



Brussels, 16 January 2015
(OR. en)

5327/15

Interinstitutional File:
2013/0256 (COD)

EUROJUST 4
EPPO 3
CATS 4
COPEN 6
CODEC 54

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	17045/14 EUROJUST 223 EPPO 79 CATS 210 COPEN 322 CODEC 2543
No. Cion doc.:	12566/13 EUROJUST 59 EPPO 4 CATS 36 COPEN 109 CODEC 2163
Subject:	Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - Revised text on Chapter IV and Annex II

Delegates will find a revised text on Chapter IV and Annex II of the draft Regulation in the Annex.

This text takes account of the discussions at the COPEN Working Party meeting of 13 January together with the written comments received from Member States (Doc. 5360/15 EUROJUST 6 EPPO 5 CATS 6 COPEN 8 CODEC 60).

Chapter IV

¹Processing of Information

Article x

Definitions

For the purposes of this Regulation:

- a) ²‘personal data’ means any information relating to an identified or identifiable natural person hereinafter referred to as “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/her physical, physiological, ~~mental~~, economic, cultural or social identity;
- b) ‘operational personal data’ means all personal data processed by Eurojust to fulfill the tasks laid down in Article 2;
- c) ‘administrative personal data’ means all personal data processed by Eurojust apart from those that are processed to fulfill the tasks laid down in Article 2;

¹ CION has a reservation on Chapter IV and maintains that Regulation 45/2001 should apply to all data processed at Eurojust. FI, AT and PT have scrutiny reservations on the Chapter.

² Definitions will be reviewed in the future, possibly taking into account the ongoing negotiations on the "data protection package".

d) 'processing of personal data' hereinafter referred to as '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;

~~e) '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;~~

fe) 'transfer of personal data' means the communication of personal data, actively made available, between a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data;

~~g) 'the data subject's consent' means any freely given specific and informed indication of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed;~~

g) National Supervisory Authority/Authorities means the national competent authorities of designated by the Member States who to monitor independently, in accordance with its national law exchange the processing of personal data in that specific Member State.

Article 26a

General data protection principles

Personal data shall be:

- (a) processed fairly and lawfully;**
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing of personal data for historical, statistical or scientific purposes shall not be considered incompatible provided that Eurojust provides appropriate safeguards, in particular to ensure that data are not processed for any other purposes;**
- (c) adequate, relevant, and not excessive in relation to the purposes for which they are processed;**
- (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;**
- (e) kept in a form which permits identification of data subjects and for no longer than necessary for the purposes for which the personal data are processed,;**
- (f) processed in a manner that ensures appropriate security of personal data and confidentiality of data processing.**

Article 31a-26b

Administrative personal data

- 1. Regulation (EC) No 45/2001 shall apply to all administrative personal data held by Eurojust.**

~~2. The Data Protection Officer at Eurojust shall carry out the functions foreseen by Article 24 of Regulation (EC) No 45/2001 with regard to administrative personal data.~~

~~3. If the Data Protection Officer considers that the provisions of Regulation (EC) No 45/2001 related to the processing of administrative personal data have not been complied with, he or she shall inform the Administrative Director, requiring him or her to resolve the non-compliance with a specified time. If the Administrative Director does not resolve the non-compliance within a specified time, the Data Protection Officer shall inform refer the matter to the College and shall agree with the College a specified time for a response. If the College does not resolve the non-compliance of the processing within the specified time, the Data Protection Officer shall refer the matter to the European Data Protection Supervisor.~~

Article 27

Processing of operational personal data

1. Insofar as it is necessary to **perform its tasks**, ~~achieve its explicitly stated task~~, Eurojust may, within the framework of its competence and in order to carry out its operational functions, process by automated means or in structured manual files in accordance with this Regulation only the personal data listed in point 1 of Annex 2, on persons who, under the national legislation of the Member States concerned are suspected **or accused** of having committed or having taken part in a criminal offence in respect of which Eurojust is competent or who have been convicted of such an offence.
2. Eurojust may process only the personal data listed in point 2 of Annex 2, on persons who, under the national legislation of the Member States concerned, are regarded as witnesses or victims in a criminal investigation or prosecution regarding one or more of the types of crime and the offences referred to in Article 3, ~~or persons under the age of 18~~. The processing of such personal data may only take place if it is strictly necessary for the **fulfilment** of the ~~expressly stated~~ tasks of Eurojust, within the framework of its competence and in order to carry out its operational functions.

