007431/EU XXVIII. GP
Eingelangt am 19/12/24

Council of the European Union

Brussels, 19 December 2024
(OR. en)

17074/24
ADD 1

Interinstitutional File:
2024/0321(NLE)

ENFOPOL 534
CRIMORG 167
CT 133
IXIM 268
COLAC 190
CORDROGUE 128
JAI 1894

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	18 December 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2024) 580 final - ANNEX
Subject:	ANNEX to the Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the Agreement between the European Union and the Federative Republic of Brazil on cooperation with and through the European Union Agency for Law Enforcement Cooperation (Europol) and the Federal Police of Brazil

Delegations will find attached document COM(2024) 580 final - ANNEX.

Encl.: COM(2024) 580 final - ANNEX

www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 18.12.2024
COM(2024) 580 final

ANNEX

ANNEX

to the

Proposal for a Council Decision

on the conclusion, on behalf of the European Union, of the Agreement between the European Union and the Federative Republic of Brazil on cooperation with and through the European Union Agency for Law Enforcement Cooperation (Europol) and the Federal Police of Brazil

www.parlament.gv.at

ANNEX

DRAFT AGREEMENT BETWEEN THE EUROPEAN UNION AND THE FEDERATIVE REPUBLIC OF BRAZIL ON COOPERATION WITH AND THROUGH THE EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL) AND THE FEDERAL POLICE OF BRAZIL

THE EUROPEAN UNION, hereinafter also referred to as the "Union" or “EU",

and

THE FEDERATIVE REPUBLIC OF BRAZIL, hereinafter also referred to as “Brazil”,

hereinafter jointly referred to as "the Contracting Parties",

CONSIDERING that by allowing the exchange of personal and non-personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the competent authorities of Brazil, this Agreement will create the framework for an enhanced operational cooperation between the Union and Brazil in the field of law enforcement, while safeguarding the human rights and fundamental freedoms of all individuals concerned, including the right to privacy and data protection,

CONSIDERING that this Agreement is without prejudice to mutual legal assistance arrangements between Brazil and the Member States of the Union allowing for the exchange of personal data,

CONSIDERING that this Agreement does not impose any requirement on the competent authorities to transfer personal or non-personal data and that the sharing of any personal or non-personal data requested under this Agreement remains voluntary,

HAVE AGREED AS FOLLOWS:

CHAPTER I

GENERAL PROVISIONS

ARTICLE 1

Objective and scope

(1) The objective of this Agreement is to establish cooperative relations between the European Union Agency for Law Enforcement Cooperation (Europol) and the competent authorities of Brazil and to allow the transfer of personal and non-

www.parlament.gv.at

personal data between them, in order to support and strengthen the action by the authorities of the Member States of the Union and those of Brazil, as well as their mutual cooperation in preventing and combating criminal offences, including serious crime and terrorism, while ensuring appropriate safeguards with respect to the human rights and fundamental freedoms of individuals, including the right to privacy and data protection.

(2) The scope of this Agreement covers the cooperation between Europol and the competent authorities of Brazil in the fields of activities and within the competence and tasks of Europol, as set out in the Europol Regulation, as applied in accordance with the Treaty on European Union and the Treaty on the Functioning of the European Union, and in this Agreement.

ARTICLE 2

Definitions

For the purposes of this Agreement, the following definitions apply:

(1) 'Contracting Parties' means the European Union and the Federative Republic of Brazil;

(2) 'Europol' is the European Union Agency for Law Enforcement Cooperation, set up under the Europol Regulation;

(3) 'Europol Regulation' or 'Regulation (EU) 2016/794' is the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ EU L 135, 24.5.2016, p. 53), or any amendment thereto or successor thereof;

(4) 'competent authorities' means, for Brazil, the domestic law enforcement authorities that under Brazil's national law are responsible for preventing and combating criminal offences as listed in Annex II ("competent authorities of Brazil") and for which a designated national contact point within the Brazilian Federal Police shall act as the central point of contact with Europol in accordance with Article 26, and, for the Union, Europol;

