THE SECOND ACTIVITY REPORT OF THE EUROPOL JOINT SUPERVISORY BODY

NOVEMBER 2002 - OCTOBER 2004

Europol and the Joint Supervisory Body

Europol is the organisation created to assist EU Member States in preventing and combating serious international crime, though only where such crime involves an organised criminal structure and affects at least two Member States. On a practical level, Europol's main tasks are to facilitate the exchange of information between Member States and provide analytical expertise.

As Europol handles a large amount of sensitive information about individuals, the Europol Convention contains a number of provisions requiring Europol to take account of the rights of individuals when using this information. The Convention also provides for the creation of the Joint Supervisory Body — an independent body charged with ensuring that Europol complies with data protection principles.

In order to encourage transparency the Europol Convention requires the Joint Supervisory Body to publish an activity report at regular intervals — this is the second such report.

Contents

Foreword

It is my honour to present the second activity report of the Europol Joint Supervisory Body (the JSB). The report covers the period from November 2002 to October 2004 and reflects the accomplishments of the JSB under the chairmanship of Klaus Kalk. On behalf of all my colleagues in the JSB, I would like to pay tribute to Mr Kalk's dedication to our tasks and his clear stance in favour of human dignity and the fundamental right to data protection. I am also aware that the achievements of this body have only been possible because of the commitment and enthusiasm of the two chairmen of the Appeals Committee for this period, Mario Varges Gomes and Giuseppe Busia, together with the combined efforts of all the JSB's members and its secretariat.

The report gives an accurate overview of the main topics that the JSB has dealt with in a period strongly marked by the measures put in place to fight terrorism after the tragic events of September 11 2001 in the US and, very recently, by the bomb attacks in Madrid on March 11 2004. In all its opinions and actions, the JSB has showed that it is perfectly possible and not at all inconsistent to support the shared goal of fighting international terrorism and organised crime while, at the same time, safeguarding the rights of individuals.

Finally, after the inclusion of data protection as a fundamental right in the Charter of Fundamental Rights of the European Union and in the draft Constitutional Treaty, and as the EU's pillars continue to converge, it is becoming increasingly evident that the field of police and judicial co-operation requires a clear and specific set of data protection rules, with the provision of independent advice and harmonised supervision. Various initiatives dealing with this issue are due to be considered in the coming months and the JSB intends to monitor developments closely, offering assistance and advice with a view to ensuring that any proposed changes result in a practical framework, while also respecting data protection rights and values.

Emilio Aced Félez
Chairman

Chapter I

Introduction

Since the Treaty of Amsterdam committed Member States to creating 'an area of freedom, security and justice', one of the EU's key objectives has been to improve co-operation between law enforcement authorities. More often than not, such co-operation involves the exchange of personal data.

Recent terrorist atrocities have given fresh impetus to this trend towards closer co-operation and, with Member States convinced of the need to work together to tackle terrorism, there has been a reassessment of the measures that the EU has in place to safeguard security.

This opening chapter gives an account of the way in which the Europol Joint Supervisory Body has responded to some of the changes that have occurred in this area, focusing in particular on two developments: one that came about as a result of a decision taken by the Director of Europol, the other following an initiative to update the provisions of the Europol Convention.

Europol & the US

Shortly after the terrorist attacks on the United States in September 2001, the Director of Europol took the decision to allow Europol to transmit personal data to the US.

Rules governing Europol's transmission of personal data to third states normally require a formal agreement between Europol and the state in question. Such agreements set out provisions concerning the categories of data to be transmitted and the purposes for which these data may be used; and an agreement cannot be concluded unless the opinion of the Joint Supervisory Body (the JSB) has first been obtained.

In exceptional circumstances, however, the Director of Europol can bypass this procedure and take the decision to transmit personal data without an agreement if he considers this to be absolutely necessary in order to safeguard the essential interests of Member States or prevent imminent danger.

In response to the Director's decision, the JSB issued an opinion in which it stressed that only a formal agreement would provide a satisfactory legal basis for long-term co-operation between Europol and the US, and that the decision should in no way amount to an indefinite authorisation to transmit data to the US.

During negotiations to draw up an agreement between Europol and the US both parties sought to address a number of important points, including the purposes for which data could be used and the question of supervising the agreement's implementation.

The JSB's opinion on the draft agreement recognised that it was 'imperative' to improve co-operation between the US and Europol in the fight against serious crime; and, noting the significant progress made during the course of the negotiations, the JSB concluded that the Council could allow the Director of Europol to finalise the agreement.

