(Acts adopted under Title VI of the Treaty on European Union)

RULES OF PROCEDURE ON THE PROCESSING AND PROTECTION OF PERSONAL DATA AT EUROJUST

(Text adopted unanimously by the college of Eurojust during the meeting of 21 October 2004 and approved by the Council on 24 February 2005)

(2005/C 68/01)

TITLE I

DEFINITIONS

Article 1

Definitions

For the purpose of these rules and any other text implementing them:

(a) *'Eurojust Decision'* means the Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, as modified by the Council Decision of 18 June 2003;

(b) *'The College'* means the College of Eurojust, as referred to in Article 10 of the Eurojust Decision;

(c) *'National Member'* means the National Member seconded to Eurojust by each Member State, as referred to in Article 2(1) of the Eurojust Decision;

(d) *'Assistant'* means a person who may assist each National Member, as referred to in Article 2(2) of the Eurojust Decision;

(e) *'Eurojust's staff'* means the Administrative Director, as referred to in Article 29 of the Eurojust Decision, as well as the staff referred to in Article 30 of the Eurojust Decision;

(f) *'the Data Protection Officer'* means the person appointed in accordance with Article 17 of the Eurojust Decision;

(g) *'the Joint Supervisory Body'* means the independent body established in accordance with Article 23 of the Eurojust Decision;

(h) *'personal data'* means any information relating to an identified or identifiable natural person (*'data subject'*); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

(i) *'processing of personal data'* (*'processing'*) means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(j) *'personal data filing system'* (*'filing system'*) means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(k) *'controller'* means the person, who alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or European laws or regulations, the controller or the specific criteria for his nomination may be designated by national or European law;

(l) *'processor'* means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(m) *'third party'* means any natural or legal person, public authority, agency or any body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process data; and

(n) *'recipient'* means a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not.

TITLE II

SCOPE OF APPLICATION AND STRUCTURE

Article 2

Scope of application

1. The present rules of procedure shall apply to the processing of personal data by Eurojust, wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system in accordance with the Eurojust Decision.

2. The present rules shall apply to all information collected and further processed by Eurojust, that is to say, information drawn up or received by it and in its possession, concerning matters relating to the policies, activities and decisions falling within Eurojust's sphere of responsibility.

3. The present rules shall not apply to information which has been transmitted to a National Member of Eurojust exclusively in the context of his or her judicial powers, as defined in Article 9(3) of the Eurojust Decision.

Article 3

Structure

1. All personal data shall be considered case-related or non-case-related. Personal data shall be considered as case-related if it is linked to the operational tasks of Eurojust, as defined in Articles 5, 6 and 7 of the Eurojust Decision.

2. Case-related data shall be processed in accordance with Titles III and IV. Non-case-related data shall be processed in accordance with Titles III and V.

TITLE III

PRINCIPLES OF GENERAL APPLICATION TO EUROJUST

Article 4

Right to privacy and data protection

Eurojust shall act in full respect of the human rights and fundamental freedoms of individuals and in particular of their right to privacy with regard to the processing of their personal data, regardless of nationality or place of residence.

Article 5

Principles of lawfulness and fairness, proportionality and necessity of processing

1. Personal data must be processed fairly and lawfully.

2. Eurojust shall only process personal data that are necessary, adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.

3. Eurojust shall define its processing operations and systems in accordance with the aim of collecting or further processing only personal data that are necessary as defined in paragraph 2. In particular, use is to be made of the possibilities for aliasing and rendering data anonymous, in so far as this is possible, taking into account the purpose of the processing and that the effort involved is reasonable.

Article 6

Data quality

1. Eurojust shall ensure that personal data are accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

2. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed, in accordance with Article 5(2).

Article 7

Data security

1. In accordance with Article 22 of the Eurojust Decision and with the present rules, Eurojust shall put in place the necessary technical measures and organisational arrangements to protect personal data against accidental or unlawful destruction, accidental loss or unauthorised disclosure, alteration, access or any unauthorised form of processing. In particular, measures must be taken to ensure that only those authorised to access personal data can have access to such data.

