COUNCIL OF THE EUROPEAN UNION

Brussels, 15 May 2009

9604/09

LIMITE

ENFOPOL 108
EUROPOL 27

NOTE

from:	Europol
to:	Delegations
Subject:	Report to the Council on the use of personal data in the Check the Web project

Delegations will find in annex a report by Europol on the use of personal data in the Check the Web project as a response to the request in the Council Conclusions on the continuation of work on combating terrorism adopted by the Justice and Home Affairs Council on 27-28 November 2008. The Council Conclusions invited Europol to report by the end of April 2009 on how to increase the dissemination of personal data in order to make the best use of the Check the Web portal.

EUROPOL

The Hague, 27 April 2009

Director

To: Mr Ivan Langer
Chairman of the JHA Council

Copy: Mr Viktor Čech
Chairman of the Europol Management

Dear Mr Langer,

You will find enclosed the Europol report on the use of personal data in the Check the Web project. This report follows the request made by the Council in its Conclusions on the continuation of work on combating terrorism adopted on 14 November 2008 (doc. 15684/08 JAI 638 ENFOPOL 228).

I am pleased to report that solutions have been identified in order to store, search, process and also analyse personal data in the framework of the Check The Web project. I am convinced this represents a significant step forward in the fight against terrorist propaganda on internet.

Europol will continue working on the implementation of these new possibilities in close consultation with the Europol Management Board and the Europol Joint Supervisory Body.

Yours sincerely,

Rob Wainwright

Director

Annex: Europol report to the Council on *"how to increase dissemination of personal data to fight Islamist extremist propaganda on the Internet* (file no.2566-476)

File no. 2566-477 (389968-v1)

Raamweg 47, The Hague
The Netherlands

PO Box 90850
NL - 2509 LW The Hague

31 (0)70 302 5000
31 (0)70 345 5896

EUROPOL

The Hague, 27 April 2009

File nº2566-476

Report to the Council

How to increase dissemination of personal data to fight Islamist extremist propaganda on the Internet

INTRODUCTION

During the first semester of 2007, the German Presidency of the European Union described the following initiative in their programme:

"*To fight terrorist threats, the Presidency will press for a form of cooperation between all security authorities involved in Internet surveillance in the Member States, in consultation with Europol.*"[1]

The Check the Web project was born and Europol had the responsibility to develop a portal to facilitate the exchange of information on Islamist extremist propaganda on the Internet. The portal's name is the Check the Web portal (CTW). It was deployed in June 2007. In February 2009 the CTW project team deployed a second version of the portal which offers additional functionalities to its users.

1 Presidency programme, title page 17: Strengthening security controlling migration and promoting integration, subtitle: Close cooperation and a united front in the fight against terrorism, Paragraph 4

In November 2008, the Council requested Europol to "r*eport to the Council on how to increase dissemination of personal data in order to make the best use of this secure information portal"*[1].

