seizures, forfeited property or frozen assets;
- Documentation of telephone tapping;
- Documentation of room bugging;
- Documentation of crime scene investigations;
- Documentation of medico-legal investigations.

**Is this information always considered as non coercive according to your national law?**

If information is already obtained and accessible it can be transmitted with permission of judicial authorization and it is not considered as coercive. In case information is not collected it is considered as coercive and can be obtained only via mutual assistance.

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

English

**Replies to urgent requests can be provided in the following languages:**

English

**Answers can be provided to urgent requests written in the following languages :**

English

3. **PREFERRED CHANNEL**

Flexible choice of the channels for the information exchange.

- SIS-NET
- EUROPOL
- INTERPOL
- Bilateral cooperation channels
- Mutual administrative international customs assistance (“Naples II Convention)

## LUXEMBOURG

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

The Luxembourg competent law enforcement authorities within the meaning of article 2 (a) of Framework Decision 2006/960 (see doc. 11314/08 of 1 July 2008 CRIMORG 103) are managing or may have direct access to the following information:

- persons wanted by the Luxembourg or foreign judicial authorities;
- persons concerned by an administrative decision the violation thereof is a criminal offence;
- persons having been refused to enter or to stay in Luxembourg;
- wanted / missing persons;
- information concerning prison inmates;
- all persons for which a police record exists;
- victims and witnesses of criminal offences;
- persons being especially protected;
- photographs and fingerprints of persons convicted or suspected of crime, missing persons, unidentified bodies, unknown helpless persons, crime scene traces and other objects;
- DNA profiles of persons convicted or suspected of crime, missing persons, unidentified bodies, as well as unidentified traces;
- stolen vehicles or stolen goods;
- all persons for which a criminal drug offence record exists.

#### *Is this information always considered as non coercive according to your national law ?*

In principle yes, but if the requested information need to be obtained by means of coercive measures, Framework Decision 2006/960/JHA is anyway not applicable. As regards information that had previously been obtained by means of coercive measures or which is part of an ongoing

investigation, the Luxembourg competent law enforcement authorities can exchange the concerned information only with the authorisation of the competent magistrate (i.e. Prosecutor or investigating judge), in accordance with Luxembourg national law. Hence, it seems irrelevant for the purposes of this fact sheet whether the information in the above list has previously been obtained by means of coercive measures.

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

The Luxembourg competent law enforcement authorities have direct access to the following databases managed by other authorities:

- general register of Luxembourg residents;
- general social security register (companies, employers and employees);
- register of aliens;
- register of asylum seekers;
- register of visa requests;
- register of commercial and business authorisations;
- register of driving licences;
- vehicle register;
- register of persons and companies subjected to VAT;
- firearms register;
- register of anonymised national mobile telephone numbers regarding provider assignment.

*Is this information always considered as non coercive according to your national law ?*

See comment above.

These databases are directly accessible accordingly to the conditions of the Luxembourg law.

**Information/databases accessible by law enforcement authorities but managed by private entities**

The Luxembourg competent law enforcement authorities have direct access to the following databases managed by private entities:

- Public Register of Businesses and Companies;
- Database of domestic telephone companies in case of emergency calls

*Is this information always considered as non coercive according to your national law ?*

Yes.

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

There is no database the access thereof by the Luxembourg competent law enforcement authorities is always submitted to a judicial authorisation, but the access may require the authorisation of a judicial authority, depending on the procedural stage and the factual situation of a given case.

*Is this information always considered as non coercive according to your national law ?*

See comment above.

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

- French;
- German;
- English.

**Replies to urgent requests can be provided in the following languages:**

- French;
- German;
- English.

**Answers can be provided to urgent requests written in the following languages :**

- French;
- German;
- English.

**3. PREFERRED CHANNEL**

- INTERPOL NCB
- SIRENE
- ENU/EUROPOL Liaison Officer
- Mutual administrative international customs assistance ("Naples II Convention")



## HUNGARY

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- information on wanted persons (HERMON)
- border-control and registration system (HERR)

*Is this information always considered as non coercive according to your national law ?*

Yes

#### Information/databases directly accessible by law enforcement authorities but managed by other authorities

- database of persons convicted of crime (criminal records) and of final court judgements (“A”)
- modus operandi database (“B”)
- database of persons accused of crime (“E”)
- database of foreigners under coercive immigration measures (“J”)
- database of persons under coercive measures (“K”)
- database of persons under the prohibition of leaving the country (“N”)
- DNA database (“S”)
- database of persons with residence permit (“T”)
- database of persons under the prohibition of stay in and entry into Hungary and persons registered for other immigration purposes (“R”)
- register of lost documents of foreign persons (“U”)
- Schengen Information System (SIS)
- vehicle registration database
- driving licence register
- passport register

- register of personal data and place of domicile
- I.D. card register

*Is this information always considered as non coercive according to your national law ?*

Yes

**Information/databases accessible by law enforcement authorities but managed by private entities**

- databases handled by telecommunication providers
- databases handled by financial organisations (banks)

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- access to data handled by the tax authority
- access to data handled by healthcare and connected institutions
- access to data classified as business secret
- in other cases, as a general rule, a judicial authorisation is not necessary to the access by law enforcement authorities, except in special cases of international legal assistance where prosecutor's authorisation is required
- other than that the right to access can be limited by the degree of the access right and the purpose of requesting data

*Is this information always considered as non coercive according to your national law ?*

Yes

## 2. LANGUAGES USED IN CASE OF URGENCY

**The following languages will/can be used for sending a request in case of urgency:**

*Hungarian and English* in the 24/7 service

Alternatively, regarding requests sent to the Hungarian Prosecutors Office during office working hours additional languages are available depending on capacities:

*French, German, Russian.*

**Replies to urgent requests can be provided in the following languages:**

*Hungarian and English* in the 24/7 service

Alternatively, regarding requests sent to the Hungarian Prosecutors Office during office working hours additional languages are available depending on capacities:

*French, German, Russian.*

**Answers can be provided to urgent requests written in the following languages :**

*Hungarian and English* in the 24/7 service

Alternatively, regarding requests sent to the Hungarian Prosecutors Office during office working hours additional languages are available depending on capacities:

*French, German, Russian.*

## 3. PREFERRED CHANNEL

Bilateral cooperation channels, Interpol, EJN.

## MALTA

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases directly accessible by law enforcement authorities but managed by other authorities

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases accessible by law enforcement authorities but managed by private entities

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

## **2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

....

**Replies to urgent requests can be provided in the following languages:**

.....

**Answers can be provided to urgent requests written in the following languages :**

.....