2. All measures taken shall be appropriate to the risks presented by the processing and to the nature of the data processed.

3. Eurojust shall develop a comprehensive security policy in accordance with Article 22(2) of the Eurojust Decision and with these rules. This policy shall take full account of the sensitivity of the work carried out by the judicial cooperation unit and shall include rules regarding classification of documents, screening of personnel working for Eurojust and actions to be taken in the case of security breaches. The Joint Supervisory Body shall be consulted regarding the security policy of Eurojust.

4. All Eurojust postholders shall be adequately informed about the Eurojust security policy and shall be required to use the technical and organisational measures put at their disposal in line with the applicable data protection and security requirements.

Article 8

Right of information to the data subjects

1. Without prejudice to the special provisions in Title IV in respect of case-related data and in Title V in respect of non-case-related data, data subjects must be provided with information as to the purpose of the processing and the identity of the data controller, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him or her and any further information such as the legal basis of the processing operation for which the data are intended, the time limits for storing the data and the right to have recourse at any time to the Joint Supervisory Body in so far as such further information is necessary, having regard to the purposes and the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. This information must be provided at the latest at the moment of the collection of the data from the data subject or, when receiving the data from a third party, at the time of undertaking the recording of personal data or, if disclosure to a third party is envisaged, no later than the time when the data are first disclosed or, in the cases provided for in Chapter II of Title IV of these rules, as soon as the purposes of the processing, national investigations and prosecutions and the rights and freedoms of third parties are not likely to be jeopardised.

Article 9

Rights of the data subjects to access, correction, blocking and deletion

1. The data subject shall have a right to access, correction, blocking, and, as the case may be, deletion. Eurojust shall define, where necessary in cooperation with the respective national authorities involved, procedures to facilitate the exercise of these rights by data subjects.

2. The Data Protection Officer shall ensure that data subjects are informed of their rights at their request.

Article 10

Confidentiality of processing

In accordance with Article 25 of the Eurojust Decision, all persons called upon to work within and with Eurojust are bound by strict confidentiality obligations. All necessary measures shall be taken by Eurojust to ensure that these obligations are complied with and that any breaches of such obligations are promptly reported to the Data Protection Officer and the head of the Security Department, who shall ensure that appropriate steps are taken.

Article 11

Internal processors

Unless required to do so by national or European law, a person acting as processor within Eurojust, with access to personal data, shall not process them except on instructions from the controller.

Article 12

Enquiries, information requests and claims by Eurojust postholders

1. For the purposes of Article 17(2) and (4) of the Eurojust Decision, the Data Protection Officer shall, on request, provide information to any Eurojust postholder regarding data processing activities of Eurojust. The Data Protection Officer shall respond to enquiries and act on any information requests or claims regarding an alleged breach of the provisions of the Eurojust Decision, these rules or any other rules governing the processing of personal data by Eurojust. No one shall suffer prejudice on account of having raised an alleged breach of the provisions governing the processing of personal data with the Data Protection Officer.

2. All persons working at Eurojust shall cooperate with the College, the National Members, the Data Protection Officer and the Joint Supervisory Body in the framework of enquiries, investigations, audits or any other data protection related activities.

TITLE IV

RULES FOR CASE-RELATED PROCESSING OPERATIONS

CHAPTER I

Conditions to make the processing of personal data legitimate

Article 13

Personal data processed in the context of case-related activities

1. In the context of case-related activities, Eurojust shall, insofar as it is necessary to achieve its objectives, process personal data by automated means or in structured manual files in accordance with Articles 14, 15 and 16 of the Eurojust Decision.

2. The National Member/s processing personal data concerning individual cases shall determine the purposes and means of the processing of personal data and shall be therefore considered as controller or, where applicable, co-controllers.