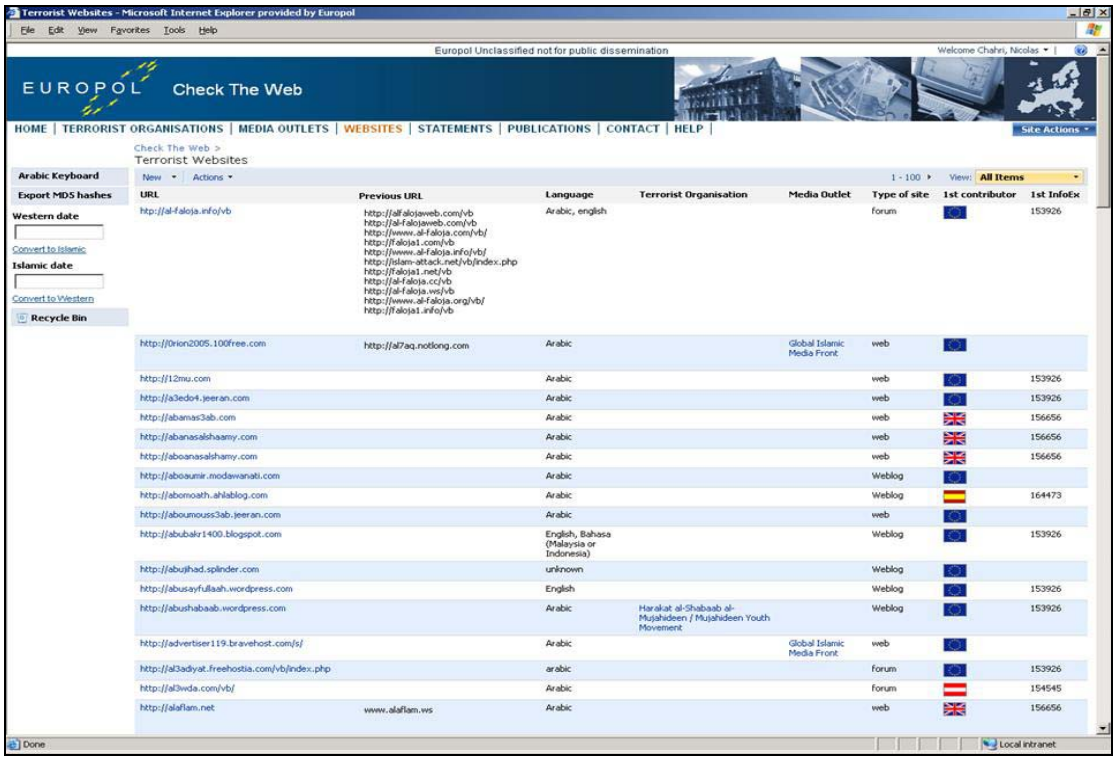
DESCRIPTION OF THE CHECK THE WEB PORTAL

The project aims to create an electronic portal, to be hosted by Europol, for storing information regarding Islamist extremist websites and statements of terrorist organisations published on the Internet, with the objective to put that information at the disposal of the 27 Member States' (MS) competent authorities

The portal is hosted on the Europol secure Intranet network. It is accessible by the counter terrorism competent authorities of the MS (view access only). It presents five topics that the competent authorities can access and use for law enforcement purposes:

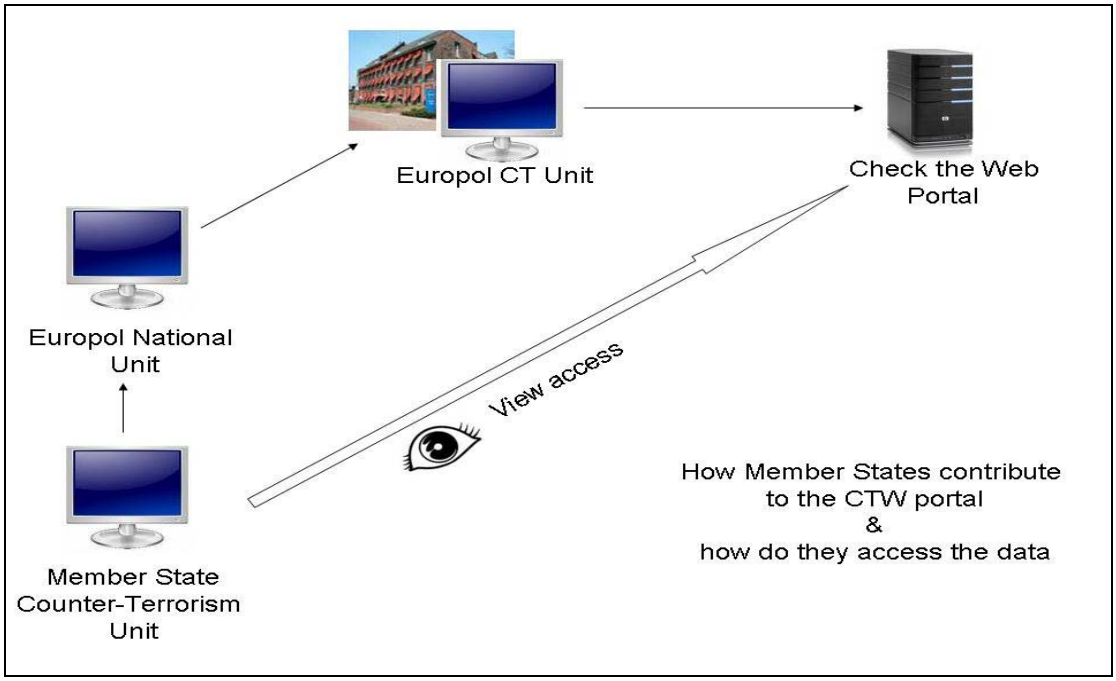
- a list of Islamist extremist websites, with the corresponding URLs;
- a list of statements of terrorist organisations, with translations when available;
- a list of Islamist extremist magazines, with translations of their tables of contents when available;
- a list of terrorist organisations;
- a list of contact points in EU Member States and at Europol.

[1] Doc. 15684/08 JAI 638, ENFOPOL 228 Council conclusions on the continuation of work on combating terrorism, page 5



(Screenshot of the check the Web portal)

Designated officers within Europol's Counter Terrorism Unit (SC5) are responsible for managing the content of the portal and are the only ones with full access rights.



