



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 19 September 2012

13851/12

**SIRIS 75
COMIX 501**

COVER NOTE

from: Mr Jean-Philippe Walter, Chair of the Schengen Joint Supervisory Authority
to: Mr Christos Drakos, Chairman of the Working Party for Schengen Matters
(SIS/SIRENE)

Subject: Report of the Schengen Joint Supervisory Authority on the follow-up of the
recommendations concerning the use of Article 99 alerts in the Schengen
Information System

Delegations will find in the annex a report of the Schengen Joint Supervisory Authority on the follow-up of the recommendations concerning the use of Article 99 alerts in the Schengen Information System.

JOINT SUPERVISORY AUTHORITY



AUTORITÉ COMMUNE DE CONTRÔLE

Mr Christos Drakos
 Chairman of the SIS/SIRENE Working Group
 Council of the European Union
 175, Rue de la Loi
 B-1048 BRUSSELS

Brussels, 31 August 2012

Report of the Schengen Joint Supervisory Authority on the follow-up of recommendations concerning the use of Article 99 alerts in the Schengen Information System

Dear Mr Drakos

The Schengen Joint Supervisory Authority recently finalised a follow-up to its 2007 inspection of Member States' implementation of Article 99 of the Schengen Convention.

The enclosed report focuses on three of the recommendations made in 2007:

1. Authorities responsible for Article 99 alerts should develop formal, written, structured procedures to ensure Article 99 data are accurate, up to date and lawful.
2. The appropriate national authorities responsible for Article 99 alerts should better control these alerts and inspect them every six months. Additional guidelines should be set out.
3. Where different authorities are responsible for the quality and integrity of data it should be ensured that these different responsibilities are organised and interlinked in such a way that data are kept accurate, up to date and lawful, and that the control of these data is guaranteed.

The overall conclusion drawn by the Joint Supervisory Authority is that most Schengen States still need to invest in cooperation procedures in the area of law enforcement at national level to ensure that all conditions allowing an Article 99 alert to be made are in place. While the procedures when reviewing these alerts – either after six months or close to the retention period – appears sufficient, this is not the situation preceding the alert.

The report shows that some areas still require attention in order to achieve legal compliance. It was therefore decided to distribute the report to you and other relevant stakeholders in order to raise awareness of these issues and highlight the areas requiring attention.

Should you require any further information on this matter, please do not hesitate to contact us.

Yours sincerely


 Mr Jean-Philippe Walter
 Chair of the Schengen Joint Supervisory Authority
 (Signed by the Data Protection Secretary)

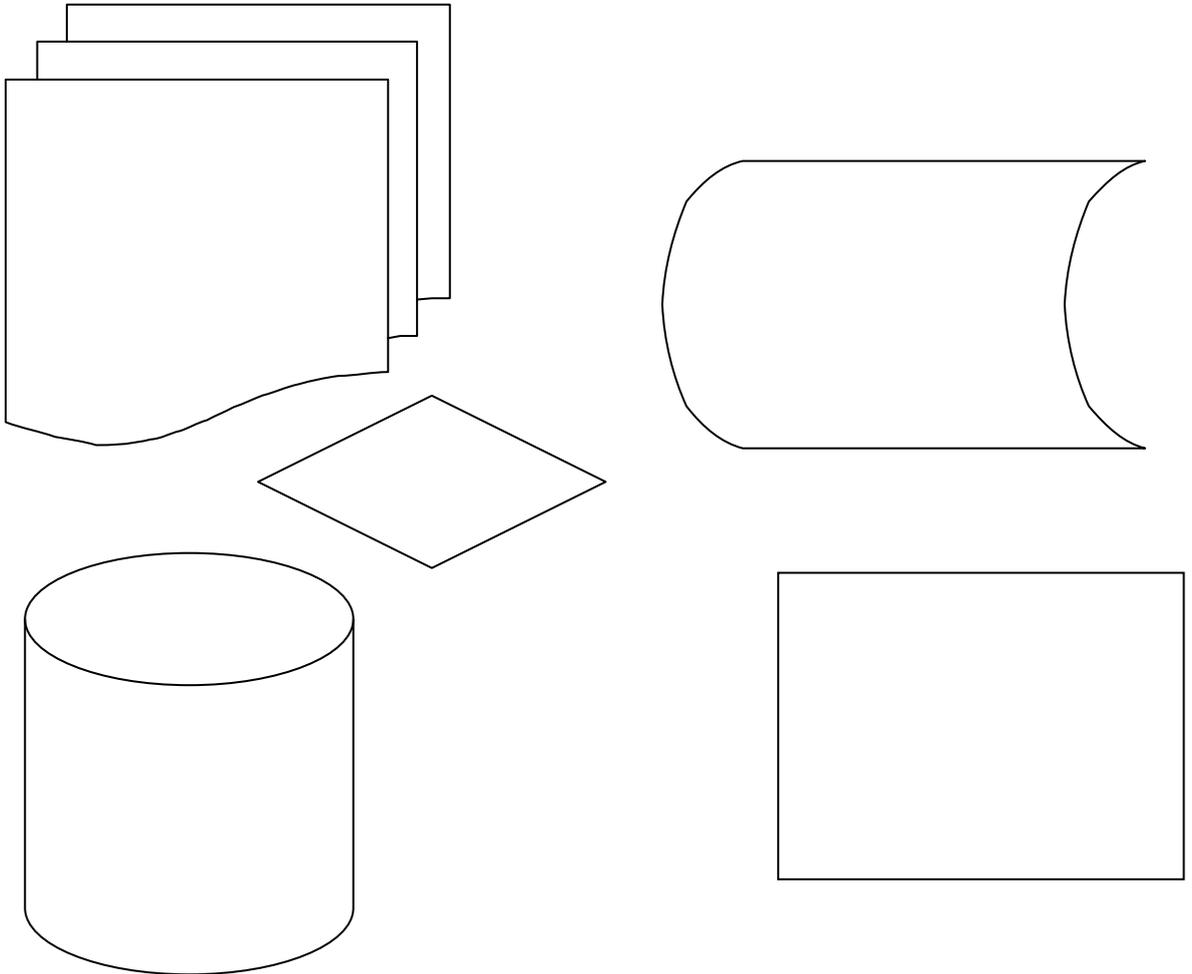
Rue de la Loi 175 - Bureau: 0070FL59 - B-1048 Brussels
 Phone: 32(0)2281 50 26 - Fax: +32(0)2281 51 26

1

ARTICLE 99 SCHENGEN CONVENTION

Schengen Joint Supervisory Authority

Report on the follow-up of the recommendations made regarding Article 99 alerts



Brussels, 14 June 2012
11-22Rev02

Introduction

In its December 2010 plenary meeting the JSA decided to conduct a follow-up to its initial inspection of Art. 99 of the Schengen Convention.