The JSB emphasised, however, that 'in view of the law and regulation in the United States of America in relation to the protection of personal data' there would have to be effective supervision to ensure that both parties to the agreement complied with its provisions.

How is the JSB monitoring the agreement between Europol & the US?

Since the agreement was signed the JSB has:

- Established links with the Chief Privacy Officer at the US Department of Homeland Security. The Chief Privacy Officer is responsible for ensuring that the Department of Homeland Security complies with the agreement's provisions and other relevant privacy measures. In March 2004 the Chief Privacy Officer's deputy attended a meeting of the JSB to inform members of the existing privacy legislation in the US. The members of the JSB also took the opportunity to ask a number of questions about the exact role of the Chief Privacy Officer. The JSB is keen to build on this relationship in future as it will provide an opportunity to establish what happens to data sent to the US under the agreement — as well as allowing the JSB to discover what is being done in the US to check the accuracy of data sent to Europol.

- Monitored developments. It came to the attention of the JSB that, as a result of changes in US legislation, the FBI would no longer be required to take reasonable efforts to ensure the accuracy of data held in the National Crime Information Center, the country's largest criminal-justice database. This development is a cause for concern given that the FBI is one of the federal authorities entitled to exchange personal data with Europol under the agreement. The JSB sought further information from Europol in order to establish whether this development would affect personal data transmitted under the terms of the agreement. The JSB regrets that, to date, it has not received a response.

The JSB remains committed to monitoring compliance with the agreement. Since the agreement was signed, it would appear that most of the information passed between EU and US law enforcement authorities has been exchanged under existing bilateral agreements

between the US and individual Member States. However, as the volume of information exchanged between Europol and the US increases, future inspections of Europol will focus on examining personal data exchanged under the agreement to ensure that there is compliance with the relevant provisions. Furthermore, the JSB will seek to co-ordinate supervision, working with national data protection authorities in the Member States and the Chief Privacy Officer at the Department of Homeland Security in the US.

Amending the Europol Convention: Retention Periods

In 2002 the EU's Danish Presidency launched an initiative to amend the Europol Convention. The Joint Supervisory Body issued an opinion, which commented on those proposals that related to the processing of personal data. The Danish Presidency took account of the JSB's concerns and many proposals were amended accordingly.

When a draft Protocol to amend the Europol Convention was published in December 2002 it included a proposal to extend the period for which personal data could be held in Europol's analysis files. Article 21 of the Europol Convention stipulates that when information on an individual is held in analysis files at Europol, it must be deleted after three years if no additional information on the individual in question has been added during that time. The draft Protocol aimed to extend this retention period to five years.

Initially, the JSB had seen no justification for extending this period of retention. However, Europol argued that for certain crimes — and terrorism in particular — longer retention periods were necessary in order to carry out effective analysis.

In February 2003 the JSB's inspection team examined Europol's analysis files in detail and arrived at the conclusion that longer retention periods were indeed necessary in some cases, but that a test of necessity rather than a rigid time limit ought to be used to determine whether or not personal data should be retained.

With this in mind, the JSB proposed that the Europol Convention should be amended so that the retention period would relate to the file itself rather than to the personal data contained within the file. Europol would have to delete analysis files after a three year period unless, at the end of the three year period, Europol considered the continuation of a particular file to be *strictly necessary*. In such cases the file could be continued for a further three years.

Although Europol would be able to apply this test of necessity at the end of each three year period, after taking the decision to continue a file Europol would be required to repeat the procedure for opening an analysis file set out under Article 10 of the Europol Convention.

This would give the JSB and the Europol Management Board the opportunity to examine the reasons for continuing a particular file and so the process would be kept under scrutiny, eliminating the possibility of a file continuing indefinitely.

To safeguard against personal data being retained unnecessarily, it was proposed that the Convention should still require Europol to carry out an annual review of the need for the continued retention of personal data held in analysis files. In addition, the JSB could specifically ask the inspection team to look at any continued files when carrying out an inspection.

The JSB's proposed amendment was accepted and included in the final version of the Protocol to amend the Europol Convention.[1]

Working Together to Promote Data Protection

There are now numerous EU initiatives involving the collection, retention or exchange of personal data for law enforcement purposes; notable examples include measures to allow the exchange of data on air passengers and proposals to require the retention of communications data. These and other developments, such as suggestions that Europol might one day become an investigative organisation, could have significant implications for the rights of individuals. Consequently, the Joint Supervisory Body has sought to work with other data protection authorities to ensure that data protection concerns are taken into account by policy makers.