3. In exceptional cases, Eurojust may also, for a limited period of time which shall not exceed the time needed for the conclusion of the case related to which the data are processed, process personal data other than those referred to in paragraphs 1 and 2 relating to the circumstances of an offence where they are immediately relevant to and included in ongoing investigations which Eurojust is coordinating or helping to coordinate and when their processing is strictly necessary for the purposes specified in paragraph 1. The Data Protection Officer referred to in Article 31 shall be informed immediately of recourse to this paragraph and of the specific circumstances which justify the necessity of the processing of such personal data. Where such other data refer to witnesses or victims within the meaning of paragraph 2, the decision to process them shall be taken jointly by at least two the relevant national members.
4. **Operational p**Personal data, processed by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic data³ concerning medical health or sex life may be processed by Eurojust only when such data are strictly necessary for the national investigations concerned as well as for coordination within Eurojust and if they supplement other **operational** personal data **relating to the same person** already processed. The Data Protection Officer shall be informed immediately of recourse to this paragraph. Such data may not be processed in the Index referred to in Article 24(4). Where such other data refer to witnesses or victims within the meaning of paragraph 3, the decision to process them shall be taken by the College.
- ~~5. Regulation (EC) No 45/2001 shall apply to the processing of personal data by Eurojust in the context of its activities. This Regulation particularises and complements Regulation (EC) No 45/2001 in as far as personal data processed by Eurojust for its operational tasks are concerned.~~
- 4a No decision which produces adverse legal effects concerning a data subject shall be based solely on automated processing of data referred to in paragraph 4., unless the decision is expressly authorised pursuant to national or Union legislation.**

³ SI scrutiny reservation

Article 28

Time limits for the storage of operational personal data

1. **Operational personal** data processed by Eurojust shall be stored by Eurojust for only as long as is necessary for the performance of its tasks. In particular, without prejudice to paragraph 3, the personal data referred to in Article 27 may not be stored beyond the first applicable among the following dates:
 - a) the date on which prosecution is barred under the statute of limitations of all the Member States concerned by the investigation and prosecutions;
 - b) the date on which **Eurojust is informed that** the person has been acquitted and the judicial decision became final. **When the judicial decision becomes final the Member State concerned shall inform Eurojust without delay;**
 - c) three years after the date on which the judicial decision of the last of the Member States concerned by the investigation or prosecution became final;
 - d) the date on which Eurojust and the Member States concerned mutually established or agreed that it was no longer necessary for Eurojust to coordinate the investigation and prosecutions, unless there is an obligation to provide Eurojust with this information in accordance with Article 21(5) or (6);
 - e) three years after the date on which data were transmitted in accordance with Article 21(46), or (57).

2. Observance of the storage deadlines referred to in ~~points (a), (b), (c) and (d)~~ of paragraph 1 shall be reviewed constantly by appropriate automated processing **particularly from the moment in which the case is closed by Eurojust**. Nevertheless, a review of the need to store the data shall be carried out every three years after they were entered; **such a review shall then apply to the case as a whole**. If data concerning persons referred to in Article 27(4) are stored for a period exceeding five years, ~~the~~ **the** European Data Protection Supervisor ~~shall~~ **shall** be informed accordingly.