The initial inspection resulted in a number of recommendations, three of which form the subject of this follow-up activity:

1. Authorities responsible for Art. 99 alerts should develop formal, written, structured procedures to ensure Art. 99 data are accurate, up to date and lawful.
2. The appropriate national authorities responsible for Art. 99 alerts should better control these alerts and inspect them every six months. Additional guidelines should be set out.
3. Where different authorities are responsible for the quality and integrity of data it should be ensured that these different responsibilities are organised and interlinked in such a way that data are kept accurate, up to date and lawful, and that the control of these data is guaranteed.

Delegations were provided with a checklist relating to these three recommendations; the checklist was intended to serve as a questionnaire for the competent national authorities. Upon receipt of those authorities' responses, delegations were to assess whether the situation has improved and whether the recommendations are implemented.

As of 14 June 2012, 21¹ delegations had submitted their responses. While Switzerland also informed us of the results of a general survey on Art. 99, those results are not presented here; this type of alert is not used in Switzerland.

Conclusions

A comparison between the results of the first inspection and the follow-up activity is not straightforward; while many Schengen States contributed to the follow-up inspection, they were not members of the Schengen community at the time of the first inspection.

These conclusions are thus only based on the 21 contributions received and present an overall assessment as to whether sufficient measures are in place to fulfil all data protection requirements.

Concerning the recommendation that authorities responsible for Art. 99 alerts should develop formal, written, structured procedures to ensure Art. 99 data are accurate, up to date and lawful, the answers received show that in the vast majority of the Schengen States participating in this survey (participating Schengen States) specific procedures for Art. 99 alerts are in place. Such measures are intended to ensure that data are accurate, up to date and lawful. Whether these procedures are sufficient depends on their content and their relation with other conditions. For example, when someone is alerted using the Art. 99 alert following a prosecution (or other judicial investigation proceedings), it is important that information from that proceeding is made available when that information may lead to the deletion of that alert. The survey demonstrated that an obligation to inform the alerting authority exists in only two participating Schengen States; much is apparently left to the discretion of the authorities involved.

¹ Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Slovakia, Slovenia, Spain, Sweden.

A similar situation exists between the different police or other investigation authorities. Where they hold information that could be essential for the alerting authority to assess whether all conditions for the Art. 99 alert are in place, in most participating Schengen States there is no procedure in place obliging them to inform each other.

The need to check information is better arranged in the process of preparing an alert. Most responses indicate that there are checks in relevant police files as to whether all conditions for an Art. 99 alert are in place.

The recommendation to inspect the Art. 99 alerts every six months is followed by five participating Schengen States. Many others only review the alert in the procedure for continued storage as referred to in Art. 112(1) of the Schengen Convention. In some situations a review is conducted after a hit.

When reviewing an alert just before the one year retention time, most participating Schengen States have instructions in place detailing how the review should be done, including checking other available information. Although the procedures, instructions, and authorities involved clearly vary widely, the conclusion that they comply with the recommendations made is justified.

The overall conclusion is that most participating Schengen States must still invest in cooperation procedures in the area of law enforcement at national level to ensure that all conditions are in place allowing an Art. 99 alert to be made. While the procedures when reviewing these alerts – either after six months or close to the retention period – may be sufficient, this is not the situation preceding the alert.

Summary of responses received

1: Authorities responsible for Art. 99 alerts should develop formal, written, structured procedures to ensure Art. 99 data are accurate, up to date and lawful.

A. What has been done to ensure this? Which written procedures exist, apart from the SIS Manual?

- Denmark: The Danish National Police have formal written guidelines regarding the procedures for Art. 99 alerts. The guidelines are both aimed at the personal in the Danish SIRENE Bureau and authorities requesting Art. 99 alerts. The procedure for Art. 99 alerts are as follows: A formal application form has to be used when requesting an Art. 99 alert. The guidelines for an Art. 99 alert are sent to the requesting authority along with the application form. When the application form is returned to the Danish SIRENE Bureau it is approved by a senior legal advisor before the alert is inserted into SIS.
- Austria: Art. 99 alerts and corresponding national alerts are to be issued on the basis of the Code of Police Practice (SPG) and the Provision on Wanted Persons-Databases and Information 2009 (FIV 2009). The objectives set out by Art. 99 CISA have been included into the national provisions, which are issued by the Federal Ministry of the Interior for all authorities and services authorised to view and issue such alerts.
- Estonia: Chapter 4 of Directive No. 50, 'Approval of the Procedure for Searching and Surveillance of Persons and Identification of Unidentified Persons and Dead Bodies', deals with the alerts set pursuant to Art. 99.
- Luxembourg: There is no specific written procedure. The alerts are to be considered as investigation acts which are decided by judicial authorities and are governed by the rules of normal criminal proceedings.
- Iceland: In 2009, the National Police Commissioner issued two Art. 99 alerts – one because of suspicion of serious financial crimes and the other because of suspicion of drug smuggling. The first alert was deleted after about ten weeks. The latter was deleted right away because authorities in another country had issued an Art. 95 alert on the individual in question. These are the only Art. 99 alerts issued by Icelandic police authorities. In the light of these few alerts, they have not considered it necessary to develop formal procedures on these alerts. However, each case, in which an Art. 99 alert might be an option, is considered in the light of the SIRENE Manual before decision on an alert is taken.
- Finland: Apart from the SIS manual there is a national SIRENE manual, which includes instructions on all categories of alerts. There are also separate instructions for Art. 99 alerts. At the moment there is an ongoing project at the SIRENE office; the aim of this project is to transfer all instructions into an electronic platform; at the same time the instructions are to be updated when necessary. In 2010 Finland made 16 alerts on the basis of the Art. 99(2) concerning persons and 2 alerts concerning vehicles. There were no alerts on the basis of Art. 99(3) in 2010.
- Slovenia: Written procedures within: Slovenian Police Code; Internal Practical guidance on the SIS for end-users and SIRENE operators; Professional guidance of work on the International Police Cooperation Section.