The JSB has for some time been closely aligned with its sister authorities — the Schengen Joint Supervisory Authority and the Customs Joint Supervisory Authority, which are responsible for supervising the Schengen information system and the customs information system respectively. All three supervisory authorities are served by the same secretariat based in Brussels, and moves to co-ordinate the efforts of the authorities have included the creation of a working group made up of technical experts from the national data protection authorities. This group, which was set up to provide technical support to the joint supervisory authorities, is currently developing a standard tool for carrying out inspections of the third-pillar information systems.

In addition, a recent invitation to submit evidence to a House of Lords Select Committee prompted the three joint supervisory authorities to hold a joint meeting, together with

[1] Council Act of 27 November 2003 drawing up a Protocol amending the Europol Convention

representatives of the Eurojust Joint Supervisory Body — and this resulted in the adoption of a joint opinion on data protection in the third pillar. It is anticipated that there will be further such meetings, allowing the joint supervisory authorities to discuss matters of common interest.

It is clear, however, that many new EU initiatives involving personal data do not fall within the specific mandates of the joint supervisory authorities; indeed, not all initiatives fall neatly under any one of the traditional EU pillars.

For this reason, at the 2004 conference of European data protection authorities in Rotterdam, it was agreed that representatives of those data protection authorities operating at EU level should meet to co-ordinate their efforts. The first meeting of this 'planning' group took place in June 2004 and involved the European Data Protection Supervisor, the chairs of the joint supervisory authorities, and the chair of the Article 29 Working Party, which is responsible for advising the Commission on data protection matters in the first pillar.

There was a further development when, in September 2004 at the conference of international data protection authorities in Wrocław, a closed session of the European authorities passed a resolution calling on the EU institutions to provide a forum in which EU data protection authorities might discuss the data protection implications of developments in the third pillar. Until such a forum exists, those third-pillar initiatives that fall outside the remit of the joint supervisory authorities will be examined by a working party of the European data protection authorities.

Chapter II

Part A — Supervisory Work

1. Inspecting Europol

One of the ways in which the Joint Supervisory Body fulfils its general task is by carrying out on-site inspections of Europol's activities.

Inspection — February 2003

In December 2002 the JSB gave its inspection team a mandate to examine Europol's analysis files and information systems, and the level of compliance with formal agreements between Europol and third states.

In February 2003 the inspection team spent three days inspecting Europol. Adopted in July 2003, the final report acknowledged that the level of data protection at Europol had improved since the first inspection in 2000. It was also noted, however, that Europol had experienced some problems safeguarding data quality. This was largely because Europol has to rely on the quality of data received from Member States. The JSB therefore suggested that the national data protection authorities should seek to address this problem at national level.

The inspection team came to the overall conclusion that, based on the checks made during the inspection, Europol's processing of personal data was being carried out in compliance with the relevant data protection provisions. It was also noted that in some specific areas, such as auditing and logging, Europol had implemented systems that adhered to high standards of data protection.

A number of recommendations were made with a view to improving Europol's compliance still further and a follow-up inspection took place in November 2003.

Inspections — Strategic Objectives

It is evident that Europol's role is developing quickly, with more personal data being processed. The JSB is determined that inspections of Europol should keep pace with these developments and so, in 2003, the JSB set out a number of objectives intended to guide future inspections. In brief, these are as follows:

- inspections of Europol should take place annually;
- there ought to be more emphasis on inspecting the quality of personal data held by Europol; and
- the inspection team should be given greater discretion regarding the scope of the inspection, having the flexibility to examine particular areas of concern as they arise.

Inspection — March 2004

With these objectives in mind, the JSB approved another inspection of Europol, emphasising that this inspection should focus on the quality of data processed by Europol in analysis files.

The three-day inspection began on 30 March 2004. Prior to the inspection, the team had selected a number of analysis files to be examined. For each file, the team assessed compliance with the original order opening the file to determine whether the categories of personal data held and the Member States participating in the work of the file were the same as those listed in the order. Samples of data were taken from each of the files and the quality was compared against the source document.

Although some inaccuracies were found, on the whole the quality of data was found to be satisfactory — at least in so far as the data in the files reflected data supplied by Member States. It was noted, however, that there was a general failure on the part of Member States to assess data properly (checking source, reliability and so on). Once again, the JSB stressed that co-operation between Member States and Europol must be improved in order to address this problem.