(The flow of information between MS and Europol with CTW)

MS send their contributions to Europol. The content managers of the Europol's Counter Terrorism (CT) unit will then upload this information on the portal. Authorised users in the Member States and at Europol have read-only access rights to the contents of the portal.

On 20 February 2009, a new and improved version of the CTW portal was made available to the Member States. The new portal offers additional features including the possibility to compare documents seized on computers of perpetrators with the content of Check the Web by means of crosschecking hash codes.

DATA PROTECTION RELATED BACKGROUND

The portal has generated expectations in the Member States which cannot easily be aligned with the current legal framework. As a general rule, Europol can only process personal data within computerised systems as referred to in Articles 6 and 6a of the Europol Convention (*see Annex 1*).

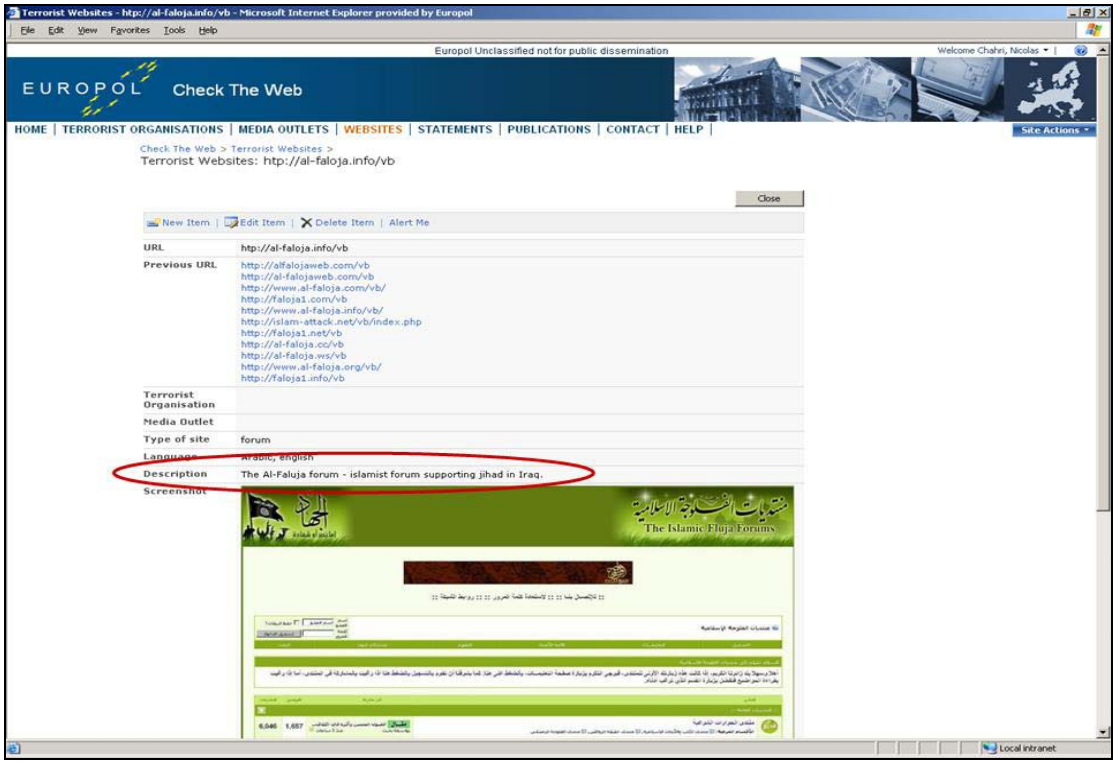
Europol's Joint Supervisory Body (JSB) therefore suggested at the very beginning of the development of CTW to legally embed the portal into an Analysis Work File (AWF) environment. The setup of CTW as an AWF was, however, not favoured at the time since the portal was originally foreseen as an Internet portal providing access to a wide law enforcement community. In addition, view access to AWFs from MS was at the time technically not feasible.

This is why an exception was agreed upon with the JSB in order to establish CTW outside the environment provided for in Articles 6 and 6a of the Europol Convention, to the extent that only personal data which are already publicly accessible are processed.

The assumption that no personal data could be processed on CTW was thus at no point correct. Personal data were processed in various forms on CTW from the beginning: as part of the displayed websites, in statements of terrorist organisations and in any other form of publication available on CTW. The JSB, however, emphasised that CTW must not be used for any processing that properly comes within the scope of the Europol computerised systems as referred to in Article 6 of the Europol Convention (Information System, AWFs, Index System) and 6a of the Europol Convention (processing data for the purpose of determining whether such data are relevant for Europol's tasks).