Article 14

Lawfulness and fairness of processing

Personal data may be collected and further processed in the context of case-related activities insofar as the processing is necessary for the performance of the tasks of Eurojust in reinforcing the fight against serious crime.

Article 15

Purpose limitation

Personal data processed by Eurojust in the framework of investigations and prosecutions shall under no circumstances be processed for any other purpose.

Article 16

Data quality

1. When information is transmitted to Eurojust by a Member State or an external party in the context of an investigation or prosecution, it shall not be responsible for the correctness of the information received but shall ensure, from the moment of reception, that all reasonable steps are taken to keep the information updated.

2. If Eurojust detects any inaccuracy affecting the data in question, it shall inform the third party from whom the information was received and shall correct the information.

Article 17

Special categories of data

1. Eurojust shall take appropriate technical measures to ensure that the Data Protection Officer is automatically informed of the exceptional cases in which recourse is made to Article 15(4) of the Eurojust Decision. The case management system shall ensure that such data can not be included in the index referred to in Article 16(1) of the Eurojust Decision.

2. When such data refer to witnesses or victims within the meaning of Article 15(2) of the Eurojust Decision the case management system shall not record this information unless a decision of the College is documented.

Article 18

Processing of the categories of personal data referred to in Article 15(3) of the Eurojust Decision

1. Eurojust shall take appropriate technical measures to ensure that the Data Protection Officer is automatically informed of the exceptional cases in which, for a limited period of time, recourse is made to Article 15(3) of the Eurojust Decision.

2. When such data refer to witnesses or victims within the meaning of Article 15(2) of the Eurojust Decision, the case management system shall not record this information unless a decision taken jointly by at least two National Members is documented.

CHAPTER II

Rights of the data subjects

Article 19

Right of information of the data subjects

1. In the context of the operational work of Eurojust, data subjects shall be provided with information as to the processing, as soon as it is apparent that the provision of this information to the data subject would not undermine:

(a) the fulfilment of Eurojust's tasks in reinforcing the fight against serious crime; or

(b) national investigations and prosecutions in which Eurojust assists; or

(c) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in clauses (a) and (b); or

(d) the rights and freedoms of third parties.

2. Recourse to the cases enumerated in paragraph 1 shall be recorded in the temporary work file related to the case, mentioning the basis for the decision which has been taken by the National Member(s) responsible for this file.

Article 20

Right of access of the data subjects

Every individual shall be entitled to have access to personal data concerning him or her processed by Eurojust under the circumstances laid down in Article 19 of the Eurojust Decision.

Article 21

Procedure for the exercise of the rights of the data subjects

1. Individuals wishing to exercise their rights as data subjects may address their requests directly to Eurojust or through the authority appointed for this purpose in the Member State of his or her choice, which shall transmit the request to Eurojust.

2. Requests for the exercise of rights shall be dealt with by the National Member(s) concerned with the request, who shall provide a copy of the request to the Data Protection Officer for its registration.

3. The National Member(s) concerned with the request shall carry out the necessary checks and inform the Data Protection Officer of the decision reached in the specific case. This decision will take full account of these rules and of the legislation applicable to the request as defined in Article 19(3) of the Eurojust Decision, of the grounds for denial enumerated in Article 19(4) of the Eurojust Decision and of consultations with the competent law enforcement authorities that shall take place before reaching a decision, as stated in Article 19(9) of the Eurojust Decision.

4. The Data Protection Officer shall, should the case so require, carry out additional checks in the case management system and inform the National Member(s) concerned if any additional relevant information has been found through these checks. The National Member(s) concerned may, on the basis of the information provided by the Data Protection Officer, decide to reconsider the initial decision.

5. The Data Protection Officer shall communicate the final decision taken by the National Member(s) concerned to the data subject, in line with Article 19(6) of the Eurojust Decision, and shall inform the data subject of the possibility to appeal to the Joint Supervisory Body if he or she is not satisfied with the reply given by Eurojust.