## **3. PREFERRED CHANNEL**

## NETHERLANDS

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE<sup>1</sup>

#### Information/databases managed and directly accessible by law enforcement authorities:

1. Basic Enforcement Database (BED)
  - a. persons suspect of criminal offence/punishable act
  - b. persons regarded as public order violators (location bans)
  - c. missing persons (incl. dental records)
  - d. reports on crime committed
2. Basic Investigation Database (BID)
  - a. fugitive convicted persons
  - b. fugitive suspected and accused persons
  - c. stolen goods - vehicles
3. National Schengen Info system
  - a. fugitive convicted and suspected persons
  - b. missing persons
  - c. stolen vehicles – goods
  - d. stolen/lost driving licences
  - e. stolen/lost passports – id-cards
  - f. stolen/lost firearms
4. Database Current Investigations (provisional)
5. Missing Persons database
6. Photo Confrontation Module (pictures related to BED)
7. Fingerprint database (under revision)
8. Fingerprints of missing persons and mortal remains
9. Modus operandi database Murder/Rape
10. Modus operandi database Armed Robbery
11. Analysis System Other types of crime
12. Permit holders legal firearms
13. Shooting incidents and tracings (IBIS)
14. Documentation of crime scene investigation (instrument traces)

***Is this information always considered as non coercive according to your national law ?***

*This information is considered non-coercive under national law.*

---

- <sup>1</sup> *The appearance of a database or data on this list does not automatically imply its (future) availability for LEAs in other Member States.*

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

1. Stadium bans (Nat. Football organisation- KNVB)
2. Vehicle registration data (Nat. Vehicle and Driving Licence Registration Authority - RDW)
  - a. stolen/lost vehicles
  - b. licence – ownership
  - c. vehicle insurance data
3. Driving licence registration data (Nat. Vehicle and Driving Licence Registration Authority – RDW)
  - a. driving licences
  - b. persons
  - c. stolen/lost driving licences
4. Valid and invalid issues travel document (Municipal Basic Administration)
5. Travel documents excluded from public traffic (Cf. I.3.e.) (MBA)
6. Undesirable foreign nationals (Immigration Service – IND)
7. Aircraft Register (Inspectorate Transport and Public Works)
8. Vessel Information System (Ministry Transport and Public Works)
9. Ships mortgage Register (vessel owner; pleasure and professional craft)
10. Municipal Population Register (personal data) – National Reference
11. Trade Register (names; addresses of companies and institutes) (Chamber of Commerce)
12. Land Register (Real property ownership)
13. Mortgages Register
14. Users of telephone and fax numbers; owners of website (Central Information Point CIOT)
15. Suspicious and unusual financial transactions (database FIU/KLPD)

***Is this information always considered as non coercive according to your national law ?***

*This information is considered non-coercive under national law.*

**Information/databases accessible by law enforcement authorities but managed by private entities**

1. Register Advanced Passenger Information (Airline companies) – N.B. direct access by border police only.

***Is this information always considered as non coercive according to your national law ?***

*This information is considered non-coercive under national law.*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

1. Judicial Documentation System
  - a. persons accused and/or convicted of punishable act
  - b. decisions on persons regarding street bans
2. Reference Index Prison inmates (VIP)
  - a. persons accused and/or convicted of punishable act currently in custody
3. Photographs from existing databases/registers
4. Photograph to be taken
5. Fingerprints in new passport
6. Fingerprints of foreign nationals (Immigration Service - IND) – subset of I.8
7. Status of foreign nationals - (Immigration Service - IND)
8. DNA-profiles (Netherlands Forensic Institute)
9. Register Advanced Passenger Information (Airline companies)
10. Flight Reservation Information
11. Aircraft Cargo Information
12. Income and capital (Tax authorities – FIOD)
13. Central Registration of debts and fines (BKR)
14. Reports, analyses and intelligence concerning criminal investigations
15. Registration of telephone and internet traffic
16. Bank particulars, transactions, account holders, insurance policies
17. Suspicious and unusual financial transactions (database FIU/KLPD)
18. Criminal Intelligence Register (soft data)

***Is this information always considered as non coercive according to your national law ?***

*This information is always obtained via coercive means.*

**2. LANGUAGES USED IN CASE OF URGENCY**

**Sending a request in case of urgency:**

For Europol and Sirene channels: *English*

For the Interpol channel: *English - German - French - Spanish*

N.B. On all occasions the *Dutch* language can be used (although formally this is not a language to be used as agreed upon in the handbooks for these three channels).

**Replies to urgent requests can be provided in the following languages:**

For all channels: *English*

N.B. In case the request is *received in Dutch* the answer may be provided in the Dutch language as well.



**Answers can be provided to urgent requests written in the following languages :**

For all channels: *English*

For Interpol: Also in *German, French or Spanish* only during office hours from 08:00 hrs till 17:00 hrs on Monday till Friday. Translation can be provided on a case by case basis (in accordance with the language used in the original request), depending on the availability of the translators in the translation department.

N.B. In case the request is received in the Dutch language the answer can/will be provided in the Dutch language as well (e.g. a request received from Belgium).

### **3. PREFERRED CHANNEL**

*No preference channel (flexible approach).*

Principle is that after the initial choice, subsequent exchanges of information on the same matter/case will be *continued using the same channel*.

In case of urgent necessity, it may be possible to deviate from this principle in agreement with the other country involved.

## AUSTRIA

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

(The following information is available in the Austrian Information system (EKIS):

- Wanted and missing persons (e.g. arrest warrants, information about covert surveillance, where about for police, courts and public prosecutors);
- Fingerprints , photographs and DNA of persons suspected or convicted of crime;
- Lost and stolen objects (e.g. stolen vehicles, documents, firearms; in principle all objects with a number can be inserted in this database);
- Information extracted from the criminal record and crimes reported to the competent judicial authorities (e.g. report about a crime that was committed by a person)
- Information about vehicles, issued documents, firearms and the residence of a person (e.g. information about the owner of a vehicle, id-document or firearm);
- Visa and residence permits on foreign nationals.

### Information/databases managed and directly accessible by law enforcement authorities:

- Wanted Persons and Objects
- Criminal records index
- Vehicle registration database
- Register for documents
- Database for firearms
- Fingerprints and Photographs
- Personal register (residence of a person)
- Stolen arts
- Register for foreign citizens

*Is this information always considered as non coercive according to your national law?*

Yes. This information is necessary for the work of the law enforcement authorities. There exists a legal basis in the national law.

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Central DB for Social security
- Information concerning prison inmates
- Ownership of real property

*Is this information always considered as non coercive according to your national law?*

---

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Database of telephone subscribers;
- Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, e-mail or website subscriptions or addresses

*Is this information always considered as non coercive according to your national law?*

---

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- Information on bank accounts and banking transactions;
- Information obtained following a search and seizure;
- Information obtained as a result of a telephone taping;
- Information obtained as a result of a bodily examination or a molecular genetic examination;
- Information obtained as a result if an IT-supported comparison of data;
- Data and results of an investigation that have been obtained in the course of national criminal proceedings without the use of coercive measures.