BROADENED POSSIBILITIES UNDER CURRENT SETUP

The issue Europol faced regarding the processing of personal data on CTW related to the free text field only. A high risk was perceived that users would use the freetext field not only to summarise the open source material as such, but also to include background knowledge, from other police files or from ongoing investigations, which is not publicly accessible. The solution to that problem – identified at the time the portal was built – was that no personal data should be entered in the free text field.



(Screenshot of the free text field in the topic "websites" of the Check the Web portal)

Experience has meanwhile shown that this approach does not suit operational needs. Furthermore, auditing mechanisms have been implemented which enable a reasonable mitigation of the risk outlined above.

In this context, Europol has explored the possibilities to process personal data on CTW as it is currently setup. A distinction is now made between "analysis" on the one hand and "summaries of open sources" on the other. Europol has - as a first step - adjusted the Use Policy in order to reflect this distinction (*see Annex 2*).

A pure summary of open source material does not come within the scope of the AWFs, even if it is extensive and contains personal data. The only precondition is that no information from police files or investigations which is not publicly accessible shall be entered in the free text fields. Such pure summaries of open source material are treated like the open source material itself and can therefore be processed on CTW.

However, the processing of "analysis" on CTW – in the form of establishing links between open source information on the one hand and non-publicly accessible information stemming from police files or ongoing investigations on the other – remains prohibited because it comes within the scope of the AWFs as long as the current setup is applied. This approach was subsequently consulted with and supported by the JSB.

FUTURE OBJECTIVE: FULLY FLEDGED ANALYSIS ON CTW

The objective is to exchange fully fledged assessments and analysis on the portal.

To this end, Europol is exploring the possibility to embed CTW into the legal environment of Article 10 of the Europol Convention (*see Annex 3*) and the related implementing rules. This approach has recently been encouraged by the JSB in a first provisional response to a request from Europol (*see Annex 4*).

Added value and feasibility

Since the web portal would be legally embedded in the framework of Article 10 of the Europol Convention, the storage, processing and even analysis of personal data on the portal would become possible, including the possibility to share analysis data and results and to search for personal data on the portal. This will allow the exchange of analysis results and assessments via the portal and thus transform CTW into a meaningful tool with real added value for the Member States.

Direct access from Member States is already legally foreseen. Article 10(2), second sub-paragraph, which was added to the Convention by the "Danish Protocol", provides that *"...all participants may retrieve data from the file"*. The future CTW could be the first example where this new provision would be applied in practice, by allowing all participants to retrieve data from the CTW legally set up in an AWF environment, i.e. to have view access to the portal. The access to the portal would be considered as an implementation of the (direct) access that analysis group participants have on the basis of Article 10. CTW could thereby remain a tool in which all 27 Member States participate.

Implications for Users

The procedural implications connected to this new legal environment appear manageable and would not cause considerable constraints in practice. The Europol Director would have to sign an opening order for the portal in accordance with Art. 12 Europol Convention, including the drawing up of a data collection plan.

The counter terrorism officials using CTW would need to be nominated as experts for this new file under the regime of Article 10 of the Europol Convention. The number of experts to be nominated might vary depending on the needs of the respective Member States. There is no legal provision limiting the number of experts.

As far as the use of the information put on the portal is concerned, Article 10(8) would apply, which means that the Member State that provided the information would have to give its consent before it can be used by other participants. However, Member States could give general consent for all the information they provide to the portal. According to this general agreement, information submitted to be included in the portal could be used by all other participants. Given such a general consent, in practice nothing would change as compared to the current situation in this regard.

The time limits for examination and duration of storage as laid down in Article 21 of the Convention would need to be adhered to (*see Annex 5*). This basically means that the necessity of storage would form the decisive element, which would in fact not constitute a restriction negatively affecting operational business.

It should be mentioned that the set-up of the portal within an Article 10 Europol Convention environment would also, at least from a legal point of view, open up the possibility provided for in Article 10(9) of the Convention, i.e. the association of third parties with whom Europol has concluded an operational cooperation agreement, on the condition that all participants agree. However, it must be clearly understood that this would not open up the possibility under Article 10(2) to have view access to the portal, since that provision applies to participants of the analysis group only (as opposed to associated parties). It would remain to be seen if this legal option would ever be implemented in practice, given the fact that all 27 MS would have to unanimously agree on the association of any third party.

Technical adjustments to the current IT system

The amount of work involved in implementing changes will depend on the number and complexity of new business requirements. In case no new requirements or minimal impact requirements are requested when CTW is moved into the Article 10 Europol Convention framework, this will not necessitate major technical adjustments to the current CTW portal system. Examples of areas where there might be new requirements are auditing and data retention policy.

Depending on the requirements, and whether they will be implemented as business policies and procedures or as technical changes, the technical impact will be further studied and estimated.