3. When one of the storage deadlines referred to in ~~points (a), (b), (c) and (d)~~ of paragraph **1(a)** has expired, Eurojust shall review the need to store the data longer in order to enable it to perform its tasks and it may decide by way of derogation to store those data until the following review. The reasons for the continued storage must be justified and recorded. If no decision is taken on the continued storage of personal data at the time of the review, those data shall be deleted **immediately**. ~~automatically after three years. However, once prosecution is statute barred in all Member States concerned as referred to in point (a) of paragraph 1, data may only be stored if they are necessary in order for Eurojust to provide assistance in accordance with this Regulation.~~
4. Where, in accordance with paragraph 3, data have been stored beyond the dates referred to in paragraph **1(a)**, a review of the need to store those data shall take place every three years by ~~the European Data Protection Supervisor~~ **HJSB**.
5. ~~Where a file contains non-automated and unstructured data, once the deadline for storage of the last item of automated data from the file has elapsed, all documents in the file shall be returned to the authority which supplied them and any copies shall be destroyed~~ **with the exception of any original documents which Eurojust has received from national authorities and which need to be returned to their originator.**
6. Where Eurojust has coordinated an investigation or prosecutions, the national members concerned shall inform **the other national members concerned whenever they receive information that the case has been dismissed or any final all judicial decisions related to the case have become final.** ~~Eurojust and the other Member States concerned of all judicial decisions relating to the case which have become final in order, inter alia, that point (b) of paragraph 1(a) may be applied.~~

*Article 28a*⁴

Data Security of operational personal data

1. Eurojust and, insofar as it is concerned by data transmitted from Eurojust, each Member State, shall, as regards the processing of operational personal data within the framework of this Regulation protect personal data against accidental or unlawful destruction, accidental loss or unauthorised disclosure, alteration and access or any other unauthorised form of processing.
2. Eurojust and each Member State shall implement appropriate technical and organisational measures with regard to data security and in particular 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 only have access 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 are transmitted when data are communicated (communication control);
 - (g) ensure that it is subsequently 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);

⁴ Scrutiny reservation Slovakia

- (h) **prevent unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during 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 occurrence of faults in the functions is immediately reported (reliability) and that stored data cannot be corrupted by system malfunctions (integrity).**
3. **Eurojust and Member States shall define mechanisms to ensure that security needs are taken on board across information system boundaries.**
 4. **In case of a security breach, involving personal data, Eurojust shall notify, without undue delay and, where feasible, not later than 24 hours after having become aware of it, the breach to the Data Protection Officer, to the European Data Protection Supervisor ~~to the JSB~~ as well as to Member States affected.**

Article 29

Logging and documentation of operational personal data

1. For the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security, Eurojust shall keep records of any collection, alteration, access, disclosure, combination or erasure of **operational** personal data ~~used for operational purposes~~. **It shall also keep records of transmission to third parties.** Such logs or documentation shall be deleted after 18 months, unless **they** are further required for on-going control.

2. Logs or documentation prepared under paragraph 1 shall be communicated on request to ~~the European Data Protection Supervisor~~~~[JSB]~~ ~~the European Data Protection Supervisor~~~~[JSB]~~ shall use this information only for the purpose of data protection control, ensuring proper data processing, and data integrity and security.

Article 30

Authorised access to operational personal data

Only national members, their deputies and their Assistants, persons referred to in Article 20(2) in so far as they are connected to the Case Management System and authorised Eurojust staff may, for the purpose of achieving Eurojust's tasks and within the limits provided for in Articles 24, 25 and 26, have access to **operational** personal data processed by Eurojust ~~for its operational tasks~~.