*Is this information always considered as non coercive according to your national law?*

The above-mentioned information (except the information mentioned in the last indent) is in general considered as coercive according to our national law.

## 2. LANGUAGES USED IN CASE OF URGENCY

**The following languages will/can be used for sending a request in case of urgency:**

German / English / French

**Replies to urgent requests can be provided in the following languages:**

German / English / French

**Answers can be provided to urgent requests written in the following languages :**

German / English / French

## 3. PREFERRED CHANNEL

## POLAND

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- persons suspected of (concrete) crime
- persons suspected of criminal activities (criminal intelligence)
- wanted/missing persons
- unidentified persons
- photographs
- fingerprints
- DNA
- persons subjected to police control
- stolen vehicle
- stolen property or documents
- modus operandi
- driving bans
- traffic offenders
- lost firearms, issued firearms licenses, licenses issued to private security companies
- mass events (in particular sport events)
- traffic accidents and collisions (offenders, victims, vehicles)
- persons and vehicles which cross the border of Poland

*Is this information always considered as non coercive according to your national law ?*

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- administrative registers on persons
- registered vehicles, vehicle owners, issued driving licenses
- persons detained
- persons arrested
- foreign nationals (residence permits, visas, refusal of stay, expulsion from the territory of Poland, etc.)
- business entities, associations, foundations, social and professional organizations, public healthcare institutions

*Is this information always considered as non coercive according to your national law ?*

**Information/databases accessible by law enforcement authorities but managed by private entities**

- telecommunications data (for example phones, faxes, mobile phones, IT telecommunications equipment, routing equipment)
- postal data
- debts (the consumer financial obligations which are recorded by banks, other financial institutions, insurance companies, telecommunication companies etc.)

*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- bank data
- insurance data
- financial data
- control of content of correspondence, communication and deliveries
- controlled purchase, sale or seizure of material goods (secret supervision of manufacturing, transport, warehousing and circulation of items resulting from crime)

*Is this information always considered as non coercive according to your national law ?*

2. **LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

English, Polish

**Replies to urgent requests can be provided in the following languages:**

English, Polish

**Answers can be provided to urgent requests written in the following languages :**

English, Polish

3. **PREFERRED CHANNEL**

INTERPOL

## PORTUGAL

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases directly accessible by law enforcement authorities but managed by other authorities

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases accessible by law enforcement authorities but managed by private entities

- ...
- ...
- ...



*Is this information always considered as non coercive according to your national law ?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

....

**Replies to urgent requests can be provided in the following languages:**

.....

**Answers can be provided to urgent requests written in the following languages :**

.....

**3. PREFERRED CHANNEL**

## **ROMANIA**

1. **INFORMATION AVAILABLE**
2. **LANGUAGES USED IN CASE OF URGENCY**
3. **PREFERRED CHANNEL**

### 1. **INFORMATION AVAILABLE**

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- Wanted Database: national and international wanted persons;
- Auto Theft Database: auto thefts and registration plates;
- Interdit Database: persons not allowed to leave their city or the country and persons not allowed to travel to certain cities;
- Objects Database: stolen and lost goods;
- Incarcerated Database: arrested persons;
- “Banking Fraud” Database: persons suspected for or committed offences in the banking system;
- DNA Database: judicial genetic data and personal data;
- Fingerprint Database: digital fingerprints;
- I.B.I.S. Database: ammunition information;
- IMAGETRAK Database: digital facial recognition;
- C.D.N. Database: photographs and information on persons missing under suspicious circumstances, unknown persons and bodies;
- Romanian Police System Of Intelligence Reports Database: the system is an integrated part of the Romanian Police intelligence analysis system and ensures, on one hand, the national integration with i2 system which already exists in Romanian Police, and on the other hand, the functions for transfer, collation and storage of criminal data and information;
- Protect Database: information on specialised private security companies, companies specialised in alarm systems, administrators of these companies, officially certificated security personnel;
- National Arms Registry Database: complex information on weapons, weapon holders and operations with weapons and ammunition;

- Explosives Database: authorisations for the transfer and transit of explosives;
- Road Accidents Database;
- Criminal Records.

*Is this information always considered as non coercive according to your national law ?*

The meaning of expression « **non coercive** » is not clear, in this context.

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Driving licences;
- National identity cards;
- Vehicle data and vehicle owner;
- Trade companies/legal persons register;
- Customs databases;
- Population National Registry;
- National passports databases;
- Intellectual property rights;
- Border entries and exits;
- Information on Aliens;
- Interpol eASF database;
- Europol IS database;

*Is this information always considered as non coercive according to your national law ?*

The meaning of expression « **non coercive** » is not clear, in this context.

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Internet services providers
- phone services provider

*\* only with judicial (prosecutor ) authorities approval*

*Is this information always considered as non coercive according to your national law ?*

N/A

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- ...
- ...
- ...

*Is this information always considered as non coercive according to your national law ?*

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

- Romanian
- English

**Replies to urgent requests can be provided in the following languages:**

- Romanian
- English

**Answers can be provided to urgent requests written in the following languages :**

- Romanian
- English

**3. PREFERRED CHANNEL**

## SLOVENIA

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

Information according doc. 5815/3/05	Coercive Y/N
Persons suspected of (concrete) crime	N
Persons suspected of criminal activities (criminal intelligence)	N
Decisions prohibiting entry to premises or restraining orders	N
Wanted/missing persons	N
Photographs	N
Fingerprints	N
DNA	N
Modus operandi	N
Other registers that describe crimes committed or types of crime	N
Stolen vehicles or stolen goods	N
Reports (complaints) on crimes committed	N
Customs authorities' information on import and export of goods	N
Observations or observation reports	N
Photographs	N
Film or video recordings	N
Questioning or other records of conversations with persons who co-operate with crime-fighting authorities	N
Statements provided by under-cover agents	N
Other compilations that contain appraised or non-appraised information on crime or criminal activities	N
Operational analyses	N
Documented questioning of suspects, witnesses, plaintiffs, experts etc.	N
Documentation of search of premises including search for communication data, seizures, forfeited property or frozen assets	N
Documentation of telephone tapping (including so-called surplus information)	N <sup>1</sup>
Documentation of room bugging	N
Documentation of crime scene investigations	N
Documentation of medico-legal investigations	N

<sup>1</sup> Measures like telephone tapping and room bugging are carried out only by the decision of judicial authorities. While executing these measures, the police can access to documentation autonomously. After the execution of measures has been completed, the permission of judicial authorities is needed for access to documentation.

