COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 21.4.2006
COM(2006) 167 final

REPORT FROM THE COMMISSION

on the operation Council Common Position 2005/69/JHA

{SEC(2006) 502}

REPORT FROM THE COMMISSION

on the operation Council Common Position 2005/69/JHA

INTRODUCTION

On 25th March 2004, the European Council, through its Declaration on combating terrorism, instructed the Council to take forward work on the creation of an integrated system for the exchange of information on lost and stolen passports having recourse to the Schengen Information System ("SIS") and the Interpol database.

As a result the Council issued Common Position 2005/69/JHA as a first response to that request, and it was envisaged that this would be followed up by the establishment of the technical functionality in SIS II to achieve that aim.

The Common Position obliges Member States to ensure that their competent authorities exchange data on issued and blank passports that are stolen, lost or misappropriated and formatted for integration in a specific information system, whilst at the same time ensuring that the fundamental rights of data subjects are respected.

1. KEY REQUIREMENTS OF THE COMMON POSITION

Given the terms of the Common Position, the Commission has identified 5 distinct obligations that have been placed upon the Member States:

- To exchange all present and future passport data (as defined) with Interpol
- To only share such data with Interpol members that have an adequate level of protection for personal data and to respect the fundamental rights and liberties regarding the automatic processing of personal data
- To ensure that such data is exchanged with Interpol immediately after it has been entered into the national database or SIS
- To ensure that their competent law authorities use the Interpol database to access such information when appropriate for performance of their task;
- To ensure that they set up relevant infrastructures to facilitate consultation by December 2005 at the latest.

2. PURPOSE OF THE REPORT AND METHOD OF EVALUATION

As a result of Article 4 of the Common Position, the European Commission has been instructed to submit a report to the Council on the operation of the Common Position within the Member States.

On the basis of this report, the Council is to assess the extent to which Member States have complied with the Common Position and take appropriate action.

Pursuant to this task, on 3rd August 2005 the Commission sent a questionnaire to all 25 Member States. This questionnaire was designed to produce answers which would help ascertain the extent, mode and method of operation of the Common Position.

Only 17 Member States returned answers to this questionnaire.

Responses were received from:

Austria	Belgium	Czech Rep.	Estonia	Finland
Germany	Spain	Italy	Lithuania	Luxembourg
Netherlands	Portugal	Slovenia	Slovak Rep.	United Kingdom
Poland	Latvia			

Responses were not received from:

Denmark	Greece	France	Ireland	Cyprus
Hungary	Malta	Sweden		

It should be noted that this report is submitted mindful of the requirement in Article 4 of the Common Position that the Commission provides the Council with a report by December 2005. As a result it is made on the basis of a majority cross-section of the Member States, rather than a complete collection of responses from all 25 Member States.

The quality of the national information received by the Commission inevitably influences the quality and value of this report. Some of the information received by the Commission was ambiguous, incomplete, makes reference to domestic law and other provisions without providing further details, and has been provided the basis of variable interpretations of the questions asked depending on the Member State in question. Likewise, given the variable interpretations which can be given to the relatively broad terms of the Common Position, it is not always immediately clear from the answers given as to whether implementation of key Articles has taken place, this sometimes being a question of extent rather than an absolute measure.

3. RESPONSE SUMMARIES

3.1. How did your MS implement the Common Position on exchanging certain data with Interpol (2005/69/JHA)?

Responses to this question indicated that Member States were at a variety of stages of operation of the Common Position. The answers demonstrate that, in general at least, there has been decent progress in the operation of the Common Position, albeit not in its entirety. The majority of answers suggest that implementation of the central provisions of Article 3(1) has taken place for many Member States, the central provisions of Art 3(3) have posed a much greater challenge. In most cases, relevant data has been (or is on the point of being)

provided to Interpol. The answers appear to indicate, however, that only a small number of Member States have managed to establish infrastructures for competent law authorities to search relevant Interpol databases.

3.2. Does your MS exchange all passport data (as defined in Article 2(1) of CP 2005/69/JHA) with Interpol as required in Art. 3 (1) of CP 2005/69/JHA?

Out of 17 respondents, 11 exchange passport data with Interpol, whilst 3 of the respondents will be doing so imminently. Those which do not currently exchange such information include Spain, Estonia and Slovakia. The type of data that is exchanged is not always as complete as is required under the Common Position, with Poland, for example only providing data on passports which are lost or stolen as a result of crime.

3.3. 3.2Does your MS pursuant to Art. 3 (3) of CP 2005/69/JHA exchange all passport data immediately also with Interpol after it has been entered in your relevant national data base or the SIS if you participate in it? Please describe your workflows, in particular how you ensure that data is immediately exchanged with Interpol after having been entered into the relevant national data base or SIS.