It was also noted that in some cases there was an apparent disparity between the details in the order opening a particular file and the reality of what was actually happening. For example, the opening orders did not always present a recent overview of the parties contributing to the file, and in some cases only a few of the categories of data listed in the opening order were actually being processed in the file. The team recommended that after an analysis file had been open for a certain period (perhaps a year) Europol should reassess the file to clarify the nature of contributions from participating states. The opening order might then need to be updated to reflect the true extent of participation.

The Europol Information System

When Europol was established one of its priorities was to develop an EU-wide information system, which would hold information on persons suspected of involvement in offences for which Europol was competent. One of the JSB's main tasks would be to monitor this system — the Europol Information System — and assess compliance with data protection provisions.

It is worth providing a brief account of the system's development, which has been beset by difficulties.

The process of planning and developing the system first began in 1996. There were contractual problems early on and these were compounded by additional demands being made of the system — for example, it was decided to extend the system to include Euro-counterfeiting functionalities. Consequently, there have been numerous versions of the system in development. A limited version of the system, which allows Europol to discharge its responsibilities in respect of the Euro, came into operation in 2001.

Recent problems with the final version of the system were outlined in Europol's 2003 Annual Report:

'Delivery of the Europol Information System (EIS) . . . was planned for February 2003. However, it was not delivered due to the underestimation of the number of problems that would arise . . . . The expected revised delivery date of June was met but when delivered, the product was not up to standard.'

Once the final version of the system is operational in Member States (it is anticipated that this could be before the end of 2004), the JSB intends to work with national data protection authorities to monitor the system closely, keeping its use under scrutiny. Moreover, a large part of future inspections will be dedicated to examining the system to ensure that it complies with the relevant data protection provisions.

2. Europol — A Supporting Role

There is an ongoing debate about exactly what form Europol's analytical support to Member States should take. The issue was first raised in the light of a discovery made by the JSB's inspection team.

MSOPES

During the first inspection of Europol in November 2000 the inspection team discovered that Europol was providing analytical support to investigations being carried out by Member States. These projects — known as Member States' Operational Projects with Europol Support (MSOPES) — involved the creation of analysis files at Europol; but with Member States, rather than Europol, taking responsibility for these files.

Although Europol has a general task of aiding investigations in the Member States, Article 10 of the Europol Convention lays down a procedure that must be followed when opening an analysis file at Europol. In addition to setting out the categories of personal data that may be held in such files, this article requires the Director of Europol to provide the JSB with the opportunity to comment on an order opening a new analysis file. MSOPES files, however, were not being opened in accordance with this procedure. The JSB made it clear that the creation and use of analysis files at Europol was limited to Article 10 of the Europol Convention and that, consequently, the creation of MSOPES files was unlawful. Taking the JSB's concerns into account, the Council decided not to create a legal basis for MSOPES, and the associated files at Europol have been discontinued.

Joint Investigation Teams

The JSB is now considering the extent of the analytical support provided by Europol under another structure. The Treaty of Amsterdam included a commitment to create 'joint investigation teams', and it was hoped that these teams would aid joint investigations conducted by two or more Member States.

A Council Framework Decision[2] introduced common rules for these teams and indicated that they could include 'officials of bodies set up pursuant to the Treaty on European Union' — a definition that includes Europol staff. Specific details regarding Europol's participation in joint investigation teams were subsequently set out in a Protocol adopted by the Council.[3] Although the provisions set out in this Protocol make it clear that Europol staff are to participate in a 'support capacity', Europol staff assisting in a joint investigation team would be integrated into the team's chain of command, and Europol information would be shared directly via Europol team members; furthermore, information collected by the team would be entered in Europol databases.

[2] Council Framework Decision of 13 June 2002 on joint investigation teams

[3] Council Act of 28 November 2002 drawing up a Protocol amending the Europol Convention

The JSB acknowledges that once the Protocol amending the Europol Convention has been ratified by Member States, Europol will be able to participate in joint investigation teams and exchange information with other members of a particular team. This will not add to the list of authorities with which Europol is currently entitled to exchange information. However, if participation in a joint investigation team were to involve the creation of analysis files at Europol, parallels might well be drawn with the situation that arose with MSOPES, particularly as the Protocol does not introduce a legal basis that would allow the creation of analysis files outside the scope of Article 10.

The JSB sought information on whether Europol had formulated a policy on the kind of support that would be offered to joint investigation teams. Specifically, the JSB enquired as to the way in which Europol intends to use its analytical services.

It appears that Europol is in the process of deciding exactly how it might support joint investigation teams once the Protocol has been ratified by all Member States. Until the Protocol has been ratified, Europol can only support joint investigation teams in accordance with the existing provisions of the Europol Convention. Europol has informed the JSB that the support provided to joint investigation teams in this interim period will be limited to analysis of information and intelligence in line with the provisions of the Convention; identification of information gaps; dissemination of analytical reports providing assessments of assembled intelligence; and identification of new projects as a result of analysis.