*Is this information always considered as non coercive according to your national law ?*

See table.

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

Information according doc. 5815/3/05	Coercive Y/N
Firearms tracing	N
Driving licences	N
Passports	N
National identity cards	N
Information (held by Prison Administration Services) concerning prison inmates.	N
Decisions, permits, fingerprints etc concerning foreign nationals.	N
Vehicle data and vehicle owner (cars)	N
Data concerning aircraft and owner of aircraft	N
Vessel data and owner of vessel or boat	N
Administrative registers on persons (census)	N
Address and accommodation	N
Ownership of real property	N
Income and wealth information	N
Registered debts such as taxes, maintenance, fines, debts to individual guarantors etc.	N
Persons convicted of crime (criminal records)	N

*Is this information always considered as non coercive according to your national law ?*

See table.

**Information/databases accessible by law enforcement authorities but managed by private entities**

Information according doc. 5815/3/05	Coercive Y/N
Company board of directors, operations, share capital etc.	N
Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, e-mail or website subscriptions or addresses.	N
Identification (distinguishing marks or dental records)	Y
Transport companies' passenger and freight lists.	Y

*Is this information always considered as non coercive according to your national law ?*

See table.

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

Information according doc. 5815/3/05	Coercive Y/N
Telecom monitoring	Y
Storage and production of telecom traffic (communication data) generated by various information technology systems and handled by telecom operators and Internet Service Providers.	Y
Unusual or suspicious (money) transactions	Y
Information held by banks, financial institutions and insurance companies on balances, transactions, holding of credit cards or insurance policies.	Y

*Is this information always considered as non coercive according to your national law ?*

See table.

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

English, Slovenian

**Replies to urgent requests can be provided in the following languages:**

English, Slovenian

**Answers can be provided to urgent requests written in the following languages :**

English, Slovenian

**3. PREFERRED CHANNEL**

## **SLOVAKIA**

1. **INFORMATION AVAILABLE**
2. **LANGUAGES USED IN CASE OF URGENCY**
3. **PREFERRED CHANNEL**

### 1. **INFORMATION AVAILABLE**

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- Persons suspected of (concrete) crime (four databases/ 2 of them not directly accessible by SPOC)
- Persons suspected of criminal activities (criminal intelligence) (not directly accessible by SPOC – classified information)
- Wanted/missing persons including identification (distinguishing marks or dental records)
- Fingerprints
- DNA (not directly accessible by SPOC)
- Modus operandi (not directly accessible by SPOC – classified information)
- Stolen vehicles or stolen goods
- Driving licences
- Passports
- National identity cards
- Firearms
  - Decisions, permits, fingerprints etc concerning foreign nationals. (not directly accessible by SPOC)
- Vehicle data and vehicle owner (cars)
- Administrative registers on persons
- Address and accommodation
- Unusual or suspicious (money) transactions (not directly accessible by SPOC, preferred channel – FIU-net)

***Is this information always considered as non coercive according to your national law ? YES***



**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Persons convicted of crime (not directly accessible by SPOC<sup>1</sup> yet)
  - Information (held by Prison Administration Services) concerning prison inmates (accessible only during working hours)
- Company board of directors, operations, share capital etc
- Ownership of real property

*Is this information always considered as non coercive according to your national law? YES*

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Holders of telephone and cell-phone  
Only on written request and during working hours:
- Data concerning aircraft and owner of aircraft
- Vessel data and owner of vessel or boat

*Is this information always considered as non coercive according to your national law? YES*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- Information held by banks, financial institutions and insurance companies on balances, transactions, holding of credit cards or insurance policies (preferred channel – FIU-net)
- Telecom monitoring
  - Storage and production of telecom traffic (communication data) generated by various information technology systems and handled by telecom operators and Internet Service Providers.
  - Observations or observation reports,
  - film or video recordings,
  - questioning or other records of conversations with persons who co-operate with crime-fighting authorities,
  - statements provided by under-cover agents,
  - other compilations that contain appraised or non-appraised information on crime or criminal activities,
  - documented questioning of suspects, witnesses, plaintiffs, experts etc.,

- documentation of search of premises including search for communication data, seizures, forfeited property or frozen assets,
- documentation of telephone tapping (including so-called surplus information),
- documentation of room bugging,
- documentation of crime scene investigations,

*Is this information always considered as non coercive according to your national law? NO*

## **2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

English

**Replies to urgent requests can be provided in the following languages:**

English

**Answers can be provided to urgent requests written in the following languages :**

English

## **3. PREFERRED CHANNEL**

---

<sup>1</sup> SPOC = Single Point of Contact for FWD 960/2006

## **FINLAND**

1. **INFORMATION AVAILABLE**
2. **LANGUAGES USED IN CASE OF URGENCY**
3. **PREFERRED CHANNEL**

### 1. **INFORMATION AVAILABLE**

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- persons suspected of criminal activities (criminal intelligence)
- DNA
- fingerprints
- photographs
- passports and national identity cards, including lost foreign passports
- firearm licenses, firearm classification
- identification information (distinguishing marks)
- wanted/missing persons
- stolen vehicles or stolen goods
- reports (complaints) on crimes committed
- documentation of telephone tapping or room bugging (previously obtained by coercive measures)
- information held by customs authorities
- border guard's information system

*Is this information always considered as non coercive according to your national law ?*

Yes

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- population information system (basic information related to the identification of people, buildings and real estate)
- visa information
- decisions, permits, fingerprints etc. concerning foreign nationals
- driving licenses, vehicle data and vehicle owner, traffic licenses
- vessel data and owner of vessel or boat
- income and wealth information (tax information)
- trade register (company board of directors, operations, share capital etc.)
- information concerning prison inmates
- persons suspected of (concrete) crime
- decisions prohibiting entry to premises or restraining orders
- holders of telephone, cell-phone, fax, e-mail or website addresses
- register of debt regulations (public register with only limited direct access)
- register of bankruptcy and reorganization proceedings (public register with only limited direct access)
- business prohibition register (public register with only limited direct access)

*Is this information always considered as non coercive according to your national law ?*

Yes

**Information/databases accessible by law enforcement authorities but managed by private entities**

- transport companies' passenger and freight lists
- passenger register (accommodation information)
- credit information
- information held by banks, financial institutions and insurance companies

*Is this information always considered as non coercive according to your national law ?*

Yes

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- criminal records

*Is this information always considered as non coercive according to your national law ?*

Yes

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

Finnish, Swedish, English

**Replies to urgent requests can be provided in the following languages:**

Finnish, Swedish, English

**Answers can be provided to urgent requests written in the following languages :**

Finnish, Swedish, English

**3. PREFERRED CHANNEL**

## SWEDEN

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

The Swedish answer to the questionnaire about the availability of information, as provided in document 5815/3/05, is still valid. In addition, room bugging is now allowed in Swedish legislation.