Very few of the respondents claim to have achieved the *immediate* exchange of data with Interpol. Only 3 Portugal, the Netherlands and Germany claim to have achieved this (though it is in fact unclear that the Netherlands is yet providing information at all), and in the case of Portugal, this is still by means of fax/email. However, 7 Member States exchange information daily, either on the same day that information is received at national level, or the following morning.

3.4. Does your MS distinct between Interpol members to share this data with and those not to share this data with according Art. 3 (1) of the CP 2005/69/JHA? If so, how does your MS distinct? Did you require reciprocity in the data exchange?

Out of 17 respondents, 14 do not distinguish between members of Interpol when exchanging information, and 2 have not yet decided their policy in this regard. This leaves the Netherlands as the only Member State which does distinguish between Interpol members. Such an open approach on the part of the Member States is most likely on the basis of their being no exchange of *personal*/*nominal* information – a factor pointed out by the UK, Germany, Portugal and the Czech Republic. If searches of non-personal information on the Interpol database give rise to requests for further, personal information, Member States are likely to be more discriminating in who they give this to. In the case of the UK, for example, it is noted that once information exchange did involve the exchange of personal information, each individual request would be risk assessed before such information was handed over.

In terms of reciprocity, only 2 out of 17 respondents (Portugal and Slovakia) state that they require, or would require, reciprocity of exchange. Portugal's response makes it clear that such reciprocity would only be required in relation to the bilateral exchange of nominal information, following an information 'hit' by the searching party of the (non-personal) database information provided to Interpol. Again, this implies that reciprocity is more likely to be a factor in Member States' willingness to exchange information once personal or nominal data is involved.

3.5. What modalities has your MS agreed upon with Interpol for exchanging all passport data in its possession pursuant to Art. 3 (2) of CP 2005/69/JHA?

Out of the 17 respondents, 6 may, subject to the requirements set forth in paragraph 1, agree modalities for exchange with Interpol. Of the remainder, 2 simply cite the Interpol regulations as being the basis for exchange and 2 offer ambiguous answers. Otherwise, cited modalities include:

- exchange according to the Schengen Guidelines (Germany)
- An agreement to exchange using planned real time DATIREL system (Spain)
- Automatic transfer of information from national database to SIS, and thence to Interpol ASF/STD system (Finland)
- Use of the I – 24/7 (Italy and Latvia)
- Ad hoc consultation at a central level (Luxembourg); and
- Provision of information electronically via NCIS to Interpol, and use of I – 24/7 to exchange subsequent sensitive information (UK).

3.6. How does your MS ensure that the competent law enforcement authorities query the Interpol database for the purpose of this CP each time when appropriate for the performance of their tasks according Art. 3 (4) of CP 2005/69/JHA?

Answers given to this question were often of a very non-specific nature, and overall offer an ambiguous general response. Overall, very few Member States seen to have taken positive steps in the implementation of this Article, and where they have, they appear to have been of a relatively lightweight nature.

Cited methods to monitor and regulate this type of data exchange include internal rules and guidelines, provision of information about Interpol and the provision of a code of connection agreement. In many cases, Member States have simply stated the means by which such information can be accessed – for example through central contact points, ASF-mail/e-ASF, access of information via the EASYFORM application and through central contact points.

The nature of the majority of the responses imply that Member States have not given a particularly proactive interpretation to Article 3(4), and for the most part feel that the simple provision of potential access (in one form or another) to competent authorities is sufficient to satisfy the requirement set out in the Article. This seems at odds with the text of the Article, and particularly with Member States' obligation to "*ensure*" law enforcement authorities consult the Interpol database where appropriate.

3.7. How have these competent authorities been defined?

Methods of definition vary, and have been made on the basis of national legislation, national consultations, 'need to know' evaluations, the Interpol Constitution/'Statutes' or have not yet been decided. The range of authorities include:

– Federal Ministry for internal affairs, security directorates and regional administrative bodies and directorates of federal police (Austria)

– Authorities likely to contribute effectively to the prevention and suppression of ordinary law crime (Czech Republic)

– Federal criminal police, federal police directorate and the state offices of relevant Bundeslander. Customs criminological office to be included in future (Germany)

– National contact points or bureaus (Finland, Italy and Luxembourg)

– Those defined according to Interpol standards and national law (Poland)

– All law enforcement authorities including customs (Portugal)

– Police authorities only (Slovenia); and

– All law enforcement agencies or those having a legal requirement to access such data; includes Department for Work & Pensions, Trading Standards (UK).

