Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA) (repealed)

CHAPTER V

DATA PROTECTION AND DATA SECURITY

Article 27

Standard of data protection

Without prejudice to specific provisions of this Decision, Europol shall take account of the principles of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and of Recommendation No R (87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987. Europol shall observe those principles in the processing of personal data, inter alia, in respect of automated and non-automated data held in the form of data files, especially any structured set of personal data accessible in accordance with specific criteria.

Article 28

Data Protection Officer

1 The Management Board shall appoint, on the proposal of the Director, a Data Protection Officer who shall be a member of the staff. In the performance of his or her duties, he or she shall act independently.

2 The Data Protection Officer shall in particular have the following tasks:

- a ensuring, in an independent manner, lawfulness and compliance with the provisions of this Decision concerning the processing of personal data, including the processing of personal data relating to Europol staff;
- b ensuring that a written record of the transmission and receipt of personal data is kept in accordance with this Decision;
- c ensuring that data subjects are informed of their rights under this Decision at their request;
- d cooperating with Europol staff responsible for procedures, training and advice on data processing;
- e cooperating with the Joint Supervisory Body;
- f preparing an annual report and communicating that report to the Management Board and to the Joint Supervisory Body.

3 In the performance of his or her tasks, the Data Protection Officer shall have access to all the data processed by Europol and to all Europol premises.

4 If the Data Protection Officer considers that the provisions of this Decision concerning the processing of personal data have not been complied with, he or she shall inform the Director, requiring him or her to resolve the non-compliance within a specified time.

If the Director does not resolve the non-compliance of the processing within the specified time, the Data Protection Officer shall inform the Management Board and shall agree with the Management Board a specified time for a response.

If the Management Board does not resolve the non-compliance of the processing within the specified time, the Data Protection Officer shall refer the matter to the Joint Supervisory Body.

5 The Management Board shall adopt further implementing rules concerning the Data Protection Officer. Those implementing rules shall in particular concern selection and dismissal, tasks, duties and powers and safeguards for the independence of the Data Protection Officer.

Article 29

Responsibility in data protection matters

1 The responsibility for data processed at Europol, in particular as regards the legality of the collection, the transmission to Europol and the input of data, as well as their accuracy, their up-to-date nature and verification of the storage time limits, shall lie with:

a the Member State which input or otherwise communicated the data;

b Europol in respect of data communicated to Europol by third parties, including data communicated by private parties in accordance with Article 25(3)(b) and (c) and Article 25(4) as well as data communicated via the contact point of a third State with which Europol has concluded a cooperation agreement in accordance with Article 23 or which result from analyses conducted by Europol.

2 Data which have been transmitted to Europol but have not yet been input in one of Europol's data files shall remain under the data-protection responsibility of the party transmitting the data. Europol shall, however, be responsible for ensuring the security of the data in accordance with Article 35(2) in that until such data have been input in a data file, they may be accessed only by authorised Europol staff for the purpose of determining whether they can be processed at Europol, or by authorised officials of the party which supplied the data. If Europol, after appraising them, has reason to assume that data supplied are inaccurate or no longer up-to-date, it shall inform the party which supplied the data.

3 In addition, subject to other provisions in this Decision, Europol shall be responsible for all data processed by it.

4 If Europol has evidence that data input into one of its systems referred to in Chapter II are factually incorrect or have been unlawfully stored, it shall inform the Member State or other party involved accordingly.

5 Europol shall store data in such a way that it can be established by which Member State or third party they were transmitted or whether they are the result of an analysis by Europol.

Article 30

Individual's right of access

1 Any person shall be entitled, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed by Europol and to have such data communicated to him or her in an intelligible form, or checked, in all cases under the conditions laid down in this Article.

2 Any person wishing to exercise his or her rights under this Article may make a request to that effect without excessive costs in the Member State of his or her choice to the authority appointed for that purpose in that Member State. That authority shall refer the request to Europol without delay, and in any case within one month of receipt.

3 The request shall be answered by Europol without undue delay and in any case within three months of its receipt by Europol in accordance with this Article.

4 Europol shall consult the competent authorities of the Member States concerned before deciding on its response to a request under paragraph 1. A decision on access to data shall be conditional upon close cooperation between Europol and the Member States directly concerned by the communication of such data. In any case in which a Member State objects to Europol's proposed response, it shall notify Europol of the reasons for its objection.

5 The provision of information in response to a request under paragraph 1 shall be refused to the extent that such refusal is necessary to:

a enable Europol to fulfil its tasks properly;

b protect security and public order in the Member States or to prevent crime;

c guarantee that any national investigation will not be jeopardised;

d protect the rights and freedoms of third parties.