As remarked in the Swedish comments to the questionnaire, the answers are given as general statements. Please note therefore that some types of information may be released only if certain conditions are met, for instance that the investigation or pre-investigation at hand involves an offence for which a certain penalty can be imposed. The release of information may also be preceded by an assessment of confidentiality. Thus, every request has to be examined and decided on a case-by-case basis. None of these factors will pose any specific problems as to the transmission to foreign law enforcement bodies, other than those relevant in relation to national authorities.

#### Information/databases managed and directly accessible by law enforcement authorities:

- Register of persons convicted of crime (criminal records)
- Register of persons suspected of (concrete) crime
- Register of persons suspected of criminal activities (criminal intelligence register)
- Decisions prohibiting entry to premises or restraining orders
- Register of wanted/missing persons
- Photographs register
- Fingerprints register
- DNA register
- Identification register (register of distinguishing marks or register of dental records)
- Modus operandi register
- Other registers that describe crimes committed or types of crime
- Register of stolen vehicles or stolen goods
- Firearms tracing register
- Reports (complaints) on crimes committed

- Driving licences register
- Passports register
- Register of national identity cards
- Firearms register
- Observations or observation reports
- Photographs
- Film or video recordings
- Questioning or other records of conversations with persons who co-operate with crime-fighting authorities
- Statements provided by under-cover agents
- Other compilations that contain appraised or non-appraised information on crime or criminal activities.
- Operational analyses
- Documented questioning of suspects, witnesses, plaintiffs, experts etc.
- Documentation of search of premises including search for communication data, seizures, forfeited property or frozen assets
- Documentation of telephone tapping (including so-called surplus information)
- Documentation of room bugging
- Documentation of crime scene investigations
- Documentation of medico-legal investigations
- Telecom monitoring
- Storage and production of telecom traffic (communication data) generated by various information technology systems and handled by telecom operators and Internet Service Providers.
- Register of unusual or suspicious (money) transactions

***Is this information always considered as non coercive according to your national law ?***

When obtained subsequent to a decision by a judicial authority it can be exchanged through police channels.

**Information/databases directly accessible by law enforcement authorities but managed by other authorities**

- Information (held by Prison Administration Services) concerning prison inmates.
- Decisions, permits, fingerprints etc concerning foreign nationals.
- Vehicle data and vehicle owner (cars) register
- Data concerning aircraft and owner of aircraft
- Vessel data and owner of vessel or boat.
- Customs authorities' register of import and export of goods
- Administrative registers on persons (census)
- Register of address and accommodation
- Company board of directors, operations, share capital etc.
- Ownership of real property
- Income and wealth information
- Registered debts such as taxes, maintenance, fines, debts to individual guarantors etc.

*Is this information always considered as non coercive according to your national law ?*

Yes.

**Information/databases accessible by law enforcement authorities but managed by private entities**

- Holders, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, e-mail or website subscriptions or addresses.
- Transport companies' passenger and freight lists.

*Is this information always considered as non coercive according to your national law ?*

When obtained subsequent to a decision by a judicial authority it can be exchanged through police channels, subject to the usual, general conditions and confidentiality rules mentioned above.



**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- Information held by banks, financial institutions and insurance companies on balances, transactions, holding of credit cards or insurance policies.

*Is this information always considered as non coercive according to your national law ?*

No, in certain cases a decision is needed from a judicial authority to use a coercive measure. However, when obtained subsequent to a decision by a judicial authority it can be exchanged through police channels, subject to the usual, general conditions and confidentiality rules mentioned above.

**2. LANGUAGES USED IN CASE OF URGENCY**

Requests in urgent cases can be received in Swedish, Norwegian, Danish and English. Requests will be sent and answered in Swedish and English.

**The following languages will/can be used for sending a request in case of urgency:**

Swedish and English

**Replies to urgent requests can be provided in the following languages:**

Swedish, Norwegian, Danish and English

**Answers can be provided to urgent requests written in the following languages :**

Swedish and English

**3. PREFERRED CHANNEL**

## UNITED KINGDOM

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- details of persons convicted of crime
- details of persons suspected of crime / criminal activities (criminal intelligence)
- decisions prohibiting entry to premises or restraining orders
- wanted / missing persons
- photographs / fingerprints / DNA of persons convicted or suspected of crime
- identification marks
- modus operandi
- data on crimes committed or types of crime
- stolen property including vehicles
- firearms / firearms tracing
- reports (complaints) on crimes committed
- observations or observation reports
- photographic / film / video material
- operational analyses

*Is this information always considered as non coercive according to your national law ?*

No

#### Information/databases directly accessible by law enforcement authorities but managed by other authorities

- driving licences
- passports
- information concerning prison inmates
- decisions, permits, fingerprints etc concerning foreign nationals

- vehicle data and vehicle owners
- aircraft data and aircraft owners
- vessel (boat) data and vessel owners
- transport companies' passenger and freight lists
- (some) census information
- addresses / accommodation
- ownership of real estate property

***Is this information always considered as non coercive according to your national law ?***

Not necessarily. In some cases a UK Data Protection Act application may have to be completed to obtain the information. This may require further facts on the case.

**Information/databases accessible by law enforcement authorities but managed by private entities**

- personal, financial checks etc (Experian)
- company boards of directors, operations, share capital etc
- telephone data – subscribers, billing, cell-siting

*Is this information always considered as non coercive according to your national law ?*

Some types of telephone subscriber information may be considered as non coercive although this may require more facts of the case being made available.

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- Banking data
- Telephone surveillance data

*Is this information always considered as non coercive according to your national law ?*

No

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

English

**Replies to urgent requests can be provided in the following languages:**

English, Spanish, French

**Answers can be provided to urgent requests written in the following languages :**

English, Spanish, French

**3. PREFERRED CHANNEL**

## ICELAND

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

### 1. INFORMATION AVAILABLE

#### Information/databases managed and directly accessible by law enforcement authorities:

- LÖKE ( Icelandic Police Information System, includes all information on Criminal Records)
- Schengen Information System
- AFIS
- Interpol i24/7
- Driving License data base, information on all holders of Icelandic driving license
- Icelandic Firearm Register

*Is this information always considered as non coercive according to your national law ?*

#### Information/databases directly accessible by law enforcement authorities but managed by other authorities

- Passport register (name and passports issued in Iceland).
- ERLENDUR, information system on holders of Icelandic residence and / or work permits and visas issued in Iceland.
- Icelandic National Register and SKYRR hold information of all those who have been domiciled in Iceland since 1952. Registered items include ID number, name, domicile, etc. In addition, all changes to an individual's civil status are registered, among them birth, baptism, marital status, domicile, death, etc

*Is this information always considered as non coercive according to your national law ?*

**Information/databases accessible by law enforcement authorities but managed by private entities**

- *EKJA*, information on vehicle registration, owners etc.;
- *BJALLA*, information on number of points that a person's has in its driving license;
- Information from Internet Service Providers;
- obtaining information from public authorities concerning telephone conversations through a particular telephone, or telecommunications through particular telecommunications equipment, shall be provided to police without a court decision if the approval of the possessor and actual user of a telephone or telecommunications equipment;
- The police may request that Internet Service Providers and Telecommunication Service Providers preserve computer data, include all data on computer communications.
- Hotel registration forms are available to police upon demand.
- The Telephone registry.