The JSB intends to monitor the situation in order to ensure that there is compliance with the Europol Convention. It will be particularly interesting to see how Europol interprets its role in joint investigation teams once the Convention has been amended.

3. Opening Analysis Files

Every time Europol wants to start a new analysis file under Article 10 of the Europol Convention an order must be drawn up opening the file. This order should set out, among other things, the purpose of the file and the categories of personal data to be held. These orders must be approved by the Europol Management Board, which is obliged to send the order to the JSB for comment. It is the JSB's policy to issue an opinion on every 'opening order' it receives.

During the period covered by this report the JSB has issued opinions on nine orders to open separate analysis files. In most cases the JSB had no comment to make, though on one occasion the JSB sought clarification on a number of points and questioned the inclusion of

several categories of data in the opening order. Europol responded by removing these data categories from the order.

At the time of writing, Europol is processing personal data in nineteen separate analysis files.

4. Agreements with Third States/Bodies

If Europol intends to transmit personal data to a state outside the EU, a formal agreement must first be signed between Europol and the state in question. Before concluding such an agreement Europol is obliged to obtain the JSB's opinion.

In the past two years Europol has signed agreements with the following third states: the Slovak Republic, Cyprus, Latvia, Lithuania, and Malta (all of which have since joined the EU and are no longer third states), and Bulgaria and Romania. In each case the JSB made a number of general remarks but concluded that, from a data protection perspective, there were no obstacles to prevent Europol from finalising the agreement.

Eurojust

Europol has also signed a formal agreement with Eurojust, the authority charged with improving judicial co-operation throughout the EU. In its first opinion on the draft agreement between Europol and Eurojust, the JSB noted that the Council Decision establishing Eurojust required the Council to consult the Eurojust Joint Supervisory Body before approving the agreement. As the procedure in this case involved two joint supervisory bodies, the Europol JSB made it clear that it would want to take account of the Eurojust JSB's opinion before adopting a final position. Since the Eurojust JSB was not yet in operation when the Europol JSB issued its first opinion (in May 2003), this first opinion was to serve as a provisional opinion on the draft agreement.

In its provisional opinion the JSB stressed that even after the agreement had been concluded, national members of the Eurojust College would only be entitled to receive personal data from Europol within the scope of Article 6 of the Council Decision establishing Eurojust: they must not receive data for other purposes. The opinion also suggested that the agreement should be amended so that Europol and Eurojust would be obliged to respect any conditions placed on the use of data transmitted under the agreement.

Once the Eurojust JSB had been formed, its chairman and Mr Kalk (the then chairman of the Europol JSB) met to discuss the agreement. In December 2003 the Europol JSB issued

a second opinion stating that there were no longer any obstacles preventing the agreement from being finalised — with the proviso that the exchange of data could not begin until Eurojust had implemented additional measures to safeguard data security.

- The JSB's opinions on all these agreements can be found on the JSB's website at http://europoljsb.ue.eu.int.

5. Rights

The Europol Convention affords individuals a number of rights. Under Article 19 of the Convention individuals have a right of access to any information that Europol might be holding on them. If information relating to an individual is found to be incorrect, then that individual can ask Europol to correct or delete the information in question.

Figures provided by Europol reveal that there were ten requests for access made in 2002; in 2003 only six requests were made; and, in 2004, Europol has so far received ten requests for access (up to and including September).

Individuals can ask the JSB to ensure that the manner in which their personal data have been collected, stored, processed, and utilised by Europol is lawful and accurate. The JSB has so far received two such requests — and, after checks were made, Europol was found to have acted in compliance with the Europol Convention in both cases.

Part B — Managing the Joint Supervisory Body

The Joint Supervisory Body met nine times between November 2002 and October 2004. The JSB is composed of representatives of the national data protection authority of each Member State. A list of members can be found on the JSB's website.

One of the challenges facing the JSB has been to prepare for EU enlargement. At the same time, the JSB has been reflecting on how it can be more transparent, more accessible to those it serves. Brief details of both these developments are outlined below.

1. Preparation for Enlargement

At its meeting in June 2003, the JSB welcomed new colleagues from the accession states. Although the ten countries were not due to join the EU until 2004, representatives from the accession states were invited to attend this and future meetings as observers in the hope that this would provide them with an opportunity to familiarise themselves with the workings of the JSB. Before the meeting, a questionnaire had been distributed with a view to collecting information on data protection legislation in the accession states and the extent to which this legislation applies to the police.