As such there are a variety of definitions made on a variety of bases. It is clear however that criminal law enforcement authorities (as the term is generally understood), will have access to exchange information-even if such access is only of an indirect nature (i.e. through central contact points).

3.8. Has your MS developed guidance on the cases where consultation of the Interpol database is deemed appropriate?

Out of the 17 respondents, 12 appear to have not developed such guidance (though of these, 4 appear to be planning to do so in future, whilst 7 give the impression that the development of such guidance is neither necessary nor planned). The answers given by four of the Member States are unclear as to whether such guidance has been developed, or whether it is considered necessary. The nature of the answers given by these Member States seem to imply that the simple fact of potential availability satisfies any need for law enforcement authorities to be trained or guided in the use of the Interpol database. Only 1 of the 17 respondents (the UK) has developed specific guidance and training in this respect.

As such, it again appears that the Member States, in general, are not taking a particularly proactive line in terms of training their law enforcement authorities. The development of guidance and training for law enforcement authorities does not seem to be considered necessary by the majority for satisfaction of the general requirement set out in Article 3(3).

3.9. Has your MS already set up the infrastructure required to facilitate consultation according Art. 3(4) of the CP 2005/69/JHA)? If so, how does it look like?

Out of the 17 respondents, 7 state that they are in the process of developing or implementing such infrastructures. The answers given by 6 Member States do not make it clear as to whether such infrastructures have been developed or not. It appears that 4 Member States (UK, Belgium, Germany and Luxembourg) have established such infrastructures.

Given the stated intentions of the largest part of the respondents, as well as the structures put in place by the UK, Belgium, Germany and Luxembourg, it is clear that the majority of Member States are taking active steps to satisfy this particular requirement. Of the remaining Member States, some of the answers seem to imply a very non-demanding interpretation of what is meant by Article 3(4).

3.10. How does your MS ensure an adequate level of protection of personal data in the relevant Interpol member country and the respect of fundamental rights and liberties regarding the automatic processing of personal data?

Out of 17 respondents, 9 cite domestic (and/or international) data protection as forming the basis of protection for the exchange of such information. The fact that no personal data is exchanged is cited by a further 5 Member States. Austria is still in negotiation with Interpol over this issue, the Netherlands protects its data by restricting access to it, and no answer was received from Italy.

3.11. How does your MS ensure that if a positive identification (hit) occurs against the Interpol database the competent authorities take action in accordance with their national law?

The respondents have taken two different interpretations of this question. On the one hand some respondents have answered on the basis that they thought the question was focusing on their own ability to ensure they respond to hits made by others. Others Member States answered on the basis that they thought the question was focusing upon how they could ensure other Member States responded promptly when there was a hit.

Of those looking at their own internal ability to respond effectively, the types of methods used included:

- the use of strict internal rules and procedures
- the development of verification procedures with BCN operators
- automatic hit indicators
- involving OCNs in the process; and
- NCI control and verification.

The most commonly cited method of ensuring follow-up of information was vaguely defined internal procedures and maintenance of proper standards. This again suggests a less than proactive approach in this area. Of those looking at the ability of other Member States to follow up a 'hit' with the appropriate information, the following approaches were taken:

- the taking into account of inappropriate actions in future dealings
- that the Interpol regulations would be relied upon; and
- demands for explanations and comments if a hit takes place.

In the light of the responses, the use of internal procedures and automated 'hit' alarms will play the lead role in terms of ensuring internal effectiveness in following up 'hits'. In terms of

the external context (i.e. measures to ensure timely responses by external actors), those Member States that fail to provide information in due course are likely to be subject to informal sanctions or demands.

4. CONCLUSIONS-SPECIFIC

In order to provide a general overview of the operation of the Common Decision, it is again necessary to return to the 5 core obligations identified

4.1. To exchange all present and future passport data (as defined) with Interpol.

Given the positive responses of 11 out of 17 of the respondents, and the imminent involvement of 3 more, there appears to have been solid progress in the exchange of Interpol of national data. Those which have not exchanged data with Interpol (Spain, Estonia and Slovakia) have not provided explanations as to why such implementation has not taken place.

The relative success of Member States in implementing this part of the Common Position perhaps reflects a perception that this is the core obligation placed on the Member States – and one that must be satisfied if any particular Member State is to be recognised as implementing the Common Position. One potential area that attention should be paid to in this relatively successful area of exchange is the definition of passport data. Article 2(1) calls for the exchange of "*issued and blank passports that are stolen, lost or misappropriated*". In some cases Member States exceed this requirement by providing, for example, information on ID cards and driving licenses. This in itself is no bad thing, and indeed is desirable given the relatively free ability to travel within the EU using ID cards only. On the other hand however, Poland exchanges passport information, but only in respect of those lost or stolen as a result of crime. It is logical that a passport lost as a result of absent mindedness potentially presents just as many dangers to the security of the Union as one that is stolen. As such, attention should be paid that the definition in Article 2(1) is adhered to by Member States, as gaps in the type of information being exchanged could be critical.