Communication aspects

Law enforcement officials might have a certain image in mind of what an AWF actually is. Even though CTW would be legally embedded into an Article 10 Europol Convention framework, i.e. an AWF environment, the new portal would not necessarily have to be referred to as an AWF (AWF CTW) given that this might trigger confusion at the operational level.

ISSUES INHERENT TO FURTHER ALTERNATIVES

Europol has also considered other alternatives. From Europol's perspective these other alternatives offer less advantages than the solution proposed above.

New information system under the Europol Council Decision

The potential future legal framework under the Europol Council Decision (ECD) should be considered very carefully: according to Article 10(3) of the ECD, no processing of sensitive personal data such as political opinions and philosophical beliefs will be possible within the so-called "new systems" (*see Annex 6*). CTW could not operate without these kinds of data.

Europol as a technical platform provider

If Europol was only contributing the technical platform to the Member States, Europol could no longer contribute to the content of CTW. Referring to statistics, by far the strongest contributor of content to the portal would be cut off (*see Annex 7*).

Such an approach would furthermore trigger uncertainty on the applicable data protection legal framework. It would, in particular, be unclear which data protection regime would be applied, which retention periods would be adhered to and who would bear the data protection responsibility for content entailing contributions of several Member States, for example in the free text field.

If analysis is the ultimate aim, the respective – existing – legal framework should be applied, namely Article 10 of the Europol Convention and its implementing rules.

CONCLUSIONS

Europol has identified possibilities to process personal data in CTW as it is currently set up, as long as the personal data originate from open source material.

Europol will explore the possibility to embed the CTW portal into the framework of Article 10 of the Europol Convention. The aim should be to provide a solid legal basis for the storage, searching, processing and also analysis of personal data on the portal, as well as the exchange of analysis results and assessments.

By doing this, CTW could be used to its full potential and would be transformed into an even more powerful tool for Member States in combating Islamist extremist terrorism.

Europol will continue to discuss the way forward with the Europol Management Board, in consultation with the Europol Joint Supervisory Body.

ANNEXES

Annex 1: Article 6 & 6a Europol Convention – computerised systems of collected information

Article 6: ***Computerized system of collected information***

1. Europol shall maintain a computerised system of collected information consisting of the following components:

1) An Information System (IS) as referred to in article 7 with a restricted and precisely defined content which allows rapid reference to the information available to the Member States and Europol.

2) Work files (AWF) as referred to in article 10 established for variable periods of time for the purposes of analysis and containing comprehensive and

3) An Index System (IS) containing certain particulars from the analysis files referred to point 2, in accordance with the arrangements laid down in article 11.

2. The computerised system of collected information operated by Europol must under no circumstances be linked to other automated processing systems, except for the automated processing systems of the national units.

Article 6a: ***Information processing by Europol***

In support of the execution of its tasks, Europol may also process data for the purpose of determining whether such data are relevant for its tasks, and can be included in the computerised system of collected information referred to in Article 6(1).

The Contracting Parties meeting within the Council, acting with a two-thirds majority, shall determine conditions related to the processing of such data, in particular with respect to the access and usage of the data, as well as time limits for the storage and deletion of the data that may not exceed six months, having due regard to the principles referred to in Article 14. The Management Board shall prepare the decision of the Contracting Parties and consult the joint supervisory body referred to in Article 24.[1]

Annex 2: Updated Check the Web Use Policy – personal data

Check the Web may be used to process personal data to the extent that the personal data is publicly accessible. In particular, purely descriptive summaries of open sources material, including personal data, may be inserted into the freetext field.

The portal must not be used for any processing that properly comes within the scope of the computerised systems as referred to in Art. 6 and 6a of the Europol Convention. In particular, no information from police files or investigations which is not publicly accessible shall be included into the freetext field. The processing of "analysis" on Check the Web in the form of **establishing links between open source information on the one hand and non-publicly accessible information stemming from police files or ongoing investigations on the other is prohibited as coming within the scope of the AWFs.**

All personal information stored under the topic "Contact details" is subject to the prior and explicit agreement of each individual contact point. Each Member State is responsible for providing the information on their contacts and for obtaining the agreement of the contact points on the publication of their personal details.

[1] *Article 6a inserted by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0003).*

Annex 3: Article 10 of Europol Council Decision

WORK FILES FOR THE PURPOSES OF ANALYSIS

Article 10

Collection, processing and utilization of personal data

1. Where this is necessary to achieve the objective laid down in Article 2(1), Europol may, in addition to data of a non-personal nature, store, modify, and utilise in other files data on criminal offences for which Europol is competent, including data on the related criminal offences provided for in the second subparagraph of Article 2(3) which are intended for specific analyses and which concern:1

persons as referred to in Article 8(1);
persons who might be called on to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings;
persons who have been the victims of one of the offences under consideration or with regard to whom certain facts give reason for believing that they could be the victims of such an offence; contacts and associates, and persons who can provide information on the criminal offences under consideration.