Article 31

Appointment of the Data Protection Officer

1. The Executive Board shall appoint a Data Protection Officer ~~in accordance with Article 24 of Regulation (EC) No 45/2001~~, **who shall be a member of staff specifically appointed for this purpose. In the performance of his or her duties, he or she shall act independently and may not receive any instructions.**
- 1a. **The Data Protection Officer shall be selected on the basis of his/her personal and professional qualities and, in particular, the expert knowledge of data protection.**
- ~~1b. The selection of the Data Protection Officer shall not be liable to result in a conflict of interests between his/her duty as Data Protection Officer and any other official duties, in particular in relation to the application of the provisions of this Regulation.~~
- 1be. **The Data Protection Officer shall be appointed for a term of four years. He/she shall be eligible for reappointment up to a maximum total term of eight years. He/she may be dismissed from the post of Data Protection Officer by the Executive Board only with the consent of the European Data Protection Supervisor, if he/she no longer fulfils the conditions required for the performance of his/her duties.**

2. ~~When complying with the obligations set out in Article 24 of Regulation (EC) No 45/2001, the Data Protection Officer shall:~~ **The Data Protection Officer shall in particular have the following tasks, regarding the processing of personal data, to:**
- aa) ensure Eurojust's compliance with the data protection provisions of this Regulation, Regulation 45/2001 and the relevant data protection provisions in the rules of procedure of Eurojust;**
 - a) ensure that a record of the **transfer and receipt of personal data is kept in accordance with the provisions to be laid down in the rules of procedure of Eurojust;**
 - b) cooperate with Eurojust staff responsible for procedures, training and advice on data processing **and with the European Data Protection Supervisor;**
 - bb) ensure that data subjects are informed of their rights under this Regulation at their request;**
 - c) prepare an annual report and communicate that report to the College and to ~~the~~ European Data Protection Supervisor~~;~~
3. In the performance of his or her tasks, the Data Protection Officer shall have access to all the data processed by Eurojust and to all Eurojust premises.
4. Eurojust's staff members assisting the Data Protection Officer in the performance of his or her duties shall have access to the personal data processed at Eurojust and to Eurojust premises to the extent necessary for the performance of their tasks.

5. If the Data Protection Officer considers that the provisions of Regulation (EC) No 45/2001 related to the processing of administrative personal data or the provisions of this Regulation related to the processing of **operational** personal data have not been complied with, he or she shall inform the Administrative Director requiring him or her to resolve the non-compliance within a specified time. If the Administrative Director does not resolve the non-compliance of the processing within the specified time, the Data Protection Officer shall **refer the matter to the College** ~~inform the College and shall agree with the College~~ a specified time for a response. **If the College does not resolve the non-compliance of the processing within the specified time, the Data Protection Officer shall refer the matter to the European Data Protection Supervisor/JSB.**
6. ~~The Executive Board shall adopt the implementing rules referred to in Article 24(8) of Regulation (EC) No 45/2001.~~

Article 32⁵

Modalities regarding the exercise of the right of access to operational personal data

1. Any data subject wishing to exercise the right of access to **operational** personal data relating to him or her which are held by Eurojust may make a request to that effect free of charge ~~directly to Eurojust or~~ to the authority appointed for this purpose in the Member State of their choice. That authority shall refer the request to Eurojust without delay and in any case within one month of receipt.
2. The request shall be answered by Eurojust without undue delay and in any case within three months of its receipt by Eurojust.

⁵ Slovenian scrutiny reservation on Paras 3 and 6(a) and the deletion of Para 7.

2a Access to operational personal data based on any requests made under paragraph 1 ~~shall~~ may be refused or restricted, if ~~it~~ such a refusal or restriction constitutes a necessary measure to:

(a) enable Eurojust to fulfil its tasks properly;

(b) guarantee that any national investigation or prosecution will not be jeopardised ~~or prosecution prejudiced~~;

(c) protect the rights and freedoms of others.