*Is this information always considered as non coercive according to your national law?*

**Information/databases that always require a judicial authorisation to be accessed by law enforcement authorities**

- Information on Bank Statements, holders of Icelandic bank accounts etc.
- Information on use of Credit / Debit cards
- Information from Telecommunication service providers
- Ordering public authorities to provide for monitoring or recording of telephone conversations through a particular telephone, or for recording other telecommunications through particular telecommunications equipment.
- Obtaining information from public authorities concerning telephone conversations through a particular telephone, or telecommunications through particular telecommunications equipment;
- Recording telephone conversations or monitoring other sound or signals by use of special sound recording technology or similar technology without knowledge of the persons concerned;
- Recording images or taking photographs or motion pictures without knowledge of the persons concerned.
- Medical records.

*Is this information always considered as non coercive according to your national law ?*

2. **LANGUAGES USED IN CASE OF URGENCY**

**The following languages will/can be used for sending a request in case of urgency:**

French, English, Danish, Norwegian, Swedish, Spanish and German.

**Replies to urgent requests can be provided in the following languages:**

French, English, Danish, Norwegian, Swedish, Spanish.

**Answers can be provided to urgent requests written in the following languages :**

French, English, Danish, Norwegian, Swedish, Spanish.

3. **PREFERRED CHANNEL**

## NORWAY

1. [INFORMATION AVAILABLE](#)
2. [LANGUAGES USED IN CASE OF URGENCY](#)
3. [PREFERRED CHANNEL](#)

### 1. INFORMATION AVAILABLE

#### **Information/databases managed and directly accessible by law enforcement authorities:**

- Persons suspected of crime/convicted of crime (criminal records)
- Persons suspected of criminal activities (criminal intelligence)
- Wanted/missing persons
- Stolen objects/property/goods
- Photographs
- DNA
- AFIS: Automated Fingerprint Identification System
- SIS
- INTERPOL I24/7
- Firearm licenses
- Passports

*Is this information always considered as non-coercive according to your national law?*

Yes

#### **Information/databases directly accessible by law enforcement authorities but managed by other authorities:**

- Driving licences
- Vehicle data and vehicle owner
- Population information; personal data as: name, date of birth, gender, address/accommodation etc.
- Information on company board of directors, capital etc.
- Information on ownership of real property
- Register of employees

*Is this information always considered as non-coercive according to your national law?*

Yes



**Information/databases that always require a judicial authorisation to be accessed by law**

**enforcement authorities:**

- Transport companies passenger and freight lists
- Telecommunication traffic (communication data) stored and produced by telecommunication operators and Internet Service Providers
- Information held by banks, financial institutions and insurance companies on balances and transactions etc.
- Information held by credit cards companies
- Income and wealth information

**2. LANGUAGES USED IN CASE OF URGENCY**

**The following language will/can be used for sending a request of urgency:**

English, Norwegian

**Replies to urgent requests can be provided in the following language:**

English, Norwegian

**Answer can be provided in to urgent requests written in the following language:**

English, Norwegian

**3. PREFERRED CHANNEL**

SISnet

## SWITZERLAND

1. INFORMATION AVAILABLE
2. LANGUAGES USED IN CASE OF URGENCY
3. PREFERRED CHANNEL

The Framework Decision is **not yet applicable** in Switzerland

## ANNEX III

## LIST OF COMPETENT AUTHORITIES FOR FWD 2006/960/JHA

BE	Federal Police	Customs administration		
BG	Directorate for International Operational Police Cooperation of the Ministry of Interior			
CZ	Police bodies	Public prosecutors	Customs Administration	
DK	Danish National Police and other Danish police authorities			
DE	Federal police authorities (Bundeskriminalamt, Bundespolizei) and police authorities at Land level	Tax administration	Customs Administration	Customs Administration - Division "illegal work and clandestine employment"
EE	Police Board Central Criminal Police Police Prefectures	Security Police Board	Tax and Customs Board	Board of Border Guard
	Competition Board	HQ of the Defence Forces	Prosecutor's Office	
IE	An Garda Síochána	Revenue Commissioners		
EL	Greek Police	Hellenic Coastal guard	Fire Brigade	Service for Special Audits
	Custom authorities			
ES	Centro Nacional de Comunicaciones Internacionales (Unidad de Cooperación Policial Internacional de la Comisaría General de Policial Judicial)			

FR	Police Nationale : - Les services relevant de la Direction Centrale de la Police Judiciaire	Police Nationale : - Les services relevant de la Direction Centrale de la Sécurité Publique	Police Nationale : - Les services relevant de la Direction Centrale de la Police Aux Frontières	Direction Générale de la Gendarmerie Nationale
	Direction Générale des Douanes et Droits Indirects: tous les services relevant de cette direction			
IT	Criminal Police Service of the Public Security Department at the Ministry of the Interior <i>[Servizio della Polizia Criminale del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno]</i>			
CY	Unit for Combating Money Laundering	Cyprus Police	Customs & Excise Department	
LV	State Police	Security Police	Fiscal Police	Military Police
	Corruption Prevention and Combating Bureau	Customs Authorities	State Border Guard	Captains of seagoing vessels at sea
	Commander of unit of National Armed Forces located in the territory of a foreign state	Prosecutor authorities		
LT	Financial Crime Investigation Service under the Ministry of the Interior	Lithuanian Police	Special Investigation Service of the Republic of Lithuania	Military Police of the Lithuanian Armed Forces
	Customs Department under the Ministry of Finance	Government Security Department under the Ministry of the Interior	State Border Guard Service under the Ministry of the Interior	
LU	Police grand-ducale [Grand Duchy Police] Direction Générale Service des Relations Internationales	Administration des Douanes et Accises [Customs and Excise Administration] Direction des Douanes et Accises Division ADPS		