- Germany: In addition to the SIS manual, for all supplying agencies there are the police service regulations (PDV) 384.1 (police investigation) and 384.2 (police observation), which are partly complemented for the individual Federal States by pertinent state-specific supplements. While PDV 384.1 lists fundamental regulations for the investigation (also in the SIS), PDV 384.2 points out specific regulations for discreet checks concerning the reason, purpose, duration, extension of a period, erasure etc., also in view of the SIS. For this purpose, uniform forms have been developed in some Federal States. Following the check of 2006, special leaflets to launch an international police investigation, and for a discreet checks alert, were developed in some Federal States. The police service regulations are classified as classified information "VS (classified information) - for official use only". The legal obligation of correctness, topicality and legitimacy of data result from the area-specific norms of the Police Law, the Code of Criminal Procedure and the Data Protection Act.
- Lithuania: Order no. 4-744 of the Commander of the State Border Guard Service (31/8/07) on approval of instruction on actions in case of a hit in the NSIS. Order no. 5-V-845 of the Police Commissioner General (17/11/09) on approval of procedures on performance of specific and cautious controls and on data processing, which was coordinated with the State Security Dept. and the State Border Guard Service under the Ministry of Interior; this regulates all procedures and actions on Art. 99 alerts and hits.
- The Netherlands: The NSIS Instruction (in force from 02/2008) under the responsibility of the Board of Procurators General contains rules and procedures; this Instruction is being rewritten and is expected to be proclaimed and established from 1/11/11.
- Slovakia: Internal Ministry of Interior acts specify procedures of authorities involved, and regulate reasons and terms regarding Art. 99 alerts. Order of Ministry of Interior Nr. 52/2007 on procedures regarding monitoring of persons and vehicles and Order of Ministry of Interior Nr. 50/2007 on information system of monitoring of persons and vehicles.
- Sweden: The Swedish SIRENE bureau has developed written procedures for registration according to each of the Art.s 95-99 in the Schengen Convention. A police authority makes a request for an Art. 99 alert on a specific form. The SIRENE bureau checks that the conditions for such an alert are fulfilled and that the person in question is not detained or kept in custody. The decision to enter an alert is signed by a head of unit. Only the SIRENE bureau may enter information into the SIS.
- Malta: The Police have internal regulations and circulars issued at General HQ level. These circulars are binding upon police officers. When it comes to the application of Art. 99, the internal rules replicate what is contained in the Schengen Convention on the issuing of similar alerts. There are also rules in relation to data quality. It is the intention of the Police to draw up written guidelines which formalise in detail the procedures when dealing with SIS alerts.
- Latvia: The Law on Operation of the SIS, and Cabinet Regulations No.639 of 18 September 2007. Also, Every police officer has the possibility to use the SIS end-users manual which is available on the police intranet. There are guidelines in the manual on procedures and legal conditions to which alerts should correspond.
- Poland: Authorities issuing alerts are responsible for these issues.

- Greece: Two Basic Orders of the Ministry of Citizen's Protection: Basic Order 5266/6/46 (30-10-1997): 'The application of the Convention implementing the Schengen Agreement – Checks in relation to Schengen data – Users' access, new search procedure under the N.SIS'; and Basic Order 4864/3/98-a (10-06-2008): 'Law 2514/1997 on the ratification of the Convention implementing the Schengen Agreement – Article 99 discreet surveillance and specific checks for reasons of national security.'
- Italy: Following specific inquiries and investigations, the Italian DPA issued a decision dated 10 July 2008 requiring written instructions to be laid down concerning 1. Who was to be in charge for requesting alerts to be entered in the system, and 2. What procedures were to be implemented in order to enter alerts; in particular, a specific order detailing the relevant reasons and undersigned as appropriate was necessary. The Italian Ministry for Home Affairs confirmed that these requirements had been complied with. There is a specific module available in the Schengen portal of the Ministry.
- Czech Republic: Legal background for processing of personal data within the police, and therefore in the SIS: the Police act (No. 273/2008 Coll.) and Personal data protection act (No. 101/2000 Coll.). Personal data processing procedures in the SIS further specified in internal regulations of the police (procedures of deletion, updating, data retrieval, security, responsibility etc. are described). There are more stringent conditions for issuing alerts on foreigners who are family members of EU citizens (communication between SIRENE bureaux, form O is used).
- Belgium: Apart from the SIS Manual, there are instructions on Schengen alerts by the Minister of Justice and the Minister of Home Affairs. These instructions state that prior to a Schengen alert, it should be checked whether:
 - there is enough (basic, complementary and additional) information.
 - basic information involves data registered in the SIS
 - complementary information is information that should be exchanged at international level
 - additional information is intelligence allowing SIRENE to form an opinion on the validity of the alert and to answer questions from other SIRENES without having to contact the alerting service each time
 - the conditions for issuing an alert have been met, i.e.:
 - the alert must be issued in compliance with the Schengen Convention without any misuse of purposes
 - the national alert must be issued beforehand (the individual consequently has to meet the criteria for a national alert)

A codex drawn up by the Minister of Justice and the Minister of Home Affairs includes a list of offences that may lead to an alert based on Art. 99. The instructions regarding international alerts (including those related to the SIS) are currently being adapted but have not been officially approved. It is envisaged to refer to violations likely to be subject to a European arrest warrant.

- Spain: There are in place general guidelines covering the process of issuing and reviewing alerts agreed by all the police bodies with SIS access, but there are no specific Art. 99 alerts guidelines. There are also regular meetings with representatives of all the police forces with access to SIS, SIRENE and the N-SIS manager in order to discuss, assess and to agree enhancements to the guidelines.

- Hungary: The authorities can initiate the inputting of an alert only for discreet surveillance (and not for directed checks). This procedure is regulated by Act XL of 2010 on the amendment of certain laws in the field of law enforcement and migration and the amendment of certain laws in connection with the introduction of VIS and by an internal decree issued by the Criminal Director of the National Police. The legislation determines the cases, the legal base, the competent authorities and the procedure for inputting an alert based on Art. 99. According to this the appropriate authorities in cases determined by the law can initiate the procedure via the SIRENE Bureau. In order to launch this they need to fill in a specific form which can be found in the Annex of the law and send it to SIRENE Bureau. After checking the accuracy of the data the SIRENE Bureau forwards the alert to C.SIS.

B. Is there a procedure obliging: i) courts; ii) public prosecutors or Investigating judges to inform the police (the investigating authority that sent the information to the authorities referred to under points i and ii) about their final conclusions in a specific case or concerning a specific person?

- Denmark; Latvia, Spain, Sweden: No such formal procedure in place.
- Estonia: Entering Art. 99 alerts is subject to the existence of the surveillance proceedings as set out in the Guidelines for Entering Searches for Persons in the Procedural Information System. Surveillance proceedings are terminated on the bases stipulated in S11 of the Surveillance Act. The relevant surveillance proceedings are deleted from the procedural information system and the alert is removed from the SIS when the surveillance proceedings are terminated.
- Italy: In general, when there is an obligation to include this information in the CED (i.e. the centralised police intelligence database) data must be kept up to date and accurate. It must be specified that alerts ex Art. 99 is a task of the local competent Police offices. Subjects under i) and ii) cannot operate directly on the SIS. If there is a need for inserting an alert under Art. 99 they may require police forces or in the case of public prosecutors the police officials operating at their disposal to do so.
- Finland: The authorities exchange information when necessary.
- Greece: No written procedure; however, the police may be informed in case of a conviction.
- Hungary: The inputting of an Art. 99 alert can not be initiated by the courts or the public prosecutors.
- Luxembourg: In the logic of the rule of law and the principle of the “separation of powers” the Courts are not obliged to inform the police about their final conclusions in a case. An alert is uphold as long as it is lawful and considered by the judicial authority to be useful.
- Iceland: According to answers from the SIRENE Bureau, which forms part of the National Police Commissioner’s office, the SIRENE Bureau co-operates closely with the authority requesting access and makes it clear that a notification shall be sent as soon as an alert is no longer needed. Otherwise, reference is made to the answer to question 1A.
- Slovenia: Under the provisions of the Slovenian Police Code, only the Public Prosecutor’s Office is allowed to order the use of Art. 99 under the request of the Slovenian Police, based on circumstances and reasons for doing so. Public Prosecutor’s Office permission to the

police to use Art. 99 is valid for 3 months. After this, police can extend use for another 3 months. For each 3-month extension period, police must send request to the Public Prosecutor's Office with very precise explanation of the reasons. Extension cannot be longer than 2 years total.