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

3. The competent authorities of the Member States concerned shall be consulted by Eurojust on a decision to be taken. A decision on access to data shall be conditional upon close cooperation between Eurojust and the Member States directly concerned by the communication of such data. In any case in which a Member State objects to Eurojust's proposed response, it shall notify Eurojust of the reasons for its objection. **Eurojust shall comply with any such objection. The competent authorities shall subsequently be notified of the content of Eurojust's decision through the national members concerned.**

~~4. When the right of access is restricted in accordance with Article 20(1) of Regulation (EC) No 45/2001, Eurojust shall inform the data subject in accordance with Article 20(3) of that Regulation in writing. The information about the principal reasons may be omitted where the provision of such information would deprive the restriction of its effect. The data subject shall at least be informed that all necessary verifications by the European Data Protection Supervisor have taken place.~~

~~5. Eurojust shall document the grounds for omitting the communication of the principal reasons on which the restriction referred to in paragraph 4 is based.~~

6. The national members concerned by the request shall deal with it and reach a decision on Eurojust's behalf. ~~The request shall be dealt with in full within three months of receipt.~~ Where the members are not in agreement, they shall refer the matter to the College, which shall take its decision on the request by a two-thirds majority.
- 6a **Eurojust shall inform the data subject in writing on any refusal or restriction of access, on the reasons for such a decision and of his right to lodge a complaint to the ~~European Data Protection Supervisor~~ [JSB]. If access is denied or if no personal data concerning the applicant are processed by Eurojust, the latter shall notify the applicant that it has carried out the checks, without giving any information which could reveal whether or not the applicant is known. ~~Where the provision of such information would deprive the restriction imposed by paragraph 2(ba) of its effect, Eurojust shall only notify the data subject concerned that it has carried out the checks without giving any information which might reveal to him/her whether or not personal data concerning him/her are processed by Eurojust.~~**
7. ~~When in application of Article 46 and 47 of Regulation (EC) No 45/2001, the European Data Protection Supervisor checks the lawfulness of the processing performed by Eurojust, he or she shall inform the data subject at least that all necessary verifications by the European Data Protection Supervisor have taken place.~~

Article 33⁶

Right to ~~r~~Rectification, erasure and blocking of operational personal data

- 1a Any data subject shall have the right to ask Eurojust to rectify operational personal data relating to him or her, if they are incorrect or incomplete or if their input or storage contravenes this Regulation and, where this is possible and necessary, to complete or update them.
- 1b Any data subject shall have the right to ask Eurojust to erase operational personal data relating to him/her held by Eurojust if they are no longer required for the purposes for which they are lawfully collected or are lawfully further processed.

⁶ Slovenian scrutiny reservation on Para 1 and 2.

1c Operational personal data shall be blocked rather than erased if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose that prevented their erasure.

1. If the personal data that have to be rectified, erased or whose processing has to be restricted ~~in accordance with Articles 14, 15 or 16 of Regulation (EC) No 45/2001~~ have been provided to Eurojust by Member States, third countries, international organisations **or Union bodies** ~~private parties, private persons or are the results of Eurojust's own analyses~~, Eurojust shall rectify, erase or ~~restrict~~ **block** the processing of such data.

2. If the personal data that have to be rectified, erased or whose processing has to be restricted ~~in accordance with Article 14, 15 and 16 of Regulation (EC) No 45/2001~~ have been provided directly to Eurojust by Member States, Eurojust shall rectify, erase or ~~restrict~~ **block** the processing of such data in collaboration with Member States.

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 transfer or were transmitted in breach of this Regulation or if they result from their being input, taken over or stored in an incorrect manner or in breach of this Regulation by Eurojust, Eurojust shall rectify or erase the data in collaboration with the Member States concerned.

~~4. In the cases referred to in Articles 14, 15 or 16 of Regulation (EC) No 45/2001, all addressees of such data shall be notified forthwith in accordance with Article 17 of Regulation (EC) No 45/2001. In accordance with rules applicable to them, the addressees shall then rectify, erase or restrict the processing of those data in their systems.]~~

[...]