It was particularly encouraging to learn that the data protection authorities in the accession states have been working hard to forge working relationships with police authorities. The results of the questionnaire revealed that between them the various data protection authorities had, among other things, carried out inspections of police processing, undertaken security audits, held meetings to discuss policy, and provided training to the police on data protection matters.

The JSB organised a visit to Europol for the observers so that they might gain an insight into how Europol carries out its various tasks. In October 2003, delegations from five of the accession states spent two days at Europol headquarters in The Hague. Representatives from the data protection authorities of Iceland and Norway, which are third states entitled to exchange personal data with Europol, were also present.

Although the accession states became members of the EU in May 2004, delegations only become full members of the JSB once their respective countries have acceded to the Europol Convention, fulfilling all conditions of Article 46. As at 1 October 2004, those delegations representing the data protection authorities of Cyprus, the Czech Republic, Hungary, Latvia, Lithuania and the Slovak Republic have become full members.

As members of the JSB, these new colleagues will have a crucial part to play in protecting fundamental rights throughout the enlarged EU.

2. Transparency

The JSB performs its functions on behalf of the public and so it is important that the JSB and its decision-making process should be transparent.

The JSB's Rules of Procedure stipulate that any documents produced by the JSB are confidential unless the JSB decides otherwise. The rules are now being amended in order to reverse this principle, and all documents will be accessible to the public unless there is

deemed to be an overriding public interest against publication; if, for example, the publication of a particular document would seriously undermine the work of Europol.

Documents will be made accessible to the public either directly in electronic form (on the JSB's website) or following a written application. Each application for access to a document will result in an assessment of whether there is any reason why the document cannot be made available. In cases where only part of a document is subject to an exemption preventing publication, the document will be redacted and the edited version supplied.

The JSB aims to publish all new opinions together with decisions of the Appeals Committee on its website at http://europoljsb.ue.eu.int.

Chapter III

The Appeals Committee

Individuals have a right of access to information that Europol holds on them and they also have the right to ask for such information to be checked, corrected or deleted. If an individual attempts to exercise one of these rights and is not satisfied with Europol's response, an appeal can be lodged with the JSB's Appeals Committee. Although its membership is drawn from the JSB, the Appeals Committee is independent and impartial, and not bound by directions of the JSB. Decisions taken by the Appeals Committee are final for all parties involved.

Even though the Appeals Committee has only decided in two cases over the course of the past two years, the number of applications to appeal has increased and there are several cases now before the Committee. It is reasonable to suppose that the number of appeals will continue to increase — as individuals become more aware of Europol and their rights — and the Appeals Committee has therefore been careful to streamline its procedures to ensure that future appeals are dealt with expeditiously.

The two cases detailed below resulted in decisions on important matters of principle.

- In the first case, the Appeals Committee decided that Europol must consider each request for access on its merits rather than applying a blanket approach.

- In the second case, the Appeals Committee decided that Europol must respond to a request for access in the same language used by the individual making the request, provided that the language used was an official language of the European Union.

1. Summary of the Appeal lodged by Mr Y

Mr Y contacted the Dutch data protection authority to request access to any information that Europol might be holding on him. The request was forwarded to Europol.

Europol's reply concluded that:

'Following Article 19 of the Europol Convention in combination with the applicable legislation of The Netherlands, I would like to inform you that no data concerning you were

processed that the individual would be entitled to access in accordance with Article 19 of the Europol Convention.'

In response to this Mr Y lodged an appeal with the Appeals Committee, complaining about the 'veil of secrecy' surrounding Europol's decision.

The right of access is set out under Article 19 (1) of the Europol Convention and although the extent of the right is not specifically defined, it should (in view of Article 14 of the Convention) be regarded as the same right afforded by Article 8 of the 1981 Council of Europe Convention on data protection. This right enables the individual to establish whether personal data relating to him are held and, if so, affords him the right to have these data communicated to him. Mr Y's appeal involved both aspects of the right of access.

According to Article 19 (3), the right of access is to be exercised in accordance with the law of the Member State where the right is claimed, in this case the Netherlands. Article 19 (3) also states that where the law of the Member State provides for a 'communication concerning data' (which covers both the communication of whether data are processed and communication of those data that are processed) Europol must refuse such communication if this is necessary to: allow Europol to fulfil its duties properly; protect security and public order; prevent crime; or protect the rights of third parties.