6. The request shall be dealt with in full within three months of receipt. The data subject may refer the matter to the Joint Supervisory Body if there has not been a response to his or her request within this time limit.

7. In the cases where the request has been received through a national authority, the National Member(s) concerned shall ensure that this authority is informed of the fact of a reply given by the Data Protection Officer to the data subject.

8. Eurojust shall put in place cooperation procedures with the national authorities appointed for the purpose of dealing of data subjects' rights to ensure that requests are adequately and timely forwarded to Eurojust.

Article 22

Information to third parties following correction, blocking or deletion of case-related personal data

Eurojust shall put in place appropriate technical measures to ensure that, in the cases where Eurojust corrects, blocks or erases personal data following a request, a list of the suppliers and addresses of these data is automatically produced. In accordance with Article 20(5) of the Eurojust Decision, the controller shall ensure that those included in the list are informed of the changes performed on the personal data.

CHAPTER III

Data security issues

Article 23

Automated case management system

1. Eurojust shall put in place an automated case management system integrating a filing system, that shall be used by the National Members when dealing with case-related activities and which shall include the temporary work files and index as defined in Article 16 of the Eurojust Decision. This system shall include functionalities such as case management, description of the workflow, cross-references of information and security.

2. The case management system shall be approved by the College after having consulted the Data Protection Officer, the Joint Supervisory Body and the relevant Eurojust staff and shall take full account of the requirements of Article 22 and any other relevant provisions of the Eurojust Decision.

3. The case management system shall enable National Members to identify the purpose and specific objectives for which a temporary work file is opened, within the framework of the tasks mentioned in Articles 5, 6 and 7 of the Eurojust Decision.

Article 24

Temporary work files and index

1. In accordance with Articles 14(4) and 16 of the Eurojust Decision, Eurojust shall establish an index of data relating to investigations and temporary work files which also contain personal data. Both the index and the temporary work files shall form part of the case management system referred to in Article 23 and shall respect the restrictions on the processing of personal data established in Article 15 of the Eurojust Decision.

2. National Members shall be responsible for the opening of new temporary work files linked to the cases they are dealing with. The case management system shall automatically allocate a reference number (identifier) to each new temporary work file opened.

3. Eurojust shall put in place an automated case management system allowing National Members to keep the personal data they process in a temporary work file restricted or to give access to it or to part(s) of it to other National Member(s) involved in the case to which the file relates. The case management system shall allow them to define the specific items of personal and non-personal data to which they wish to give access to other National Member(s), Assistant(s) or authorised staff members that are involved in the handling of the case as well as to select the items of information they wish to introduce in the index, in accordance with Articles 14 and 15 of the Eurojust Decision and ensuring that, at least, the following items are included in the index: reference to the temporary work file; types of crime; Member States, international organisations and bodies and/or authorities of third States involved; involvement of the European Commission or EU bodies and entities; objectives and status of the case (open/closed).

4. When a National Member gives access to a temporary work file or a part of it to one or more involved National Member(s), the case management system shall ensure that the authorised users have access to the relevant parts of the file but that they can not modify the data introduced by the original author. The authorised users can, however, add any relevant information to the new parts of the temporary work files. Likewise, information contained in the index can be read by all authorised users of the system but can only be modified by its original author.

5. The Data Protection Officer shall be automatically informed by such a system of the creation of each new work file that contains personal data and, in particular, of the exceptional cases in which recourse is made to Article 15(3) of the Eurojust Decision. The case management system shall mark such data in a way that will remind the person who has introduced the data in the system of the obligation to keep these data for a limited period of time. When such data refer to witnesses or victims within the meaning of Article 15(2) of the Eurojust Decision, the system shall not record this information unless a decision taken jointly by at least two National Members has been documented.

6. The case management system shall automatically inform the Data Protection Officer of the exceptional cases in which recourse is made to Article 15(4) of the Eurojust Decision. When such data refer to witnesses or victims within the meaning of Article 15(2) of the Eurojust Decision, the system shall not record this information unless a decision taken by the College has been documented.