- Austria: Responsibility concerning Art. 99 alerts lies with the law enforcement authorities/services, alerts can be issued without any contribution by the judicial authorities. In case of a hit, the services producing the hit have to notify the law enforcement authority/service responsible for the entry.
- Germany: As far as a judicial order is needed to perform discreet checks in the field of averting of a danger, the police must obviously also be informed about the result of the request for such an order. Public prosecution offices are obliged to inform the police about the result of criminal proceedings.
- Lithuania: No separate procedure on this. Info on decisions of courts/prosecutors is derived from the information systems; written decisions of courts/prosecutors are delivered by general procedure on delivery of court/prosecutor decisions.
- The Netherlands: Not for courts, but for public prosecutors an obligation exists according to an Instruction (on the notification of the outcome to the controller) to inform the authority responsible for the processing of police data whenever the prosecution or adjudication of a criminal case has ended (e.g. acquittal/dismissal by prosecutor).
- Slovakia: Within the frame of mutual cooperation of law enforcement authorities, there is mutual exchange of information, which is relevant for particular authorities in order to set the proper measures for successfully finalising cases. Re: execution of alerts pursuant to Art. 99, there are no particular provisions or written manuals obliging courts/public prosecutors to provide police authorities with information on specific cases according to Art. 99.
- Malta: As the public prosecutors are themselves the police, no procedure is considered necessary in this case given that the police are always informed about or aware of the conclusions.
- Belgium: No specific written procedure obliging courts/public prosecutors or investigating judges to inform the police about their final conclusions in a specific case or concerning a specific person.

C. Is there a procedure obliging police or other investigating authorities to inform each other when they should suspect that their information is of relevance for assessing the conditions for the Art. 99 alert?

- Denmark: No such formal procedure in place – but alerts reviewed at least every 6 months.
- Estonia: A police database was established pursuant to Sect.8(1) of the Police and Border Guard Act. The submission of data is regulated in Sect.11 of that Act.
- Finland: The authorities exchange information when necessary.
- Slovenia: Yes, within the Slovenian Police Code.
- Spain: Yes.

- Greece: No. But in practice, once there is an Art. 99 alert all competent authorities required to check the SIS exchange any relevant information they may possess.
- Austria: Obligations to inform other authorities are set out in the FIV 2009 and in specific reporting provisions, according to which other authorities must be notified in case of a hit or a CID case of particular importance.
- Germany: No independent procedure in the form of a service instruction or comparable regulation. Police's legal obligation to correct, block and erase data in files results from the general regulations. A regulation re: criminal proceedings obliges the body recording the data to inform the recipient of transferred data about the correction, erasure or blocking if necessary for protection of the data subjects' legitimate interests.
- Sweden: The SIRENE bureau sends a reminder to the requesting police authority after approx. 10 months to see if the alert should remain. If yes, the alert is kept for another year, if not, the alert is deleted. Also in the case of a hit, the requesting police authority is informed.
- Lithuania: Procedures for exchange of information on Art. 99 alerts are regulated by Order no. 5-V-845 of the Police Commissioner General. Such data are available to all competent authorities, when necessary additional data may be provided.
- The Netherlands: No obligatory procedure but they can inform each other following the provisions of the Police Data Act.
- Slovakia: The competent police unit acquires knowledge on persons by means of its own activities resulting from the duties set up by internal acts of the Ministry of Interior. On the basis of the knowledge acquired, the unit is qualified to weigh circumstances and opportunities of exercise of institutes of investigative operational activity pursuant to the provisions of the Act no. 171/1993 of Collection of Laws on Police Force which also includes *inter alia* the institute of discreet surveillance (monitoring).
- Malta: Although the police have a MoU on the exchange of information and mutual assistance with other law enforcement agencies such as the Customs and Armed Forces of Malta, such MOU does not specifically regulate similar instances relating to Art. 99 alerts.
- Latvia, Hungary, Belgium: No.
- Iceland: See answer to 1A.
- Luxembourg: The judiciary police acts on instruction of the public prosecutor and the investigation judge. The judiciary has not to give accounts to police. If an investigation act is unlawful it can be annulled or will not be considered following the rules of criminal proceedings.
- Italy: Question unclear; has it to do with the assessment to be performed prior to entering an alert or in case a hit is found? At all events, there do not seem to be a procedures of this kind in place. It must be considered that having in mind the reasons for inserting an alert under Art. 99 is up to the competent police forces evaluate the need of such alert on the basis of their ongoing investigation.

D. Is there a procedure obliging an authority intending to use an Art. 99 alert to check the conditions of Art. 99 not only with its own files but also with other law enforcement information including the information systems of Europol?

- Denmark: Yes, according to the Danish SIRENE Bureau's guidelines the bureau will perform such a check.
- Estonia: According to the internal work procedure observed by the police from the date of joining the Schengen visa space until 22 January 2009, alerts were entered in the SIS national register by hand by the SIRENE bureau. The SIRENE bureau made sure the data met all requirements when entering them in the system. After the search database was entered in the procedural information system, which made the submission of data to the national Schengen register automatic, the information system maintained the setting according to which the data pass an evaluation in the SIRENE bureau (before they're passed to the central European system).
- Lithuania: In each case, checks are made as to whether a national search on a person is issued by the competent Lithuanian authorities, and whether alerts by Lithuania and EU MS are published under Art. 95-99 CISA.
- Austria: The use of individual systems such as SIS, Interpol and Europol is laid down in internal provisions such as FIV 2009.
- Greece: No such obligation but there is a procedure that allows for the competent authorities to gather information either from information systems of Europol or from other law enforcement agencies and cooperate with them when necessary on a case by case basis.
- Hungary: There is no such a procedure in place. Only by following its own internal procedures that an appropriate authority can initiate a procedure for inputting an alert based on Art. 99.
- Sweden: The SIRENE bureau checks that all conditions for an Art. 99 alert are fulfilled.
- Slovakia: Authorities competent for initiation of creation of Art. 99 alerts in connection with detection/obtaining necessary information proceed pursuant to law order of the Slovak Republic consider all possible procedures, methods and tools depending to individuality of the case, which means that information obtained via Europol could contribute towards decisions to create Art. 99 alerts.
- Luxembourg: The judicial authorities have to decide if an information of Europol or a check with Europol data is indicated for the purpose of investigation.
- Finland: The authority entering the alert is responsible for checking the conditions of the alert from all the available information systems.
- Belgium: The consultation of other files such as the EIS is neither compulsory nor systematic. The police services nevertheless consult them whenever they believe the files may contain additional information necessary for the evaluation of an alert. Information is also exchanged with their international counterparts, among others in the Police Working Group on Terrorism.