The available exceptions to the right of access to police files under Dutch law are very similar to those listed in the Europol Convention, and the Appeals Committee determined that the provisions in both the Europol Convention and the Dutch law require that for every request for access there ought to be an assessment of whether it is necessary to make an exception to the full exercise of the right of access. Exceptions can only be allowed if the interests of the police or third parties outweigh the interest of the individual in exercising his right of access.

Europol's argument for neither confirming nor denying whether information was held on Mr Y hinged on Article 19 (4) of the Europol Convention. This article stipulates that if a Member State objects to the communication of data, Europol must inform the enquirer that checks have been made without providing any information which might reveal whether or not he is known. Europol argued that, in order to comply with this obligation, an individual could never be told outright that no data were held, since to do this would allow others, by comparing different responses received from Europol, to deduce that Europol was holding information on them. Thus, telling Mr Y that no data were held on him would result, so the argument went, in an indirect failure to comply with the obligation set out under Article 19 (4).

The Appeals Committee noted that although Article 19 (4) requires Europol to take account of the wishes of the different parties involved in the processing of the personal data in question, the provisions do not state what should happen in cases where no data are held.

The Appeals Committee therefore determined that the procedure in Article 19 (4) was not to be regarded as a duty for Europol in the same way as Article 19 (3). A request for access in cases where no data are processed must always be assessed on a case-by-case basis and Europol is not free to decide on that request relying only on an obligation that exists for situations where personal data are processed.

Having considered Europol's response to Mr Y's request for access, the Appeals Committee concluded that Europol's decision was not based on a individual assessment and was therefore not in compliance with Article 19 (3) of the Europol Convention. Europol should at least have verified whether the exceptions referred to in Article 19 (3) of the Europol Convention were applicable in this particular case. In the absence of any such evidence, or even of circumstances which suggested that this might be the case, Europol should not have refused a communication.

Europol's decision was deemed to have contravened the applicable Dutch law and Article 19 (3) of the Europol Convention. After a careful evaluation of the information available, the Appeals Committee concluded that in this case Article 19 (3) of the Europol Convention could not justify an exception to the right of access and, in accordance with Article 19 (7) of that Convention, the Appeals Committee decided that Europol should have made it clear to Mr Y that no data relating to him were being processed.

2. Summary of the Appeal lodged by Mr Z

After making a request for access (through the Belgian data protection authority), Mr Z received a response from Europol which concluded that:

'In accordance with the procedure as stipulated in the Europol Convention and the Belgian legislation, I would like to inform you that following your request checks of Europol files have been made. Following Article 19 of the Europol Convention in combination with Belgian legislation, I would like to inform you that no data concerning you are processed at Europol to which you are entitled to have access in accordance with Article 19 of the Europol Convention.'

Mr Z lodged an appeal with the Appeals Committee, subsequently informing the Committee that as he had 'chosen Dutch as the official language', he wanted a translation of Europol's decision, which had only been provided in English. Mr Z's appeal was deemed admissible on the basis of his complaint that he had not received a reply in his own language.

The Appeals Committee asked Europol why, given that all Mr Z's correspondence to Europol had been in Dutch, he had only ever received a response in English.

Europol informed the Committee that it was standard procedure to respond to Article 19 requests in English unless the applicant had stated that he wished to receive a response in his own language, in which case Europol would try to comply with this request provided that it did not involve disproportionate effort. Europol had not been informed, other than by the Appeals Committee, that Mr Z wished to receive a Dutch translation of the response to his request for access.

The Europol Convention does not include a specific language regime for Europol. However, in accordance with Article 14 of the Convention, the right of access to information held by Europol is to be regarded as the same right afforded by Article 8 of the 1981 Council of Europe Convention on data protection. According to Article 8 of the Council of Europe Convention, an individual has the right to have confirmation of whether personal data relating to him are stored in automated files and, if so, to have such data communicated to him 'in an intelligible form'. The Appeals Committee was of the view that the language in which the information was provided was relevant in determining whether a response could be considered intelligible.

Taking into account Europol's position as an EU body involving the active participation of the law enforcement authorities of each Member State, the Appeals Committee suggested that Europol, when dealing with requests for access under Article 19 of the Europol Convention, should apply a similar rule to that found in Article 21 of the Treaty establishing the European Community. Article 21 provides that if an individual writes to certain EU bodies in any of the EU's official languages, he can expect to receive an answer in the same language.

The Appeals Committee decided that Europol had not complied with the principles of Article 8 of the 1981 Council of Europe Convention when responding to Mr Z's request for access: Europol should have communicated its decision in the same language used by Mr Z even though he did not request this specifically. As the right of access exists to allow individuals to ensure that information about them is being held in accordance with the law, Europol must provide applicants with a response in their own language — where this is an official language of the EU.