The collection, storage and processing of the data listed in the first sentence of Article 6 of the Council of Europe Convention of 28 January 1981 with regard to Automatic Processing of Personal Data shall not be permitted unless strictly necessary for the purposes of the file concerned and unless such data supplement other personal data already entered in that file. It shall be prohibited to select a particular group of persons solely on the basis of the data listed in the first sentence of Article 6 of the Council of Europe Convention of 28 January 1981 in breach of the aforementioned rules with regard to purpose.

[1] *Article 10(1) replaced by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0008).*

The Council, acting unanimously, shall adopt implementing rules for data files prepared by the Management Board containing additional details, in particular with regard to the categories of personal data referred to in this Article and the provisions concerning the security of the data concerned and the internal supervision of their use.1

2. Such files shall be opened for the purposes of analysis defined as the assembly, processing or utilization of data with the aim of helping a criminal investigation. Each analysis project shall entail the establishment of an analysis group closely associating the following participants in accordance with the tasks defined in Article 3(1) and (2) and Article 5(3):

analysts and other Europol officials designated by the Europol Directorate;2
the liaison officers and/or experts of the Member States supplying the information or concerned by the analysis within the meaning of paragraph 6.
Only analysts shall be authorised to enter data into the file concerned and modify such data; all participants may retrieve data from the file.3

3. At the request of Europol or on their own initiative, national units shall, subject to Article 4(5), communicate to Europol all the information which it may require for the performance of its tasks under Article 3(1), point 2. The Member States shall communicate such data only where processing thereof for the purposes of preventing, analysing or combating offences is also authorized by their national law.

Depending on their degree of sensitivity, data from national units may be routed directly and by whatever means may be appropriate to the analysis groups, whether via the liaison officers concerned or not.

[1] *Article 10(1) amended by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0005).*
[2] *Article 10(2) first point replaced by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0005).*
[3] *Article 10(2), second subparagraph added by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0005).*

4. If, in addition to the data referred to in paragraph 3, it would seem justified for Europol to have other information for the performance of tasks under Article 3(1), point 2, Europol may request that:

the European Communities and bodies governed by public law established under the Treaties establishing those Communities;
other bodies governed by public law established in the framework of the European Union; bodies which are based on an agreement between two or more Member States of the European Union; third States; international organizations and their subordinate bodies governed by public law;
other bodies governed by public law which are based on an agreement between two or more States; and the International Criminal Police Organization,

forward the relevant information to it by whatever means may be appropriate. It may also, under the same conditions and by the same means, accept information provided by those various bodies on their own initiative. The Council, acting unanimously and after consulting the Management Board, shall draw up the rules to be observed by Europol in this respect.1

5. In so far as Europol is entitled under European Union or international legal instruments to gain computerised access to data from other information systems, Europol may retrieve personal data by such means if this is necessary for the performance of its tasks pursuant to point 2 of Article 3(1). The applicable provisions of such European Union or international legal instruments shall govern the use of this data by Europol.2

6. If an analysis is of a general nature and of a strategic type, all Member States, through liaison officers and/or experts, shall be fully associated in the findings thereof, in particular through the communication of reports drawn up by Europol.

[1] *Article 10(4) amended by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0008).*
[2] *Article 10(5) replaced by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0005).*

If the analysis bears on specific cases not concerning all Member States and has a direct operational aim, representatives of the following Member States shall participate therein:

Member States which were the source of the information giving rise to the decision to open the analysis file, or those which are directly concerned by that information and Member States subsequently invited by the analysis group to take part in the analysis because they are also becoming concerned;
Member States which learn from consulting the index system that they need to be informed and assert that need to know under the conditions laid down in paragraph 7.

7. The need to be informed may be claimed by authorized liaison officers. Each Member State shall nominate and authorize a limited number of such liaison officers. It shall forward the list thereof to the Management Board.

A liaison officer shall claim the need to be informed as defined in paragraph 6 by means of a written reasoned statement approved by the authority to which he is subordinate in his Member State and forwarded to all the participants in the analysis. He shall then be automatically associated in the analysis in progress.

If an objection is raised in the analysis group, automatic association shall be deferred until completion of a conciliation procedure, which may comprise three stages as follows:

the participants in the analysis shall endeavour to reach agreement with the liaison officer claiming the need to be informed; they shall have no more than eight days for that purpose;
if no agreement is reached, the heads of the national units concerned and the Directorate of Europol shall meet within three days;
if the disagreement persists, the representatives of the parties concerned on the Management Board shall meet within eight days. If the Member State concerned does not waive its need to be informed, automatic association of that Member State shall be decided by consensus.