- Slovenia: Yes, within the Slovenian Police Code and the Professional guidance of work on the International Police Cooperation Section.
- Spain: Yes, there is a national database allowing those checks. Regarding Europol, checks need to be conducted through the Europol National Unit.
- Germany: No such procedure exists. App. 2 of the PDV 384.2 says that prior to an entry into the SIS, it should be examined whether the data record of the person or of the vehicle has already been stored in the SIS. Alerts according to Art. 99 for discreet checks with alerts in other states according to Art. 99 for targeted controls are incompatible.
- Malta: No specific procedure obliging checks with other information systems available such as Europol. However, whenever the conditions for an Art. 99 alert is met, the matter is referred to the SIRENE unit by the investigator (i.e. the police officer in charge) and treated in a coordinated fashion. There might be instances where an investigation may possibly involve both Europol and SIS data. In such cases, the investigator coordinates with both units responsible for Europol and NSIS in order to ensure an effective and suitable way forward.
- The Netherlands: No, see answer to 1C.
- Italy: See answer to 1C.
- Iceland: See answer to 1A.
- Latvia: No.

E. Are there procedures/instructions to assess - after a hit of the Art. 99 alert - if: i) the data are relevant and can be used in the investigation; ii) irrelevant data are deleted; and iii) the data are used to assess the lawfulness of maintaining the alert?

- Denmark: Requesting authority will receive the data from a hit of the Art. 99 alert and will also assess the data in regard to the above-mentioned.
- Estonia: Data are reviewed every 2 months by the person who initiated the alert. If an alert is not extended in time, it is automatically deleted from the SIS national register. The person in charge of surveillance proceedings terminates all alerts relating to the proceeding when the proceeding itself is terminated.
- Finland: The national SIRENE manual includes instructions concerning hits on general level. Information about the hit is transmitted to the authority which entered the alert. The authority responsible for the alert assesses the necessary actions and the need to maintain the alert. Same procedure followed concerning Art. 99 alerts, though there are some special instructions on Art. 99 alerts.
- Slovenia: Yes, within the Slovenian Police Code where the collection, sharing, maintaining and deletion of data is precisely defined.
- Sweden: In the case of a hit, the requesting police authority is informed and will assess further actions.

- Italy: After a hit, information acquired are immediately sent to the Authority which has inserted the alert. Any further evaluation is left to that body. In general data are cancelled, although where the investigative exigencies persist data can be maintained in the system.
- Greece: No formal procedures. The requesting authority has the sole responsibility for entering the data and is the only competent authority to assess relevance and lawfulness of the data. All police divisions must adhere to Presidential Decree 141/1991.
- Germany: No known procedures/instructions explicitly referring to the points listed above under i-iii. In the appendix to PDV 384.2 the legal requirements for the storage of accrued data are listed. Data accrued in connection with Art. 99 alerts for law enforcement purposes are judicial data that will be part of the investigation file and they are governed by special regulations.
- Lithuania: In case of a hit, the initiator of the alert, which uses information for operational activities (criminal intel), pre-trial investigation, or purposes of the Law on Organised Crime Prevention is informed.
- Luxembourg: If the Public prosecutor or the investigation judge considers that an alert has not to be uphold or that the conditions of the alert are not given, that data are not relevant any more, the alert will be cancelled, like any other investigation measure. It is difficult to understand the scope of specific proceedings only for Schengen alerts different from other investigation or prevention measures.
- The Netherlands: This is discussed in NSIS Instruction under 5.6, but no specific procedure is established regarding these 3 points. Obviously, national law (Criminal Procedures Act and Police Data Act) applies.
- Austria: Correctness of the data has to be verified according to the parameters mentioned in i) to iii) by the service responsible for the Art. 99 alert and the corresponding national search notice.
- Slovakia: To evaluate obtained information, particular proceedings are specified in the Order of Ministry of Interior Nr. 52/2007 on procedures regarding monitoring of persons and vehicles and in the Order of Ministry of Interior Nr. 53/2009 on operative-searching activities. The Order is at 'confidential' level of security information because of setting up of tactical procedures. In general, there are individual proceedings how to process the information depending on each particular case. Conditions of processing information and personal particulars collected via performance of duties of the Police Force, and also information and personal data provided from abroad, are subject to regulation by Act no. 171/1993 of Collection of Laws on Police Force. The above-mentioned information and personal data are processed in the scope necessary for performance of duties of the Police Force. If the Police Force finds out – either at checks or during processing of personal data – that these data are unnecessary for performance of the duties of the Police Force, they will be erased without delay.
- Belgium: No specific written procedure, but in practice the hits are analysed to decide whether the alert will be maintained or not. Hits can thus consolidate a legal case file which already contains several elements incriminating the data subject. In cases opened by certain police services, the hits can either enhance the elements in the case file to open a legal case or invalidate information so that the investigation is abandoned.

- Malta: No such procedure exists; however, any decision on the information available further to a hit depends on the investigation itself and is always taken after consultation with the investigator.
- Latvia: No. There is a SIRENE end-users' manual available on the police intranet where guidelines regarding legal aspects are provided.
- Spain: There are no formal procedures as the requesting authority is entirely responsible for both entering the data and assessing relevance of the data and lawfulness of maintaining the alert.
- Hungary: No.
- Iceland: See answer to 1A.

2: The appropriate national authorities responsible for Art. 99 alerts should better control these alerts and inspect them every 6 months. Additional guidelines should be set out. (Art. 112(1) of the Schengen Convention obliges a review of the need for continued storage no later than 1 year after they were entered).

A. What has been done to ensure this? Which written procedures exist, apart from the SIS Manual?

- Denmark: All Danish Art. 99 alerts are automatically created with a six month expiration date. According to the Danish SIRENE Bureau's guidelines it is possible to prolong an alert but only with 6 month every time. Before an alert is prolonged the alert must undergo a review, including consultation of the requesting authority.
- Italy: There are internal circular letters that refer to the SIS Manual as the legal benchmark for all processing operations and the respective arrangements.
- Greece: Application of Basic Order 4864/3/98-a on Law 2514/1997 on the ratification of the Convention implementing the Schengen Agreement – Article 99 discreet surveillance and specific checks for reasons of national security. Pursuant to par. 9, the Informatics Division ensures that the authority responsible for the entry of the alert is notified on the imminent expiration date of the alert so the requesting authority may be informed on time in order to assess the necessity of extending the alert. Thus, 30 days prior to the expiration date (this time is considered a sufficient time period for a proper notification), the authority responsible for the entry of the alert is informed. If the requesting authority does not request the maintenance of the alert in time (i.e. that there still exist reasons for continued storage of the alert), the alert is automatically deleted. Also, the Informatics Division has put in place a system whereby SIRENE officers are informed via a specific electronic form of the expiration of the relevant alerts, within a year – at the latest - from their entry, according to art. 112(1) CISA.
- Finland: National SIRENE manual and the internal instructions of the SIRENE office include instructions on checking the validity of the alerts, though the 6-month recommendation is not followed.