HU	National Police	Prosecution Service	Customs and Finance Guard	Protective Service of Law Enforcement Agencies
MT	Malta Police Force			
NL	Netherlands Police - National Police Services Agency (KLPD)			
AT	Directorate General for Public Security, MoI	Security Directorates	District administrative authorities	Federal police directorates
	Federal Ministry of Finance, Unit IV/3, for customs and tax matters			
PL	Internal Security Agency	Central Anticorruption Bureau	Military Police	Police
	Border Guard	Customs Service		
PT				
RO	Ministry of Internal Affairs and Administrative Reform: Police	Ministry of Internal Affairs and Administrative Reform: Border Police	Ministry of Internal Affairs and Administrative Reform: Gendarmerie	Ministry of Internal Affairs and Administrative Reform: International Police Cooperation Centre
SI	The Police	Customs Administration		
SK	Police Force	Railway Police	Military Police	Customs Criminal Office
FI	Police	Customs	Border Guard	
SE	National Police Board (with exception of the security service)	The Police Authority of Blekinge /Dalarna/Gotland/Gävlegorg/Halland/Jämtlands/Jönköping/Kalmar/Kronobergs/Norrboten/Skåne/Stockholm/Södermandland/Uppsala/Värmland/Västerbotten/Västernorrland/Västmanland/Västra Götaland/Örebro/Östergötland	National Economic Crime Bureau when fulfilling police tasks	Swedish Coast Guard
	Swedish Customs			

COMPETENT AUTHORITIES

UK	All Police Forces in England, Wales, Scotland and Northern Ireland	Serious Organised Crime Agency (SOCA)	Her Majesty's Revenue and Customs (HMRC)	Border and Immigration Agency
	Serious Fraud Office	Scottish Crime and Drug Enforcement Agency (SCDEA)		
IS	National Police Commissioner			
NO	National Police, authority entitled to investigate any criminal offences			

**ANNEX IV**  
**LIST OF CONTACT DETAILS IN CASE OF URGENCY**

<b>MS</b>	<b>SERVICE</b>	<b>ADDRESS</b>	<b>TELEPHONE</b>	<b>FAX</b>	<b>EMAIL</b>
<b>BE</b>	PCN-NIP Point de Contact National / Nationaal Invalspunt	rue Fritz Toussaint 8 1000 Brussels		32 2 508 7650 32 2 644 8642	ncb.brussels@be.igcs.int
	Direction Nationale des Recherches / Nationale Opsporing Directie	Boulevard du Roi Albert II 33 / 385 1030 Brussels	32 2 576 5566 (24/7)	32 2 576 1715	dir.nat.rech.da.brussel@minfin.fed.be
<b>BG</b>	Directorate for International Operational Police Cooperation of the Ministry of the Interior.	29 "6-th septemvri" str. 1000 Sofia	359 2 982 4351	359 2 980 4047	ncb@mvr.bg
<b>CZ</b>	Police Presidium of the Czech Republic	Strojnicka 27 P.O.Box 62/MPS 170 89 Praha 7	420 974 834 210	420 974 834 716	sirene@mvr.cz interpol@mvr.cz ncb.prague@cs.igcs.int (24/7)
<b>DK</b>	Danish National Police Communication Center	Anker Heegaards Gade 5, 4 1780 København V	45 33 14 8888 ext. 4200	45 33 32 27 71	nec@politi.dk
<b>DE</b>	Bundeskriminalamt (Federal Criminal Police Office)	65173 Wiesbaden	49 611 550	49 611 55 12141	mail@bka.bund.de
	Zollkriminalamt Zentraler Lage- und Informationsdienst (ZLID) (Customs Criminal Investigation Office)	Postfach 850562 51030 Köln	49 221 6720	49 221 672 4500	zlid@zka.bfinv.de
	Bundesfinanzdirektion West (Federal Finance Office West) - Division "illegal work and clandestine employment"	Neusser Strasse 159 50733 Köln	49 221 3799 3100	49 221 3799 3701 49 221 3799 3702	poststelle@abt-fks.bfinv.de
<b>EE</b>	Central Criminal Police	Tööstuse 52 10416 Tallinn	372 612 3810 (24/7)	372 612 3812	sirene@kkp.pol.ee
<b>EL</b>	SIRENE National Section		30 210 6998260 30 210 6998262 30 210 6924585	30 210 699 8264 30 210 699 8265	sisnetmail: -sgr-oper@csis.sisnetmaileu- -sgr-head@csis.sisnetmaileu- -sgr-sirpit@csis.sisnetmaileu-  email: info@sirene-gr.com

## URGENCY CONTACT

MS	SERVICE	ADDRESS	TELEPHONE	FAX	EMAIL
	For offences relating to the Custom Code and requests for the exchange of non-urgent information, the contact point is Directorate 33, Custom Control, Directorate General for Customs and excise, Ministry of Economic Affairs and Finance		30-210-7259326 30-210-7259328 30-210-7224770	30-210-7259327 30-210-3225192	d33-a@otenet.gr rilod33b@otenet.gr
ES	Centro Nacional de Comunicaciones Internacionales Comisaría General de Policía Judicial, Unidad de Cooperación Policial Internacional	Calle Julián González Segador, s/n 28043 Madrid.	34 91 582 2900	34 91 582 2980	cenci@dgp.mir.es
FR	Ministère de l'Intérieur DCPJ/DRI SCCOPOL - point de contact central	101 rue Trois Fontanot 92000 Nanterre	33 1 4097 8880 (24/7) 33 1 4097 8220 (24/7)	33 1 4097 8248	dcpj-dri-pcc@interieur.gouv.fr
	Direction nationale du renseignement et des enquêtes douanières - brigade de surveillance et de transmission (BST)		33 1 4923 3636	33 1 4923 3923 33 1 4923 3922	pct-dnred@douane.finances.gouv.fr
IE	Garda Communications Centre	Harcourt Square Dublin 2	353 1 666 3108 353 1 666 3109		communications@garda.ie
	Customs Drugs Law Enforcement (Drugs and Arms Trafficking)	Block D, Ashtowngate Dublin 15	353 1 827 7512 353 87 254 8201 (24/7)	353 1 827 7680	antidrugs@revenue.ie
	Customs Drugs Investigations (other than Drugs and Arms Trafficking)	5th floor, Block D Ashtowngate Dublin 15	353 1 827 7756 353 87 255 4283	353 1 827 7786	ceib@revenue.ie
IT	Servizio per la Cooperazione Internazionale di Polizia della Direzione Centrale della Polizia Criminale del Dipartimento della Pubblica Sicurezza del Ministero dell' Interno				
CY	Cyprus Police Headquarters European Union and International Police Cooperation Directorate Interpol National Central Bureau	1478 Nicosia	357 2280 8064 357 2280 8063 357 2280 8553	357 2280 8605	cyinterpol@police.gov.cy
LV	International Cooperation Department of Central Criminal Police Department of State Police	Čiekurkalna 1.līnija 1, korp.4, Rīga, Latvia, LV-1026	+371 6782 9535	371 6782 9532	ssp@vp.gov.lv