7. The case management system shall ensure that only personal data referred in Article 15(1)(a) to (i) and (k) and Article 15(2) of the Eurojust Decision can be recorded in the index.

8. The information contained in the index must be sufficient to comply with the tasks of Eurojust and, in particular, with the objectives of Article 16(1) of the Eurojust Decision.

Article 25

Log files and audit trails

1. Eurojust shall put in place appropriate technical measures to ensure that a record is kept of all processing operations carried out upon personal data. The case management system shall in particular ensure that a record of transmission and receipt of data as defined in Article 17(2)(b) of the Eurojust Decision is kept for the purposes of Article 19(3) of the Eurojust Decision. Such record shall ensure, as required by Article 22 of the Eurojust Decision, that it is possible to verify and establish to which bodies personal data are transmitted and which personal data have been input into automated data processing systems and when and by whom the data were input.

2. The Data Protection Officer shall review these records regularly in order to be able to assist the National Members and the College regarding any data protection issue and shall make the necessary enquiries in cases of irregularities. Where necessary, the Data Protection Officer shall inform the College and the Joint Supervisory Body following the procedure established in Article 17(4) of the Eurojust Decision of any data protection breaches evidenced by the abovementioned records. The Data Protection Officer will ensure that, where appropriate, the Administrative Director is informed, to enable him or her to take the necessary measures within the administration.

3. The Data Protection Officer shall give full access to the Joint Supervisory Body to the records referred in paragraph 1 when so requested.

Article 26

Authorised access to personal data

1. Eurojust shall take appropriate technical measures and provide for organisational arrangements to ensure that only National Members, their Assistants and authorised Eurojust staff have, for the purpose of achieving Eurojust's objectives, access to personal data processed by Eurojust in the framework of its operational activities.

2. These measures shall take account of the purposes for which the data have been collected and further processed, the state of the art, the level of security required by the sensitive nature of the work carried out by Eurojust and the requirements imposed by Article 22 of the Eurojust Decision.

3. Each National Member of Eurojust shall document and inform the Data Protection Officer regarding the access policy he or she has authorised within his or her national desk regarding case-related files. In particular, National Members shall ensure that appropriate organisational arrangements are made and complied with and that proper use is made of the technical and organisational measures put at their disposal by Eurojust.

4. The College may authorise other Eurojust staff to have access to case-related files where necessary for the performance of the tasks of Eurojust.

Article 27

Audits and control

1. The Data Protection Officer shall monitor the lawfulness and compliance with the provisions of the Eurojust Decision, the present Rules of Procedure and any other rules regarding the processing of personal data applicable to Eurojust. To that end, the Data Protection Officer shall assist the National Members regarding data protection questions and shall run annual surveys on the compliance with the abovementioned rules within Eurojust. The Data Protection Officer shall report to the College and the Joint Supervisory Body on the results of these surveys as well as on any other relevant developments within Eurojust. The Data Protection Officer will ensure that, where appropriate, the Administrative Director is informed, to enable him/her to take the necessary measures within the administration.

2. The Joint Supervisory Body shall carry out controls and audits in accordance with Article 23(7) of the Eurojust Decision.

CHAPTER IV

Data flows to third parties or organisations

Article 28

Data flows to third parties or organisations

1. Eurojust shall endeavour to put in place cooperation agreements containing suitable provisions regarding exchange of personal data with all partners with whom exchanges of data take place on a regular basis.

2. Without prejudice to the cases in which such cooperation agreements are in place, Eurojust shall only transfer personal data to a third country or to any of the entities referred to in Article 27(1) of the Eurojust Decision if they are subject to the Convention for the Protection of the Individuals with regard to Automatic Processing of Personal Data signed in Strasbourg on 28 January 1981 or when an adequate level of protection is ensured.