When the applicability of an exemption is assessed, the interests of the person concerned shall be taken into account.

6 If the provision of information in response to a request under paragraph 1 is refused, Europol shall notify the person concerned that it has carried out checks, without giving any information which might reveal to him or her whether or not personal data concerning him or her are processed by Europol.

7 Any person shall have the right to request the Joint Supervisory Body, at reasonable intervals, to check whether the manner in which his or her personal data have been collected, stored, processed and used by Europol is in compliance with the provisions of this Decision concerning the processing of personal data. The Joint Supervisory Body shall notify the person concerned that it has carried out checks, without giving any information which might reveal to him or her whether or not personal data concerning him or her are processed by Europol.

Article 31

Data subject's right to correctionand deletion of data

1 Any person shall have the right to ask Europol to correct or delete incorrect data concerning him or her. If it emerges, either on the basis of the exercise of this right or otherwise, that data held by Europol which have been communicated to it by third parties or which are the result of its own analyses are incorrect or that their input or storage is in breach of this Decision, Europol shall correct or delete such data.

2 If data that are incorrect or processed in breach of this Decision were transmitted directly to Europol by Member States, the Member States concerned shall correct or delete such data in collaboration with Europol.

3 If incorrect data were transmitted by another appropriate means or if the errors in the data supplied by Member States are due to faulty transmission or were transmitted in breach of this Decision or if they result from their being input, taken over or stored in an incorrect manner

or in breach of this Decision by Europol, Europol shall correct or delete the data in collaboration with the Member States concerned.

4 In the cases referred to in paragraphs 1, 2 and 3, the Member States or third parties which have received the data shall be notified forthwith. The recipient Member States and the third parties shall also correct or delete those data. Where deletion is not possible, the data shall be blocked to prevent any future processing.

5 The data subject making the request shall be informed by Europol in writing without undue delay and in any case within three months that data concerning him or her have been corrected or deleted.

Article 32

Appeals

1 In its reply to a request for a check, for access to data, or for correction and deletion of data, Europol shall inform the person making the request that if he or she is not satisfied with the decision, he or she may appeal to the Joint Supervisory Body. Such person may also refer the matter to the Joint Supervisory Body if there has been no response to his or her request within the time limit laid down in Article 30 or 31.

2 If the person making the request lodges an appeal to the Joint Supervisory Body, the appeal shall be examined by that body.

3 Where an appeal relates to a decision as referred to in Article 30 or 31, the Joint Supervisory Body shall consult the national supervisory bodies or the competent judicial body in the Member State which was the source of the data or the Member State directly concerned. The decision of the Joint Supervisory Body, which may extend to a refusal to communicate any information, shall be taken in close cooperation with the national supervisory body or competent judicial body.

4 Where an appeal relates to access to data input by Europol in the Europol Information System or data stored in the analysis work files or in any other system established by Europol for the processing of personal data pursuant to Article 10 and where objections from Europol persist, the Joint Supervisory Body shall be able to overrule such objections only by a majority of two thirds of its members after having heard Europol and the Member State or Member States referred to in Article 30(4). If there is no such majority, the Joint Supervisory Body shall notify the person making the request of the refusal, without giving any information which might reveal the existence of any personal data concerning that person.

5 Where an appeal relates to the checking of data input by a Member State in the Europol Information System or of data stored in the analysis work files or in any other system established by Europol for the processing of personal data pursuant to Article 10, the Joint Supervisory Body shall ensure that the necessary checks have been carried out correctly in close cooperation with the national supervisory body of the Member State which has input the data. The Joint Supervisory Body shall notify the person making the request that it has carried out the checks, without giving any information which might reveal the existence of any personal data concerning that person.

6 Where an appeal relates to the checking of data input by Europol in the Europol Information System or of data stored in the analysis work files or in any other system established by Europol for the processing of personal data pursuant to Article 10, the Joint Supervisory Body shall ensure that the necessary checks have been carried out by Europol. The Joint Supervisory

Body shall notify the person making the request that it has carried out the checks, without giving any information which might reveal the existence of any personal data concerning that person.

Article 33

National supervisory body

1 Each Member State shall designate a national supervisory body with the task to monitor independently, in accordance with its national law, the permissibility of the input, the retrieval and any communication to Europol of personal data by the Member State concerned and to examine whether such input, retrieval or communication violates the rights of the data subject. For that purpose, the national supervisory body shall have access, at the national unit or at liaison officers' premises, to the data input by the Member State in the Europol Information System or in any other system established by Europol for the processing of personal data pursuant to Article 10 in accordance with the relevant national procedures.