- Austria: According to the internal provisions (FIV 2009), Art. 99 alerts are to be reviewed six months prior to their date of expiry. Corresponding national alerts are to be reviewed as well.
- Slovenia: Slovenian Police Code; Internal Practical guidance on the SIS for end-users and SIRENE operators; and Professional guidance of work on the International Police Cooperation Section.
- Germany: If it's a discreet check in accordance with Sect. 163(e) StPO (Code of Criminal Procedure) the order for the check must be limited to the maximum of 1 year (Sect. 163(e)(4) sentence 5 StPO (Code of Criminal Procedure)). An extension by no more than 3 months is admissible insofar as the conditions for making the order continue to apply (Sect. 163(e)(4), sentence 6 StPO). According to Sect. 163(e) Code of Criminal Procedure orders for discreet checks may be given only by the court and in exigent circumstances the order may also be made by the public prosecution office (Sect. 163(e)(4), sentence 1 and 2, StPO). So, an extension of the order exceeding twelve months also always requires judicial review as to the necessity of further storage. Federal State regulations for orders for discreet checks for preventive reasons are structured differently. The order is restricted to 9-12 months and can only be ordered by a head of an agency and/or president of police or by a person specially authorised for this purpose. An extension of the order can partially only be ordered by a court. Most state-related legal provisions include a regulation to review after 3-6 months whether the conditions for the order still apply. A written record must be made of the result of this review. Only a few Federal States have a legal basis for the order for preventive specific controls. A Federal State having such a legal basis has higher requirements for the order for preventive reasons. In this case, the order must always be ordered by a court and are generally limited to 6 months. Some Federal States work with automatically-compiled warning lists, which are sent to the competent authorities 2-5 months before expiry of the retention period. After deadline expiry, orders - if no respective extension was induced - are deleted automatically.
- Sweden: Alerts are automatically deleted after one year unless reactivated. Some time before the one year period expires (approx 10 months), a question is sent to the requesting police authority whether the alert should be kept or not. If yes, the alert is reactivated for another year, if not, it is deleted.
- Hungary: According to the relevant legislation the IT system is designed so that an Art. 99 alert (concerning persons) can be inputted and maintained only for 1 year. The procedure of inputting, deleting before 1 year and maintaining after 1 year can be initiated by the alerting authorities at the SIRENE Bureau. The SIRENE Bureau, based upon the request and after careful consideration can input, delete or maintain an alert. In every other case the data is automatically deleted after 1 year by the system.
- Lithuania: under Order no. 5-V-845 of the Police Commissioner General, all Art. 99 alerts shall be terminated automatically after expiration of the validity period (usually 6-12 months, no longer than 12 months). To extend the validity period, the procedures followed for the original alert publication must be repeated.
- The Netherlands: The current NSIS Instruction requires a review after 1 year. The new NSIS Instruction will require a review after 6 months, performed by the public prosecutor.

- Slovakia: The relevant procedure is the Order of Ministry of Interior Nr. 52/2007 on procedures regarding monitoring of persons and vehicles.
- Malta: No specific written procedures other than the provisions in CISA exist. However, SIRENE supervisors retrieve reports from SISone4ALL on a monthly basis, 1 month prior to the expiration of the review/expiry period for all alerts. A review is then carried out in consultation with the competent police units.
- Estonia: See answer to 1E.
- Iceland: Iceland: See answer to 1A.
- Latvia: There is no procedure to ensure better control / inspect the alerts every 6 months. N.SIS informs SIRENE bureau about every alert with approaching expiry date. SIRENE bureau informs responsible end-user about necessity to review maintenance of the alert into the system.
- Spain: On a monthly basis, N-SIS managers extract from N-SIS all those alerts close to expiration. The responsible Police body must assess the validity of the alert in order to communicate any possible change.
- Belgium: When examining case files, the DPA observed that the decisions to maintain an alert were not always taken in a structured and uniform way. Following this observation, written instructions on Schengen alerts were drawn up. The SIRENE bureau prints a monthly list of alerts that are about to expire. All alerts on this list are looked into in order to check whether the alert needs to be maintained. The authority that issued the alert is informed that the alert is about to expire and that if there is no request to maintain the alert, it will be deleted automatically.

B. i) Are there procedures/instructions to review the necessity and lawfulness of the alert periodically? ii) How many times with the 1 year period does such a review take place?

- Denmark: As mentioned above, all Art. 99 alerts are reviewed every 6 months. Also according to the Danish SIRENE Bureau's guidelines all alerts according to Art. 99, subsection 2, para a, must be reviewed every third month.
- Czech Republic: The police are obliged to review the necessity to process personal data according Art. 99/1 a year after they were entered (and each year after). The obligation is laid down in the police internal guidelines.
- Estonia: Yes, see answer to 1E. Reviews take place 6 times a year.
- Iceland: See answer to 1A.
- Austria: Yes, as set out in SPG, FIV 2009 and the Data Protection Act (DSG). A review has to take place prior to the expiry of the alert at the latest. An additional review is conducted in the case of a hit.
- Hungary: The review is done by the SIRENE Bureau upon request of the alerting authority or at the end of the 1 year. Alerting authorities have never requested the maintenance of an

alert after 1 year. In Hungary no personal data were kept in relation to an alert based on Art. 99 for more than 1 year.