3. The decision concerning transfers to non-parties of the Council of Europe Convention of 28 January 1981 shall be taken by the National Member(s) involved, on the basis of the assessment concerning the adequacy of the level of protection made by the Data Protection Officer. The adequacy of the level of protection shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment will result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the state or organisation in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer. Such safeguards may in particular be the result of written agreements binding the controller who makes the transfer and the recipient who is not subject to the jurisdiction of a party to the Convention. The content of the agreements concerned must include the relevant elements of data protection. In cases where the assessment of the level of protection raises difficulties, the Data Protection Officer shall consult the Joint Supervisory Body before making an assessment on a specific transfer.

4. However, even when the conditions referred in the previous paragraphs are not fulfilled, a National Member may, under the exceptional circumstances enumerated in Article 27(6) of the Eurojust Decision, transfer data to a third country with the sole aim of taking urgent measures to counter imminent serious danger threatening a person or public security. The National Member shall document such an exceptional transfer in the temporary work file related to the case, stating the grounds for such a communication, and shall inform the Data Protection Officer of such a communication. The Data Protection Officer shall verify if such transfers only take place in exceptional and urgent cases.

CHAPTER V

Time limits for the storage of personal data

Article 29

Time limits for the storage of personal data

1. Eurojust shall put in place appropriate technical measures to ensure that the time limits for the storage of personal data defined in Article 21 of the Eurojust Decision are observed.

2. The case management system shall in particular ensure that a review of the need to store data in a temporary work file is carried out every three years after they were entered. Such a review must be properly documented in the system, including the motivation for any decision taken, and the result of it shall be automatically communicated to the Data Protection Officer.

3. The case management system shall particularly mark the data recorded for a limited period of time in accordance with Article 15(3) of the Eurojust Decision. For these categories of data a review of the need to retain the data shall take place every three months and shall be documented in the same way as outlined in paragraphs 1 and 2.

4. The controller shall, where necessary, consult the College and the Data Protection Officer regarding any decision to retain the data for a longer period following a review.

TITLE V

RULES FOR NON-CASE-RELATED PROCESSING OPERATIONS

CHAPTER I

General principles

Article 30

Lawfulness and fairness of processing

Personal data must be processed fairly and lawfully. In particular, personal data may be processed only if:

(a) processing is necessary for compliance with a legal obligation to which the controller is subject, or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or

(c) the data subject has unambiguously given his or her consent, or

(d) processing is necessary in order to protect the vital interests of the data subject, or

(e) processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 4 of the present rules.

Article 31

Purpose limitation

1. Personal data must be processed for a specific and well-defined lawful and legitimate purpose and subsequently further processed only insofar as this is not incompatible with the original purpose of the processing.

2. Personal data collected exclusively for ensuring the security or the control and management of the processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences.

Article 32

Processing of special categories of data

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life or criminal convictions for non-case-related purposes is prohibited.

2. This prohibition shall not apply if:

(a) the data subject has given his or her express consent to the processing of those data or

(b) the processing is necessary for the purposes of complying with the specific rights and legal obligations of the controller, such as obligations in the field of tax or employment law applicable to the controller or, if necessary, insofar as it is agreed upon by the Data Protection Officer, subject to adequate safeguards, or

(c) the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent, or

(d) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Data referred to in paragraph 1 shall only be processed for the purpose for which they were originally collected.

Article 33

Exceptions to the right of information of the data subject

1. In the context of the non-operational work of Eurojust, exceptions to the general principle of information to the data subject are possible when the provision of this information to the data subject would undermine:

(a) an important economic or financial interest of a Member State or of the European Union or

(b) the protection of the data subject or of the rights and freedoms of others or

(c) the national security, public security or defence of the Member States.

2. The Data Protection Officer shall be informed when recourse to these exceptions is made.

Article 34

Notification to the Data Protection Officer

1. Every controller shall give prior notice to the Data Protection Officer of any processing operation or sets of such operations intended to serve a single purpose or several related purposes.