For the purpose of exercising their supervisory function, national supervisory bodies shall have access to the offices and documents of their respective liaison officers at Europol.

In addition, in accordance with the relevant national procedures, the national supervisory bodies shall supervise the activities of national units and the activities of liaison officers, in so far as such activities are of relevance to the protection of personal data. They shall also keep the Joint Supervisory Body informed of any actions they take with respect to Europol.

2 Any person shall have the right to request the national supervisory body to ensure that the input or communication to Europol of data concerning him or her in any form and the consultation of the data by the Member State concerned are lawful.

This right shall be exercised in accordance with the national law of the Member State in which the request is made.

Article 34

Joint Supervisory Body

1 An independent Joint Supervisory Body shall be set up to review, in accordance with this Decision, the activities of Europol in order to ensure that the rights of the individual are not violated by the storage, processing and use of the data held by Europol. In addition, the Joint Supervisory Body shall monitor the permissibility of the transmission of data originating from Europol. The Joint Supervisory Body shall be composed of a maximum of two members or representatives, where appropriate assisted by alternates, of each of the independent national supervisory bodies, having the necessary abilities and appointed for five years by each Member State. Each delegation shall be entitled to one vote.

The Joint Supervisory Body shall choose a chairman from among its members.

In the performance of their duties, the members of the Joint Supervisory Body shall not receive instructions from any other body.

2 Europol shall assist the Joint Supervisory Body in the performance of the latter's tasks. In doing so, it shall in particular:

a supply the information the Joint Supervisory Body requests and give it access to all documents and paper files as well as to the data stored in its data files;

b allow the Joint Supervisory Body free access at all times to all its premises;

c implement the Joint Supervisory Body's decisions on appeals.

3 The Joint Supervisory Body shall be competent to examine questions relating to implementation and interpretation in connection with Europol's activities as regards the processing and use of personal data, to examine questions relating to checks carried out independently by the national supervisory bodies of the Member States or relating to the exercise of the right of access, and to draw up harmonised proposals for common solutions to existing problems.

4 If the Joint Supervisory Body identifies any violations of the provisions of this Decision in the storage, processing or use of personal data, it shall make any complaints it deems necessary to the Director and shall request him to reply within a specified time limit. The Director shall keep the Management Board informed of the entire procedure. If it is not satisfied with the response given by the Director to its request, the Joint Supervisory Body shall refer the matter to the Management Board.

5 For the fulfilment of its tasks and to contribute to the improvement of consistency in the application of the rules and procedures for data processing, the Joint Supervisory Body shall cooperate as necessary with other supervisory authorities.

6 The Joint Supervisory Body shall draw up activity reports at regular intervals. Such reports shall be forwarded to the European Parliament and to the Council. The Management Board shall have the opportunity to make comments, which shall be attached to the reports.

The Joint Supervisory Body shall decide whether or not to publish its activity report, and, if it decides to do so, shall determine how it should be published.

7 The Joint Supervisory Body shall adopt its rules of procedure by a majority of two thirds of its members and shall submit them to the Council for approval. The Council shall act by qualified majority.

8 The Joint Supervisory Body shall set up an internal committee comprising one qualified representative from each Member State with the right to vote. The committee shall have the task of examining the appeals provided for in Article 32 by all appropriate means. Should they so request, the parties, assisted by their advisers if they so wish, shall be heard by the committee. The decisions taken in this context shall be final as regards all the parties concerned.

9 The Joint Supervisory Body may set up one or more other committees in addition to the one referred to in paragraph 8.

10 The Joint Supervisory Body shall be consulted on that part of Europol's budget which concerns it. Its opinion shall be annexed to the draft budget in question.

11 The Joint Supervisory Body shall be assisted by a secretariat, the tasks of which shall be defined in the rules of procedure.

Article 35

Data security

1 Europol shall take the necessary technical and organisational measures to ensure the implementation of this Decision. Measures shall be considered necessary where the effort they involve is proportionate to the objective they are designed to achieve in terms of protection.

2 In respect of automated data processing at Europol, each Member State and Europol shall implement measures designed to:

a deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

b prevent the unauthorised reading, copying, modification or removal of data media (data media control);

c prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

d prevent the use of automated data-processing systems by unauthorised persons using data-communication equipment (user control);

e ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation (data access control);

f ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted using data communication equipment (communication control);

g ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);

h prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during the transportation of data media (transport control);

i ensure that installed systems may, in the event of interruption, be restored immediately (recovery);

j ensure that the functions of the system perform without fault, that the appearance of faults in the functions is immediately reported (reliability) and that stored data cannot be corrupted by system malfunctions (integrity).