- Finland: According to the national SIRENE manual and the separate instructions concerning Art. 99 alerts, when the system informs that the end of the 1 year validity period is approaching, the SIRENE bureau contacts the authority which entered the alert; that authority is asked if the alert should still be valid and is reminded the alert must be deleted immediately if not needed/justified. The review is made when the end of the 1 year period of validity is approaching.
- Slovenia: Permission for the use of Art. 99 by the Public Prosecutor's Office to the Police is valid for 3 months. After this the police can extend the period for another 3 months but not longer than for 2 years. For each 3-month extension, police send request to Public Prosecutor's Office with a very precise explanation of the reasons.
- Germany, Sweden: See answer to 2A.
- Lithuania: As mentioned under 2A, Order no. 5-V-845 of the Police Commissioner General provides that all alerts must be terminated automatically after the expiration period; however, alerts are retained for no longer than necessary for the purpose for which they were published (i.e. when the purpose has been achieved), even if the validity period is not expired.
- Luxembourg: The police executes orders of the judicial authorities. It can at any moment ask if an alert is to be upheld. As pointed out, the judiciary is not obliged and can't be obliged to give justifications to the police. Review once a year at SIRENE level.
- The Netherlands: No specific procedures/instructions. Review once a year.
- Greece: No specific procedures/instructions. Review once a year.
- Poland: Such evaluation is conducted by the authority issuing an alert before the lapse of one year since issuing of the alert. Such evaluation is also conducted by the Police before expiry of one year since issuing of the alert. This obligation of the Police results from §13 of the Decision by the Commandant-in-Chief of the Police of 21/12/09.
- Slovakia: Yes. Monitoring carried out no later than 1 year after the day of making the request for monitoring both in the Slovak territory and in contracting parties and affiliated countries of the CISA. Monitoring will be finished after lapse of term of 1 year **or** if the requesting police unit, or another public body, requests cancellation of monitoring because the reasons no longer stand or the search for a person/vehicle has been started. Monitoring may be prolonged at most twice; total time of monitoring can't be longer than 3 years. Prolongation of the monitoring is accomplished on the basis of a written request of the requesting police unit or other public body; request has to be submitted no later than 5 days before expiration of monitoring. If further monitoring is needed after expiration of 3-year term, the requesting police unit or other public body must submit a new monitoring request. Review takes place continuously.
- Spain: Yes, the procedures are as described above. review takes place at least once a year.
- Malta: According to current practices, alerts are reviewed 1 month before expiry of the 1-year period. Art. 99 alerts are reviewed at least once a year. Earlier review possible on

request of the investigating officer(s) or on the basis of new information on the circumstances of the case.

- Latvia: No, there are no such procedures/instructions. By the Law obligation to follow to necessity to achieve the purpose and to maintain the alert is put to the responsibility of official of the authority who entered the alert into the System. It is stated in Art.11 of the Law on Operation of SIS that if the necessity to achieve the purpose, due to which the alert has been entered in the System, has ceased or it is not possible to ensure the achievement thereof, the officials referred to in Section 7 of this Law shall immediately revoke the decision regarding entering the alert in the System, as well as shall delete the alert in the System or shall inform regarding it the relevant institution or authority that is responsible for the deletion of the alert. Review is done on a case by case basis as it depends on goals to be achieved and intelligence.
- Belgium: Art. 99 alerts are issued for a 3-month to one-year term. The need to maintain the alert is assessed when the expiry date approaches. This review of the necessity and lawfulness of the alert therefore takes place at least yearly, but there is no specific written procedure imposing a review at regular intervals.
- Italy: Apart from the SIRENE manual, there is the User's manual and administrative Acts (circolari). No specific procedure for review frequency.

C. i) Are there procedures/instructions on how to review the alert? ii) Is there a procedure obliging the search for information available to the alerting authority in other law enforcement data processing systems, including Europol's systems?

- Denmark: According to the Danish SIRENE Bureau's guidelines the bureau asks the requesting authorities to review if the alerts are still necessary. The Danish SIRENE Bureau also performs a check in regards to law enforcement data processing systems.
- Estonia: Yes, see answer to 1D.
- Greece: See answer to 1D.
- Sweden: See answer to 2A.
- Iceland, Spain: See answer to 1A and 1D.
- Finland: The SIRENE office's internal instructions describe the alert review procedure. There is a procedure obliging the search for available information, the information systems are checked by the SIRENE office.
- Italy: Article 112 of the Convention is followed. There do not seem to be any official instruments/documents although in general if the alert is based on a specific request (such as a security measure or a ban) what happens to the latter has an influence on the maintaining or not of the first.
- Slovenia: Yes, within the Slovenian Police Code and the Professional guidance of work on the International Police Cooperation Section.
- Hungary: (i) The internal decree issued by the Criminal Director of the National Police clearly defines the cases of maintaining an alert. (ii) There is no such a mandatory procedure in place.

- Austria: (i) Yes. The services issuing the alerts have to review, whether the requirements (reasons) for the alert are still met. (ii) Alerts and the use of systems such as the national police information system EKIS, SIS, EUROPOL and INTERPOL, are regulated by internal provisions such as FIV 2009.
- Luxembourg: (i) Only the 'SIRENE Best Practices'. (ii) No.
- Germany: (i) See answer to 2A. We do not know any formal procedure that relates to the review of the alert as to its content. (ii) No; according to police service regulation 384.2, prior to entering an alert into SIS, it has to be verified whether a data set about the person has already been stored in SIS.
- Lithuania: Order no. 5-V-845 of the Police Commissioner General regulates the review of alerts; it also establishes that an alert must be terminated when the purpose for which is it published is achieved. Also see answer to 1D.
- The Netherlands: (i) The NSIS Instruction under 5.2 describes criteria for issuing an alert. (ii) No obligatory procedure; however, they can inform each other following the provisions of the Police Data Act.
- Slovakia: (i) Yes, in the Order of Ministry of Interior Nr. 52/2007 on procedures regarding monitoring of persons and vehicles and in the Order of Ministry of Interior Nr. 53/2007 on procedures regarding the searching of persons and vehicles. As for the alert, there are reviewed the conditions and reasons of its further existence which the unit requesting is responsible for. (ii) Yes, in the Order of Ministry of Interior Nr. 53/2007 on procedures regarding the searching of persons and vehicles.
- Malta: (i) Yes, there are written instructions by the head of SIRENE, regulating the reviewing of alerts. These instructions require SIRENE competent staff to seek advice from the requesting police investigators/National Security Authority and take necessary action accordingly. (ii) No procedure requiring such a search; however, when SIRENE are asked to enter an Art. 99 alert, it is the general practice for staff working at the SIRENE office to consult with the ENU and the National Central Bureau to check whether they have taken already any action regarding a subject. Moreover, prior to entering alerts, a check is always carried out in the police systems to avoid duplicate/competing alerts.
- Belgium, Latvia: No.

3: Where different authorities are responsible for the quality and integrity of data it should be ensured that these different responsibilities are organised and interlinked in such a way that data are kept accurate, up to date and lawful, and that the control of these data is guaranteed.

A. What has been done to ensure this? Which written procedures exist, apart from the SIS Manual?

- Denmark: As mentioned under question 1A, there are guidelines ensuring the quality and integrity of data when handling a request for an Art. 99 alert. There are also, as mentioned

under questions 2A-2C, procedures to ensure the quality and integrity of data when an Art. 99 alert is prolonged.