2. The information to be given shall include:

(a) the name of the controller and an indication of the organisational parts of an institution or body entrusted with the processing of personal data for a particular purpose;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subjects and of the data or categories of data relating to them;

(d) the legal basis of the processing operation for which the data are intended;

(e) the recipients or categories of recipient to whom the data might be disclosed; and

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the security measures.

3. Any relevant change affecting information referred to in the previous paragraph shall be notified promptly to the Data Protection Officer.

Article 35

Register

1. A register of processing operations notified in accordance with the previous provision shall be kept by the Data Protection Officer.

2. The register shall contain at a minimum the information referred to in Article 34(2)(a) to (f).

3. The Data Protection Officer shall make available to the Joint Supervisory Body any information contained in the register when so requested.

Article 36

Processing of personal data on behalf of controllers

1. Where a processing operation is carried out on its behalf by an external processor, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 of the Eurojust Decision and any further relevant documents and ensure compliance with those measures.

2. The carrying out of a processing operation by way of an external processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

(a) the processor shall act only on instructions from the controller; and

(b) the obligations regarding confidentiality and security established by the Eurojust Decision and the present rules of procedure shall also be incumbent on the processor unless, by virtue of Article 16 or Article 17(3), second indent, of Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data [1], the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States.

3. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to confidentiality and security measures shall be in writing or in another equivalent form.

Article 37

Automated individual decisions

The data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorised pursuant to national or European legislation or, if necessary, by the Data Protection Officer. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view or to allow him or her to understand the logic of the processing, shall be taken.

CHAPTER II

Internal rules concerning the protection of personal data and privacy in the context of internal telecommunication networks

Article 38

Scope

1. Without prejudice to the previous Articles, the rules contained in the present chapter shall apply to the processing of personal data in connection with the use and management of telecommunications networks or terminal equipment operated under the control of Eurojust.

2. For the purposes of rules contained in the present chapter, *'user'* means any natural person using a telecommunications network or terminal equipment operated under the control of Eurojust.

[1] OJ L 281, 23.11.1995, p. 31.

Article 39

Security

1. Eurojust shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment (computers, servers, hardware and software), if necessary in conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In the event of any particular risk of a breach of the security of the network and terminal equipment, Eurojust shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.

Article 40

Confidentiality of communications

Eurojust shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with Community law.

Article 41

Traffic and billing data

1. Traffic data relating to users which are processed to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection.

2. Exceptions to this general principle (such as the need to keep some traffic data if linked to the log process necessary for certain files or for the purpose of billing private calls) are allowed only if foreseen in internal rules adopted by Eurojust after consultation with the Data Protection Officer. Should the Data Protection Officer not be satisfied with the lawfulness or appropriateness of such exceptions, the Joint Supervisory Body shall be consulted.

3. Processing of traffic and billing data shall only be carried out by persons handling billing, traffic or budget management.

Article 42

Directories of users

1. Personal data contained in printed or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.

2. Such directories shall be only available to Eurojust users, for purely internal use or in other inter-institutional directories that are considered appropriate.

CHAPTER III

Specific rules

Article 43

Additional rules

Where necessary, Eurojust shall develop further rules regarding the processing of personal data in non-case-related operations. Such rules shall be notified to the Joint Supervisory Body and published in separate internal manuals.

TITLE VI

OTHER PROVISIONS

Article 44

Review of the present Rules of Procedure

1. These rules shall be reviewed regularly to assess if any amendments are necessary. Any amendment to the present rules shall follow the same procedures established for its approval in the Eurojust Decision.

2. The Data Protection Officer shall inform both the President of the College and the Joint Supervisory Body if he or she is of the opinion that amendments of the present Rules of Procedure are necessary.

3. The Joint Supervisory Body shall bring to the attention of the College any suggestions or recommendations regarding amendments of the present Rules of Procedure.

Article 45

Entry into force and publication

1. The present Rules of Procedure shall enter into force the day following their definitive approval by the Council.

2. They shall be published in the *Official Journal of the European Union*.