5. Eurojust shall inform the data subject in writing without undue delay and in any case within three months of the receipt of the request that data concerning him or her have been rectified, erased or their processing ~~restricted~~ **blocked**.
6. Eurojust shall inform the data subject in writing on any refusal of rectification, of erasure or of restrictions to the processing, and the possibility of lodging a complaint with the European Data Protection Supervisor ~~EDPS~~ **JSD** and seeking a judicial remedy.
- 6a At the request of a Member State's competent authorities, national member or national correspondent, if any, and under their responsibility, Eurojust shall rectify or erase personal data being processed by Eurojust which were transmitted or entered by that Member State, its national member or its national correspondent.**
- 6b In the cases referred to in paragraphs 1 and 2 all the suppliers and addressees of such data shall be notified immediately. In accordance with the rules applicable to them, the addressees, shall then rectify, erase or ~~restrict~~ block the processing of those data in their own systems.**

Article 34

Responsibility in data protection matters

1. Eurojust shall process **operational** personal data in such a way that it can be established which authority provided the data or where the ~~personal~~ data has been retrieved from.
2. The responsibility for the quality of **operational** personal data shall lie with the Member State which provided the ~~personal~~ data to Eurojust and with Eurojust for **operational** personal data provided by EU bodies, third countries or international organisations, as well for **operational** personal data retrieved by Eurojust from publicly available sources.
3. The responsibility for compliance with Regulation (EC) No 45/2001 and this Regulation shall lie with Eurojust. The responsibility for the legality of transfer of **operational** personal data provided by the Member States to Eurojust shall lie with the Member State which provides the ~~personal~~ data, and with Eurojust for the **operational** personal data provided to Member States, EU bodies and third countries or organisations by Eurojust.

4. Subject to other provisions in this Regulation, Eurojust shall be responsible for all data processed by it.

Article 34a

Supervision by the national supervisory authority

1. **The national supervisory authorities shall have the task of monitoring independently, in accordance with national law, the permissibility of the transfer, the retrieval and any communication to Eurojust of operational personal data by the Member State concerned and to examine whether such transfer, retrieval or communication violates the rights of the data subject.**
2. **National supervisory authorities shall keep the European Data Protection Supervisor informed of any actions they take with respect to Eurojust.**
3. **Any person shall have the right to request the national supervisory authority to verify that the transfer or communication to Eurojust of operational personal data concerning him/her in any form and the access to the operational personal 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 34b

Supervision by the European Data Protection Supervisor

1. **The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation relating to the protection of fundamental rights and freedoms of natural persons with regard to processing of operational personal data by Eurojust, and for advising Eurojust and data subjects on all matters concerning the processing of operational personal data. To this end, he/she shall fulfil the duties set out in paragraph 2, shall exercise the powers granted in paragraph 3 and shall cooperate with the national supervisory authorities in accordance with Article 35.**

2. The European Data Protection Supervisor shall have the following duties under this Regulation:

- (a) hear and investigate complaints, and inform the data subject of the outcome within a reasonable period;**
- (b) conduct inquiries either on his/her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;**
- (c) monitor and ensure the application of the provisions of this Regulation and any other Union act relating to the protection of natural persons with regard to the processing of personal data by Eurojust;**
- (d) advise Eurojust, either on his/her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before it draws up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of operational personal data;**

3. The European Data Protection Supervisor may under this Regulation:

- (a) give advice to data subjects in the exercise of their rights;**
- (b) refer the matter to Eurojust in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;**
- (c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 39 and 40;**
- (d) warn or admonish Eurojust;**

- (e) order Eurojust to carry out the rectification, blocking, erasure or destruction of data which have been processed in breach of the provisions governing the processing of operational personal data and the notification of such actions to third parties to whom such data have been disclosed;
- (f) impose a temporary or definitive ban on specific processing operations by Eurojust in breach of the provisions governing the processing of personal data;
- (g) refer the matter to Eurojust and, if necessary, to the European Parliament, the Council and the Commission;
- (h) refer the matter to the Court of Justice of the European Union under the conditions provided for in the Treaty;
- (i) intervene in actions brought before the Court of Justice of the European Union.