- Austria: Prior to issuing an alert, the issuing law enforcement authority / service must perform a check in the national police information system (EKIS) and SIS. In the case of diverging data, the data have to be adapted. Another check is performed by the central clearing house (ZCS) which is responsible for data quality. In case data divergences are detected during data transfer, the clearing house has to rectify them and inform the affected services about it. Art. 99 alerts which contradict other alerts are checked by SIRENE.
- Iceland, Spain: See answer to 1A.
- Italy: Internal circular letters have been issued by the Ministry of Home Affairs.
- Greece: From a technical perspective, the competent authority for upholding data quality/integrity is the SIRENE Bureau. In order to maintain those principles they use the Information Security Policy, applicable to all the Hellenic Police IT systems, and the Schengen Manual. They also perform technical checks, e.g. to ensure data entered are within reasonable limits, to avoid entering the same subject twice... From a legal perspective, for each alert, only one authority can be marked as 'requesting authority.' If a request for an identical alert is received from another authority, the SIRENE Bureau brings the two authorities in touch, although only the first one remains as the 'requesting authority.' Also see answers 1C-E
- Estonia: Data are submitted within the scope of surveillance proceedings. Control and supervision of surveillance proceedings is stipulated in Sect.19 of the Surveillance Act.
- Finland: This has been ensured by the cooperation between the authorities concerned. Data controller, together with the other authorities, ensures no erroneous, incomplete or obsolete data are processed. SIRENE office is, for its part, responsible that the information entered into the system is made according to the national SIRENE manual and the separate instructions concerning each type of an alert.
- Lithuania: Order no. 5-V-845 of the Police Commissioner General establishes all procedures and interactions of all competent bodies; this Order is followed by the police, State Security Dept. and State Border Guard Service under the Ministry of Interior.
- Luxembourg: None. Quality and integrity of data are ensured by the judiciary and by police as other investigation and police data.
- Hungary: No such separate authority in place. Alerting authorities are responsible for lawfulness and integrity of the alerts; SIRENE Bureau ensures the alerts are accurate, up to date and controlled lawfully.
- Slovakia: The Order of Ministry of Interior Nr. 52/2007 on procedures regarding monitoring of persons and vehicles and Order of Ministry of Interior Nr. 50/2007 on information system of monitoring of persons and vehicles. Then executive protocols concluded with intelligence agencies of the Slovak Republic. The applicant (requesting unit) is responsible for review of keeping an alert. Applicant also obliged to examine duration of conditions and reasons for which the request for monitoring (discreet surveillance) was submitted. In reasoned cases, the Section of Inspection and Inspection Service of the Ministry of Interior of the Slovak Republic carries out the inspection of data processing. This section performs tasks of an

internal inspection system of the Ministry of Interior of the Slovak Republic (within the competence of the internal DP official).

- Poland: Regulation in this regard is included in Art. 23(4) and Art. 27(2)(3) of the Act on the Participation of the Republic of Poland in SIS and Visa Information. The provisions of the Regulation by the Minister of the Interior and Administration of 13 December 2007 on issuing SIS alerts as well as updating, erasing and searching SIS data through the National IT System (Journal of Laws No. 236, item 1743) also apply in this regard.
- Germany, The Netherlands: see answers to question 1.
- Latvia: None.
- Czech Republic: The only authorised subject to enter the data according Art. 99/2,3 into the SIS is the specialised police unit. The Secret Service, Customs Service and the Inspection of Ministry of Interior could ask this authority to issue data according this Art.. These authorities are then responsible for ensuring that those data are accurate, up-to-date and lawful.
- Slovenia: Only one competent body is responsible for the quality and integrity of the data so connection/coordination is not necessary.
- Sweden: The Swedish SIRENE bureau is the only authority allowed to enter alerts in the SIS, including Art. 99 alerts.
- Malta: National SIRENE office is the sole authority responsible for entering Art. 99 alerts in SIS and for checking the quality and integrity of such data. Information is only entered after appropriate verifications take place. In view of this, no specific written procedures are considered necessary on the matter of responsibilities for data quality and integrity.
- Belgium: All police and judicial authorities that have a permanent service (24/7) may introduce an Art. 99 Alert. The authority having requested the introduction of such an alert is responsible for the quality and the integrity of the data. SIRENE will check if a national alert (measure to be taken against the person) exists and if the offence leading to the alert request is part of the scope of the European arrest warrant.

B. Is there a procedure obliging courts and public prosecutors or investigating judges to inform the police (the investigating authority that sent the information to the authorities referred to) about their final conclusions in a specific case or concerning a specific person?

- Denmark, Hungary, Latvia, Spain: No.
- Estonia: Yes.
- Finland: The authorities transmit and exchange information when they notice a need to ensure the questions mentioned above in answer to 3A.
- Slovakia: Within the frame of mutual cooperation of law enforcement authorities, there is mutual exchange of information, which is relevant for particular authorities in order to set the proper measures for successfully finalising the case.

- Luxembourg: No. Such a system raises problems in the Luxembourg criminal proceeding rules.
- Austria, Germany, Greece, Italy, Lithuania, The Netherlands: see answers to 1B.
- Iceland: See answer to 1A and 1B.
- Malta, Slovenia, Sweden: Not applicable to national scenario as only one competent body exists.
- Belgium: See answers to questions related to recommendation 2.

C. Is there a procedure obliging police or other investigating authorities to inform each other when they should suspect that their information is of relevance for assessing the conditions for the Art. 99 alert?

- Denmark, Latvia, Hungary, Luxembourg: No.
- Estonia, Germany, Greece, Italy, Lithuania, Slovakia, The Netherlands: See answers to 1C.
- Finland: See answers to 3A-B.
- Slovenia, Malta: Not applicable to national scenario as only one competent body exists.
- Belgium: See answers to questions related to recommendation 2.
- Austria: Obligations to inform other authorities are set out in the FIV 2009 and particular reporting provisions, according to which other authorities must be notified in the case of a hit or a CID case of special importance.
- Iceland, Spain (yes): See answer to 1A.

D. Is there a procedure obliging an authority intending to use an Art. 99 alert to check the conditions of Art. 99 not only with its own files but also with other law enforcement information, including Europol's information systems?

- Denmark: No, but the SIRENE bureau will perform such a check.
- Hungary, Latvia, Luxembourg: No.
- Estonia, Germany, Greece, Finland, Italy, Lithuania, The Netherlands, Slovakia, Spain: See answers to 1D.
- Belgium: See answers to questions related to recommendation 2.
- Iceland: See answer to 1A.
- Slovenia, Malta: Not applicable to national scenario as only one competent body exists.
- Austria: The use of individual systems such as SIS, Interpol and Europol is laid down in internal provisions such as FIV 2009.

**E. Are there procedures/instructions to assess - after a hit of the Art. 99 alert - if:
i) the data are relevant and can be used in the investigation; ii) irrelevant data are deleted; iii)
and that the data are used to assess the lawfulness of maintaining the alert?**

- Denmark, Estonia, Finland, Germany, Greece, Italy, Lithuania, Slovakia, The Netherlands: See answers to 1E.
- Belgium: See answers to questions related to recommendation 2.
- Iceland: See answer to 1A.
- Hungary, Latvia, Luxembourg: No.
- Austria: Data use, deletion and correction are regulated in the national provisions, especially FIV 2009, SPG and DSG.
- Spain: No formal procedures: the requesting authority is entirely responsible for both entering the data and assessing relevance of the data and lawfulness of the alert.
- Slovenia, Malta: Not applicable to national scenario as only one competent body exists.