In closing, the Committee noted that as Europol had subsequently provided Mr Z with a Dutch translation of the original decision, no further action would be necessary in this case. The Appeals Committee understands that Europol has since updated its procedures and now responds to requests for access in the language used by the applicant.

- All decisions of the Appeals Committee, together with additional information on the rights available under the Europol Convention, can be found on the JSB's website at http://europoljsb.ue.eu.int

Chapter IV

The Past Two Years

The opening chapter of this report gives an account of the way in which the JSB approached two different situations that came about as the EU was forced to reflect on its security.

In dealing with these cases the JSB adopted a pragmatic approach. The JSB's opinion on Europol's agreement with the US, with its recognition of the need to improve co-operation, has come in for some criticism from certain quarters. Nonetheless, the JSB remains committed to monitoring the implementation of the agreement to ensure that there is compliance with its provisions.

The JSB was proactive in proposing an amendment to the Europol Convention, and the proposal itself reflects the JSB's view that the data protection provisions contained within the Europol Convention are not intended to impede Europol's work, rather they are there to ensure that Europol respects the rights of individuals as it goes about its lawful tasks.

Although the addition of new colleagues from the ten new Member States has obviously made a significant difference to the JSB as a body, the enlargement has proved successful and the JSB is now benefiting from the combined experience of its new members.

The JSB has continued to carry out its oversight function, examining all the agreements that Europol has drawn up with third states and bodies and scrutinising orders to open analysis files — and the JSB places particular importance on its inspections of Europol, as these provide the inspection team with first-hand experience of Europol's work and offer an insight into how written procedures intended to safeguard rights actually work in practice. The JSB has found Europol staff to be extremely co-operative during these inspections — and follow-up inspections would suggest that Europol gives priority to implementing the JSB's recommendations.

Over the course of the past two years the JSB has tried to be constructive in its approach, while ensuring that safeguards are in place to protect fundamental rights.

The Future

There have been many developments involving Europol over the past two years and there are signs that Europol's role will continue to evolve. The creation of joint investigation teams, for example, suggests that Europol's activities are likely to become increasingly operational in nature.

At the same time, developments elsewhere — particularly plans for a second-generation Schengen Information System — have resulted in suggestions that EU-wide information systems with related purposes might be made interoperable. Any such moves ought to be approached with caution, not least because of the problems that have been encountered in developing the Europol Information System. Furthermore, any moves in this direction ought to be preceded by a privacy-impact assessment, which would assess the potential implications for the rights of individuals.

Data protection safeguards must keep pace with developments, and it will be particularly important to ensure that there is effective supervision of Europol — as well as the other EU-wide information systems. For its part, the JSB has taken steps to improve co-operation with other data protection authorities in an attempt to overcome the rather rigid arrangements for supervising data protection at EU level. The JSB would expect to contribute to any discussion on how these arrangements might be improved.

There is also the wider issue of parliamentary scrutiny of Europol. In 2002 the Commission arrived at the conclusion that the existing controls in place to supervise the work of Europol — exercised by national parliaments, the European Parliament, national data protection authorities, the JSB and the Europol Management Board — were not 'insufficient'. It was noted, however, that the indirect and fragmented nature of much of this control would suggest that 'something clearer and more transparent is needed'.[4]

Such issues fall outside the remit of the JSB but it is clear that as Europol's tasks become increasingly operational, control and scrutiny of Europol's work will have to adapt to take account of this.

[4] Communication from the Commission to the European Parliament and the Council — Democratic Control over Europol 26 February 2002 (COM (2002) 95 final)

Objectives for the coming two years

Over the next two years the JSB will strive to:

- carry out annual inspections of Europol, paying particular attention to the implementation of the Europol Information System;

- raise its profile within the EU institutions to ensure that data protection concerns are taken into account when new initiatives involving Europol are being drawn up. In particular, the JSB intends to propose that there should be regular contact with the European Parliament's Committee on Civil Liberties, Justice and Home Affairs;

- work with new colleagues from the accession countries, helping them to inform national police authorities of the Europol Convention's data protection provisions;

- work with its sister authorities and the wider data protection community to present a coherent and constructive response to new initiatives involving the use of personal data for the purposes of law enforcement;

- raise awareness of the rights afforded to individuals by the Europol Convention; and,

- continue to scrutinise orders opening new analysis files and agreements to exchange personal data with third states and bodies.