Despite the fact that not all Member States have responded to the questionnaire sent by the Commission, Interpol notes that 18 of the 25 Member States are currently participating in the stolen travel document database. According to Interpol information Austria, Denmark, Hungary, Latvia, the Netherlands, Slovakia and Sweden are not yet contributing to the database. Interpol notes that some of these Member States are extremely close to taking part in exchange, though are currently in negotiation or in the process of implementation.

The fact that for the most part the Member States have satisfied this vital requirement is reflected in Interpol figures, which show that data from the EU states relating to 6,394,305 lost or missing travel documents were provided to the Interpol database. This compares to a figure of 2,449,300 *for all other* participants in Interpol – making the EU the greatest contributor of data by far. [1] In 2002, the figure for the EU stood at 783. This demonstrates the huge growth in participation in this system, as well as the key role that EU states now play in enhancing Interpol's capabilities.

[1] Figures as at 23rd November 2005.

4.2. To only share such data with Interpol members that have an adequate level of protection for personal data.

Ensuring that other Interpol participants have adequate data protection measures in place is problematic for Member States. In most situations, contribution to or consultation of the Interpol STD database will not result in any exchange of personal data except for passport numbers of issued passports[2], thanks to the definition of 'passport data' under Article 2(1) of the Common Position. On the face of it, this means that there is reduced necessity for data protection measures *at this stage of* the information exchange – a point made by several Member States in their answers to the questionnaire. This is unless some of the Member States actually contribute personal data to Interpol's STD database – in which case an explicit means of data protection is necessary. It should be noted that the majority of Member States have indicated that they do not consider passport numbers to constitute 'personal data'.

In only one case (the Netherlands) does a Member State definitely discriminate as to whom they share data with. Two other Member States are yet to decide this. This shows great willingness on the part of the Member States to be relatively free with exchange of their data, and a certain disinterest as to whether or not the states they share data with have adequate personal data protection in place or not. Where no personal data is actually exchanged in the initial phases of a data query, then it seems quite fair that this should be so. Thus several Member States make the explicit note that there is no discrimination because contributions to the Interpol STD database does not in itself involve the exchange of personal information.

What is again left relatively mute, however, is whether such discrimination takes place once a 'hit' has been made on the Interpol STD database, and the actual personal data attached to that 'hit' then comes to be exchanged. The responses of the UK and Portugal allude to this situation, and note that each request for information would either be risk assessed before the dissemination of personal data (in the case of the UK), or would be subject to relevant data protections provisions, the 'need to know' and reciprocity (in the case of Portugal). This is likely to be the type of approach taken by most Member States had the question been specifically aimed at the post STD system 'hit' stage of personal data exchange.

4.3. To ensure that such data is exchanged with Interpol immediately after it has been entered into the national database of SIS.

This has been a relatively poor area of performance in terms of Member States ensuring that Interpol is immediately furnished with the relevant data as soon as it has been entered on the national database or SIS. It is true that a good proportion of the Member States are exchanging this information within 24 hours, which, on the face of it, demonstrates a respectable administrative turnover. It should be noted however that in the realm of law enforcement, time is absolutely of the essence; particularly when it comes to regulating of unauthorised persons across borders. The longer it takes for information to become available, the less its value is. As such, it is still advisable to stress the nature of the obligation, and the reasoning behind the explicit demand for *immediate* information. The fact that immediate exchange is possible has been demonstrated by Portugal, the Netherlands and Germany. Likewise, the fact that Portugal manages to do this through the simple use of email and/or fax

---

[2] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

demonstrates that this kind of speedy information exchange can take place without expensive and sophisticated information technology systems.

It is in all Member States' interest that exchange with Interpol takes place as soon as possible, as this will enhance the value of the information, and collectively the value of the entire exchange mechanism, to the advantage of all.

4.4. To ensure that their competent law authorities use the Interpol database to access such information when appropriate for performance of their task.

This has been one of the weakest areas of response, with Member States reflecting a prevailing attitude that by simply providing access to the Interpol database, whether directly or indirectly, to its law enforcement authorities, they are 'ensuring' that this valuable information resource is in fact used. The language of the Common Position seems to imply a more stringent and pro-active approach, which outs in place systems whereby use of the Interpol database can at the very least be encouraged amongst law enforcement officers.