4. The European Data Protection Supervisor shall have the power:

- (a) to obtain from Eurojust access to all operational personal data and to all information necessary for his/her enquiries;
- (b) to obtain access to any premises in which Eurojust carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there.

5. The European Data Protection Supervisor shall draw up an annual report on the supervisory activities on Eurojust. The national supervisory authorities shall be invited to make observations on this report, before it becomes part of the annual report of the European Data Protection Supervisor referred to in Article 48 of Regulation (EC) No 45/2001. The European Data Protection Supervisor will shall take utmost account of the observations made by national supervisory authorities and, in any case, shall refer to them in the annual report.

Article 35

Cooperation between the European Data Protection Supervisor and national data protection authorities

1. The European Data Protection Supervisor shall act in close cooperation with national **supervisory** authorities competent for data protection supervision with respect to specific issues requiring national involvement, in particular if the European Data Protection Supervisor or a national **supervisory** authority competent for data protection supervision finds major discrepancies between practices of the Member States or potentially unlawful transfers using Eurojust's communication channels, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.

2. **The European Data Protection Supervisor shall use the expertise and experience of national supervisory authorities in carrying out his/her duties set out in Article 34a(2). In carrying out joint inspections together with the European Data Protection Supervisor, members and staff of national supervisory authorities shall, taken due account of the principle of subsidiarity and proportionality, have equivalent powers as those laid down in Article 34a (4) and be bound by an equivalent obligation as that laid down in Article 34a(6).** ~~In cases referred to under paragraph 1~~ ~~the European Data Protection Supervisor and the national authorities competent for data protection supervision may, each acting within the scope of their respective competences, exchange relevant information, **and** assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems related to the exercise of independent supervision or to the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.~~

- 2a. The European Data Protection Supervisor shall keep national supervisory authorities fully informed of all issues directly affecting or otherwise relevant to them. Upon request of one or more national supervisory authorities, the European Data Protection Supervisor shall inform them on specific issues.**

2b. In cases relating to data originating from one or several Member States, including in cases referred to in Article 36(2), the European Data Protection Supervisor shall consult the national supervisory authorities concerned. The European Data Protection Supervisor shall not decide on further action to be taken before those national supervisory authorities have informed the European Data Protection Supervisor of their position, within a deadline specified by him/her which shall not be shorter than one month and not longer than three months. The European Data Protection Supervisor shall take utmost account of the position of the national supervisory authorities concerned. In cases where the European Data Protection Supervisor intends not to follow their position, he/she shall inform them, and provide a justification and submit the matter to the Cooperation Board referred to in paragraph 3.

In cases which the European Data Protection Supervisor deems to be extremely urgent, he/she may decide to take immediate action. In such cases, the European Data Protection Supervisor shall immediately inform the national supervisory authorities concerned and justify the urgent nature of the situation as well as the action he/she has taken.

3. The National Supervisory Authorities and the European Data Protection Supervisor shall meet for the purposes outlined in this Article, as needed **and at least twice a year in a Cooperation Board which is hereby established.** The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure **of the Cooperation Board** shall be adopted at the first meeting **by simple majority.** Further working methods shall be developed jointly as necessary.

4. The Cooperation Board shall be composed of a representative of a national supervisory authority of each Member State and of the European Data Protection Supervisor.

5. The Cooperation Board shall act independently when performing its tasks pursuant to paragraph 6 and shall neither seek nor take instructions from anybody.