## URGENCY CONTACT

MS	SERVICE	ADDRESS	TELEPHONE	FAX	EMAIL
LT	International Liaison Office of Lithuanian Criminal Police Bureau	Liepyno st. 7 08105 Vilnius	370 5 271 9900	370 5 271 9924	office@ilnb.lt
LU	Police Grand-Ducale Direction de l'Information Section Liaison en matière de coopération policière internationale		352 4997 2575	352 4997 2598	sirene@police.etat.lu
HU	<i>Országos Rendőr-főkapitányság, Nemzetközi Bűnügyi Együttműködési Központ (NEBEK)</i> Hungarian National Police Headquarters, International Law Enforcement Cooperation Centre (ILECC) <i>Nemzetközi Információs Osztály</i> Message Response and International Telecommunications Division	Teve u. 4-6 1139 Budapest	36 1 443 5596 36 1 443 5545	36 1 443 5815	nebek@nebek.police.hu
MT	Sirene Office Malta Police Force	Police General Headquarters Floriana VLT 2000	356 2294 2741 356 2294 2742 356 2294 2743 356 2294 2744 356 2294 2745	356 2122 3376	sirene.police@gov.mt
NL	Sirene Nederland	Europaweg 45 2711 EM Zoetermeer Postbus 3016 2700 KX Zoetermeer	31 79 345 9898	31 79 345 8800 31 900 899 8244	piketsirene@klpd.politie.nl
AT	Bundesministerium für Inneres (Federal Ministry of the Interior) Bundeskriminalamt (Federal Criminal Police Office) Office 1.3 - SPOC (Single Point of Contact)	Josef Holaubek-Platz 1 1090 Wien	43 1 248 3685 025 43 1 248 3685 027	43 1 248 3695 1136	bmi-II-BK-SPOC@bmi.gv.at
PL	Komenda Główna Policji Biuro Międzynarodowej Współpracy Policji KGP Sekcja Całodobowej Obsługi Międzynarodowego Przepływu Informacji	ul. Puławska 148/150 02-514 Warsaw	48 22 60 136 40 48 22 84 590 99	48 22 60 126 74	ncbwarsaw@policja.gov.pl
	General Police headquarters				
	Bureau of International Police Cooperation				
PT					

URGENCY CONTACT

MS	SERVICE	ADDRESS	TELEPHONE	FAX	EMAIL
RO	Centrul de Cooperare Polițienească Internațională (International Police Cooperation Centre)	Calea 13 Septembrie 1-5 Palatul Parlamentului, etaj IX sector 5, C.P. 70117 Bucharest	40 21 316 0732 40 21 314 0540	40 21 312 3600 40 21 314 1266	ccpi@mira.gov.ro
SI	Ministry of Interior Police General Police Directorate - Criminal Police Directorate	Štefanova 2 1501 Ljubljana	386 1 428 4780	386 1 251 7516	interpol.ljubljana@policija.si
SK	Prezídium Policajného zboru Úrad medzinárodnej policajnej spolupráce	Račianska 45 812 72 Bratislava	421 9610 56450	421 9610 56459	spocumps@minv.sk
	Military Police Directorate	Železničná 3 911 01 Trenčín	421960 339484 421 32 7442134	421 960 3394943	vp.sod@mil.sk
FI	National Bureau of Investigation Criminal Intelligence Division / Communications Centre	P.O. Box 285 / visiting address: Jokiniemenkuja 4 01301 Vantaa	358 71 878 6281 (24/7)	358 71 878 6299	KRP-RTP-VLP@krp.poliisi.fi
	National Board of Customs / Intelligence and Investigation		<i>Office hours:</i> 358 20 492 2640 358 20 492 2511 358 20 492 2552 358 20 492 2020 (24/7)	<i>Office hours:</i> 358 20 492 2669  358 40 383 0035 (24/7)	<i>Office hours:</i> virko@tulli.fi  customs.service@tulli.fi (24/7)
SE	National Police Board				
UK	Serious Organised Crime Agency		44 207 238 8115	44 207 238 8112	london@soca.x.gsi.gov.uk
IC	National Police Commissioner	Skúlagötu 21 101 Reykjavík	354 444 2500	354 444 2501	international@rls.is
NO	National Criminal Investigation Service (NCIS)	Brynsalléen 6 POB 8163 Dep 0034 Oslo	47 2320 8888 (24/7)	47 2320 8880	post.kripos.desken@politiet.no

## ANNEX V

**Notifications by Member States pursuant to Article 12(6):<sup>1</sup>**  
**BILATERAL OR OTHER AGREEMENTS MAINTAINED**

<b>Belgium</b>	12645/08 ADD 1 + ADD1 REV1
<b>Bulgaria</b>	5023/08 ADD 1
<b>Czech Republic</b>	5004/08 ADD 1 + ADD 1 REV 1
<b>Denmark</b>	5725/09
<b>Germany</b>	11257/08 ADD 1 + ADD 1 REV 1
<b>Estonia</b>	10112/08 ADD 1
<b>Greece</b>	5696/09
<b>Spain</b>	5916/08 ADD 1
<b>France</b>	11133/08 ADD1 + ADD1 REV 1
<b>Ireland</b>	5337/08 ADD 1
<b>Italy</b>	6181/2/08 REV 2 ADD1
<b>Cyprus</b>	5545/08 ADD 1 + ADD 1 REV 1
<b>Latvia</b>	5002/08 ADD 1 REV 1 - 5002/1/08 REV 1
<b>Lithuania</b>	6261/08 ADD 1 + ADD 1 REV 1
<b>Luxembourg</b>	11314/08 ADD 1
<b>Hungary</b>	7004/08 ADD 1
<b>Malta</b>	
<b>Netherlands, The</b>	8677/08 ADD 1
<b>Austria</b>	5003/08 + ADD 1
<b>Poland</b>	6350/08 ADD 1 + ADD 1 REV 1
<b>Portugal</b>	
<b>Romania</b>	5178/08 + ADD 1
<b>Slovenia</b>	11136/08 ADD 1 + ADD 1 REV 2 + ADD 1 REV 1 COR 1
<b>Slovak Republic</b>	5590/08 ADD 1 - 7884/09 ADD 1
<b>Finland</b>	8455/08 ADD1
<b>Sweden</b>	5812/09 ADD 1
<b>United Kingdom</b>	5612/08 ADD 1 + ADD1 REV1 + REV2 ADD1
<b>Iceland</b>	5663/08 ADD 1 + ADD 1 REV 1
<b>Norway</b>	6910/08 ADD 1

<sup>1</sup> Documents available on <http://www.consilium.europa.eu>