Where measures have been taken, they are of a relatively lightweight nature – for example through simply informing officers that this information is potentially available. Most Member States have simply left this point mute and instead set out the means by which they have made information available. This perhaps implies that once means of exchange have been put in place, no action has been taken in respect of making sure people actually use it. If people do not actually use the Interpol database, and it is effectively forgotten by rank and file officers, then it could seriously compromise the exploitation of the true utility of this very valuable information resource. As such it is surely advisable that Member States establish firm rules as to the use of the STD database, and remain constantly vigilant in ensuring these rules are being followed.

One other, potentially less onerous, way to improve the situation is the provision of education and guidance on the subject. Again, however, Member States have not been very proactive, with the clear majority not yet having developed any guidance on this subject, and almost half of the Member States not viewing such guidance as necessary in any case. Only the UK has felt the need to formulate explicit guidance of this nature.

The lack of action in this area is puzzling, as the Interpol STD database offers potentially important advantages to national law enforcement authorities, particularly in the key areas of organised crime, illegal immigration and terrorism. It is in the Member States' own interest that they should take a more proactive line on this.

Interpol figures show that despite the EU being the biggest contributor of information to the lost travel document database, it carries out only a small proportion of the searches – 8520 in 2005 as opposed to a total number of searches of 43,316. On a more positive note, Member States performed only 3955 in 2004, so there has clearly been a positive movement in terms of database use in the intervening period. That the Member States using the database get a positive return for their effort is perhaps reflect by the fact that in 2005, despite their small relative portion of total searches, EU searches resulted in 381 positive 'hits' as opposed to 457 'hits' coming about as a result of non-EU searches.

4.5. To ensure that they set up relevant infrastructures to facilitate consultation by December 2005 at the latest.

As far as can be gleaned from the answers to the questionnaire, only Belgium, Germany, Luxembourg and the UK have actually managed to meet this obligation. Seven of the remaining Member States claim that they are on the point of satisfying this requirement – because they are in the very process of developing it, or they are implementing it at the moment. Given that this is probably one of the more expensive and complicated obligations contained in the Common Position, it is understandable that progress has been slower than the simple handover of information to Interpol. It remains, however, an ostensible failure on the part of a large proportion of the Member States to put in place concrete infrastructure to let authorities get maximum value from the Interpol consultation facility. What remains unclear from the remaining answers is how many Member States have not satisfied this requirement at all, and who have not intention of doing so in the immediate future either. This position certainly requires further clarification on the part of the Member States.

CONCLUSION-GENERAL

The Member States have largely abided by the spirit of the Common Position, mainly through satisfaction of the most visible and in many ways easiest to fulfil requirement – the furnishing of the Interpol STD database with national information. Operation of the Common Position in the fullest sense of the term, however, is still incomplete and requires a more proactive, comprehensive and energetic effort on the part of the Member States to bring about the kind of operation that will offer all of the Member States maximum return from their participation in the exchange of information with Interpol.

Before the Common Position was implemented, data relating to 4,567,267 entries from EU Member States was entered on the Interpol STD database. After introduction of the Common Position these figures have risen to 6,394,305 and 18 respectively.[3] Likewise EU searches of the database rose from 3955 to 8520 over the same period, and the number of 'hits' rose from 173 to 381. Clearly there has been some progress, but arguably these increases still do not represent the optimal participation of the EU in the Interpol Stolen Travel Document database – to reach it, still greater commitment is required from some of the Member States.

The tenor of this report of the Commission has been kept because it describes the situation at the time of drafting (end of 2005). Meanwhile the Commission has received information, among others through a joint visit EU/US to the Secretariat General of the ICPO Interpol in January 2006 that the operation of the Common Position has considerably improved.

Interpol informed the participants of the joint EU (PRES/COM) / US – visit to SG ICPO in Lyon on 25 January 2006 that all Member States had exchanged lost and stolen passport data with Interpol or had at least taken concrete measures in order to do so in the near future. In February 2006 the Secretariat General of the ICPO-Interpol provided up to date statistics that show an improvement of the situation in particular as regards searches carried out by the Member States in the Interpol Stolen Travel Document database.

[3] Figures as at 23rd November 2005

Date from February 2006 it can be stated that before the Council Common Position was implemented, data relating to 4,567,267 entries from 15 EU Member States was entered on the Interpol STD database. After introduction of the Common Position these figures have risen to 7,790,792 and 21 respectively in the end of 2005.

According to these latest statistics from Interpol, Member States carried out 9087 searches in 2005 (3955 in 2004) as opposed to a total number of 211 033 (43 316 in 2004) searches globally.