8. The Member State communicating an item of data to Europol shall be the sole judge of the degree of its sensitivity and variations thereof. Any dissemination or operational use of data communicated shall be decided on by the Member State that communicated the data to Europol. If it cannot be determined which Member State communicated the data to Europol, the decision on dissemination or operational use of data shall be taken by the participants in the analysis. A Member State or an associated expert joining an analysis in progress may not, in particular, disseminate or use the data without the prior agreement of the Member States initially concerned.1

9. Europol may invite experts of third States or third bodies within the meaning of paragraph 4 to be associated with the activities of an analysis group, where:
an agreement is in force between Europol and the third State or third body, which contains appropriate provisions on the exchange of information, including the transmission of personal data, as well as on the confidentiality of exchanged information;
the association of the experts of the third State or third body is in the interest of the Member States;
the third State or third body is directly concerned by the analysis work; and
all participants within the meaning of paragraph 2 agree on the association of the experts of the third State or third body with the activities of the analysis group.

The association of experts of a third State or a third body with the activities of an analysis group shall be subject to an arrangement between Europol and the third State or third body. The rules governing such arrangements shall be determined by the Management Board acting by a majority of two thirds of its members.

Details of the arrangements between Europol and third States or third bodies shall be sent to the joint supervisory body referred to in Article 24 which may address any comments it deems necessary to the Management Board.2

[1] *Article 10(8), second sentence, replaced by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0005).*
[2] *Article 10(9) added by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0005).*

Annex 4: Correspondence between Europol and JSB

EDOC-#383096-Letter of Director to JSB requesting opinion on processing of personal data on Check the Web

EUROPOL

Director

The Hague, 20 March 2009

Mr. David Smith
Chairman Joint Supervisory Body
Rue de la Loi 175
B-1048 Brussels
BELGIUM

Subject: Opinion of the JSB on processing of personal data on Check the Web

Dear Mr. Smith,

I refer to my letter dated 15 January 2009 in which I provided the JSB with an evaluation report on the use of the Check the Web portal. I would like to take the opportunity to inform you that Europol is expected to report to the Council at the end of April 2009 "on how to increase dissemination of personal data in order to make use of its secure information portal" (Draft Council conclusions on the continuation of work on combating terrorism, 15684/08, last paragraph).

Our internal discussions on the topic have further evolved since the submission of the evaluation report. As you have already been informed, two scenarios are currently considered:

The first scenario refers to Check the Web as it is currently setup, i.e. outside the computerised systems as referred to in Art. 6 and 6a Europol Convention. It is based on a distinction between "analysis" on the one hand which would still be prohibited and "purely descriptive summaries of open sources" on the other which would be allowed in the freetext field even if they are extensive and contain personal data.

The second scenario envisages Check the Web in an AWF environment. This would mean that the processing of any kind of analysis would be possible under the precondition that the AWF legal framework is applied.

I would be grateful for receiving an initial opinion from the JSB on this important topic which could - in the best case - already be taken into consideration when drafting the report to the Council.

Yours sincerely

Max-Peter Ratzel

Signed by the Deputy Director Serious Crime Department on behalf of the Director on 23 March 2009

Director

File no. 3550-105 (#383096-v1)

Raamweg 47, The Hague
The Netherlands

P.O. Box 90850
NL - 2509 LW The Hague

31 (0)70 302 5000
31 (0)70 345 5896

EDOC-#388479-Letter from Joint Supervisory Board (JSB) Check the Web

JOINT SUPERVISORY BODY OF EUROPOL

RECEIVED
16 APR. 2009
CGI and CG Secretariat

The Director of Europol
Mr. Max-Peter Ratzel
PO Box 90850
2509 LW The Hague
The Netherlands

Brussels, 6 April 2009

Subject: Check the Web
Our ref. 09/17

Dear Mr. Ratzel,

In your letter of 20 March you informed the JSB that Europol has to report to the Council at the end of April on "how to increase dissemination of personal data in order to make use of its secure information portal". In view of the time available to answer your request you will understand that the JSB response is provisional.

In view of the recent discussions on this subject, the JSB is aware that not only the dissemination of personal data but also the presentation and the evaluation of information from open sources, as referred to in the Council Conclusions of 12-13 June 2007, is also part of the further development of the Check the Web project. It is duly noted that, in particular, the evaluation of data and sharing the results of such evaluation has lead to various discussions on how this could be achieved within the legal framework of Europol.

The two scenarios you described clearly reflect the possible choices which are apparently under discussion: maintaining the status quo, or introducing evaluating and analysing activities.