6. The Cooperation Board shall have the following tasks:

- (a) discuss general policy and strategy on data protection supervision of Europol and the permissibility of the transfer, the retrieval and any communication to Europol of personal data by the Member States;**
- (b) examine difficulties of interpretation or application of this Regulation;**
- (c) study general problems relating to the exercise of independent supervision or the exercise of the rights of data subjects;**
- (d) discuss and draw up harmonised proposals for joint solutions on matters referred to in paragraph 1;**
- (e) discuss cases submitted by the European Data Protection Supervisor in accordance with paragraph 2b;**
- (f) discuss cases submitted by any national supervisory authority; and**
- (g) promote awareness of data protection rights.**

7. The European Data Protection Supervisor and the national supervisory authorities shall, each acting within the scope of their respective competences, take utmost account of the opinions, guidelines, recommendations and best practices agreed by the Cooperation Board.

Article 36

Right to lodge a complaint with the European Data Protection Supervisor

1.bis Any data subject shall have the right to lodge a complaint with the European Data Protection Supervisor, if he/she considers that the processing by Eurojust of personal data relating to him/her does not comply with the provisions of this Regulation.

1. Where a complaint introduced by a data subject relates to a decision as referred to in Article 32 or 33, the European Data Protection Supervisor shall consult the national supervisory **authorities** ~~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 European Data Protection Supervisor which may extend to a refusal to communicate any information, shall take account of the opinion of the national supervisory **authority** ~~body~~ or competent judicial body.
2. Where a complaint relates to the processing of data provided by a Member State to Eurojust, the European Data Protection Supervisor shall ensure that the necessary checks have been carried out correctly in close cooperation with the national supervisory **authority** ~~body~~ of the Member State which has provided the data.
3. Where a complaint relates to the processing of data provided to Eurojust by Union bodies, third countries or organisations or private parties, the European Data Protection Supervisor shall ensure that the necessary checks have been carried out by Eurojust.

Article 37

Liability for unauthorised or incorrect processing of data

1. Eurojust shall be liable, in accordance with Article 340 of the Treaty, for any damage caused to an individual which results from unauthorised or incorrect processing of data carried out by it.

2. Complaints against Eurojust pursuant to the liability referred to in paragraph 1 shall be heard by the Court of Justice in accordance with Article 268 of the Treaty.
3. Each Member State shall be liable, in accordance with its national law, for any damage caused to an individual, which results from unauthorised or incorrect processing carried out by it of data which were communicated to Eurojust.

*Categories of **operational** personal data referred to in Article 27*

1. a) surname, maiden name, given names and any alias or assumed names;
- b) date and place of birth;
- c) nationality;
- d) sex;
- e) place of residence, profession and whereabouts of the person concerned;
- f) social security numbers **or other official adequate numbers used in the Member States to identify individuals**, driving licences, identification documents and passport data, customs and Tax Identification Numbers;
- g) information concerning legal persons if it includes information relating to identified or identifiable individuals who are the subject of a judicial investigation or prosecution;
- h) ~~bank accounts~~ details ~~and of~~ accounts held with banks or other financial institutions;
- i) description and nature of the alleged offences, the date on which they were committed, the criminal category of the offences and the progress of the investigations;
- j) the facts pointing to an international extension of the case;
- k) details relating to alleged membership of a criminal organisation;
- l) telephone numbers, e-mail addresses, traffic data and location data, as well as the related data necessary to identify the subscriber or user;
- m) vehicle registration data;
- n) DNA profiles established from the non-coding part of DNA, photographs and fingerprints.

- 2.
- a) surname, maiden name, given names and any alias or assumed names;
 - b) date and place of birth;
 - c) nationality;
 - d) sex;
 - e) place of residence, profession and whereabouts of the person concerned;
 - f) the description and nature of the offences involving them, the date on which they were committed, the criminal category of the offences and the progress of the investigations.
 - g) **social security numbers or other official adequate numbers used by the Member States to identify individuals, driving licences, identification documents and passport data, customs and Tax Identification Numbers;**
 - h) **bank accounts and details of accounts held with banks and other financial institutions;**
 - i) **telephone numbers, e-mail addresses, traffic data and location data, as well as the related data necessary to identify the subscriber or user;**
 - j) **vehicle registration data.**
-