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

1

In its meeting of 23 March, the JSB explored the possibilities for Europol to comply with Member States' wishes to further develop this project and at the same time stay within the limits set in the Europol Convention and the Council Decision establishing Europol.

In this respect it was noted that the first scenario: maintaining the status quo and using purely descriptive summaries of open sources, will probably lead to continuous discussions on the actual use of these summaries. The JSB is aware that it is apparently not always clear what is considered as a descriptive summary and whether the mentioning of personal data in those summaries is allowed under the legal basis of Europol. The JSB is also informed that in some of the Member States' contributions to these summaries, evaluations of the content of a web site is introduced.
In this respect I would like to refer to the conclusion drawn by the JSB in its opinion 07-22 of 26 June 2007 on Check the Web *"that this portal may be used to process personal data as described in Articles 8 and 10 of the Europol Convention to the extent that the personal data is publicly accessible, but the portal must not be used for any processing that properly comes within the scope of the systems referred to in Articles 6 and 6A of the Europol Convention."*

Since evaluation of the content is an essential part of the Council Conclusions, the JSB expects that this first scenario will soon - if not already - lead to tensions between Member States' wishes and the possibility for Europol to comply with those within its legal framework.

Taking into account the Council Conclusions of June 2007 it will be essential for the further development of Check the Web:
i) to create the possibility for Europol and/or Member States not only to collect information from public sources, but also to evaluate and analyse this information; and
ii) to disseminate this by providing direct access to Member States.

Evaluating and analysing information is a specific Europol task for which the Convention and the new legal basis created specific provisions: the rules on analytical files. These rules also allow the retrieval of information by all participants of the analysis file (Article 10(2) Europol Convention).

In view of this possibility to collect, evaluate and analyse data on terrorist activities and to disseminate these data in accordance with the existing rules on analysis files, the JSB suggests that Europol explores further the second scenario.
In this respect the JSB also notes that Article 10(2) of the new legal basis for Europol clearly links any decision on establishing new systems of processing personal data to the possibilities offered by

the existing Europol information processing systems. This article thus clearly demonstrates Member States' view that whenever the already existing information processing systems are suitable for fulfilling Europol's task, the creation of new systems should not be an option.

The JSB would like to be kept informed of any further developments and is always ready to be of assistance. In view of the discussions in the Management Board on this subject, the JSB also intends to contact the chairman of the Management Board.

Yours sincerely,

David Smith
Chairman
(Signed by the Data Protection Secretary)

Annex 5: Article 21 of Europol Convention: Time limits for the storage and deletion of Data files

1. Data in data files shall be held by Europol only for as long as is necessary for the performance of its tasks. The need for continued storage shall be reviewed no later than three years after the input of data. Review of data stored in the information system and its deletion shall be carried out by the inputting unit. Review of data stored in other Europol data files and their deletion shall be carried out by Europol. Europol shall automatically inform the Member States three months in advance of the expiry of the time limits for reviewing the storage of data.

2. During the review, the units referred to in the third and fourth sentences of paragraph 1 above may decide on continued storage of data until the next review if this is still necessary for the performance of Europol's tasks. If no decision is taken on the continued storage of data, those data shall automatically be deleted.

3. The need for continued storage of personal data relating to individuals as referred to in Article 10(1) shall be reviewed every year and the review documented. Storage of such data in a data file referred to in Article 12 may not exceed the period of existence of the file.1

4. Where a Member State deletes from its national data files data communicated to Europol which are stored in other Europol data files, it shall inform Europol accordingly. In such cases, Europol shall delete the data unless it has further interest in them, based on intelligence that is more extensive than that possessed by the communicating Member State. Europol shall inform the Member State concerned of the continued storage of such data.

5. Deletion shall not occur if it would damage the interests of the data subject which require protection. In such cases, the data may be used only with the consent of the data subject.

Annex 6: Article 10.3 of Europol Council Decision

The Management Board decision referred to in paragraph 2 shall determine the conditions and limitations under which Europol may establish the new system processing personal data. **The Management Board decision may allow processing of personal data relating to the categories of persons referred to in Article 14(1), but not the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life.** The Management Board decision shall ensure that the measures and principles referred to in Articles 18, 19, 20, 27, 29 and 35 are properly implemented. In particular, the Management Board decision shall define the purpose of the new system, access to and the use of the data, as well as time limits for the storage and deletion of the data.

Annex 7: Statistics from 08 April 2009, based on the number of websites stored on the Check the Web portal

Member States contributions: **26, 68 %** (Contributions from 8 Member States)

Europol contributions: **73, 31%**

[1] *Article 21(3) replaced by the Council Act of 27 November 2003 (Official Journal 002, 06/01/2004, p. 0006).*