(5) 'Union bodies' means institutions, bodies, missions, offices and agencies set up by, or on the basis of the Treaty on European Union ("TEU") and the Treaty on the Functioning of the European Union ("TFEU"), listed in Annex III;

(6) 'criminal offences' are the types of crime listed in Annex I and related criminal offences; criminal offences are considered to be related to the types of crime listed in Annex I if they are committed in order to procure the means of perpetrating, to facilitate or perpetrate, or to ensure the impunity of those committing such types of crime;

(7) 'personal data' means any information relating to a data subject;

(8) 'non-personal data' means information other than personal data;

www.parlament.gv.at

(9) 'data subject' means an identified or identifiable natural person; an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(10) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;

(11) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(12) 'processing' means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(13) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(14) 'supervisory authority' means one or more domestic independent authorities that is/are, alone or cumulatively, responsible for data protection in accordance with Article 14, and that have been notified according to that Article; this may include authorities whose responsibility also covers other human rights;

(15) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body, which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

EXCHANGE OF PERSONAL DATA AND DATA PROTECTION

ARTICLE 3

Purposes of processing personal data

(1) Personal data requested and received under this Agreement shall be processed only for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties within the limits of Article 4(5) and the respective mandates of the competent authorities.

www.parlament.gv.at

(2) The competent authorities shall clearly indicate, at the latest at the moment of transferring personal data, the specific purpose or purposes for which the data are being transferred. For transfers to Europol, the purpose or purposes for such transfer shall be specified in line with the specific purpose or purposes of processing set out in the Europol Regulation. The Contracting Parties may decide by common accord that the personal data transferred may be processed for a supplementary, compatible and specific purpose, which shall be specified at the moment of such common accord and shall fall within the scope of paragraph 1 of this Article.

ARTICLE 4

General data protection principles

(1) Each Contracting Party shall provide for personal data exchanged under this Agreement to be:

(a) processed fairly, lawfully, in line with the transparency requirements in Article 29(1), and only for the purpose or purposes for which they have been transferred in accordance with Article 3;

(b) adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed;

(c) accurate and kept up to date; each Contracting Party shall provide that its competent authorities take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are rectified or erased without undue delay;

(d) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

(e) processed in a manner that ensures appropriate security of the personal data.

(2) The transferring competent authority, at the moment of transferring personal data, may indicate any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its onward transfer, erasure or destruction after a certain period of time, or the further processing of it. Where the need for such restrictions becomes apparent after the information has been provided, the transferring competent authority shall inform the receiving authority accordingly.

(3) Each Contracting Party shall ensure that the receiving competent authority complies with any restriction on access or further use of the personal data indicated by the transferring competent authority as described in paragraph 2.

(4) Each Contracting Party shall provide that its competent authorities implement appropriate technical and organisational measures in such a way as to be able to demonstrate that the processing will comply with this Agreement and the rights of the data subjects concerned are protected.

(5) Each Contracting Party shall ensure that its competent authorities do not transfer personal data which have been obtained in a manifest violation of human rights recognised by the norms of international law binding on the Contracting Parties. Each Contracting Party shall ensure that the personal data received are not used to request, hand down or execute the death penalty or any form of torture and other cruel, inhuman or degrading treatment or punishment.

www.parlament.gv.at

(6) Each Contracting Party shall ensure that a record is kept of all transfers of personal data under this Agreement and of the purpose or purposes for those transfers.

ARTICLE 5

Special categories of personal data and different categories of data subjects

(1) The transfer and further processing of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18, shall be prohibited unless such transfer is strictly necessary and proportionate in individual cases for preventing or combating a criminal offence.

(2) The transfer and further processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health, or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary and proportionate in individual cases for preventing or combating a criminal offence, and if those data, except biometric data, supplement other personal data.

(3) The Contracting Parties shall ensure that the processing of personal data under paragraphs 1 and 2 of this Article is subject to appropriate safeguards guarding against the specific risks involved, including restrictions on access, measures for data security within the meaning of Article 19 and limitations on onward transfers under Article 7.

ARTICLE 6

Automated processing of personal data

Decisions based solely on automated processing of the personal data exchanged, including profiling, which may produce an adverse legal effect on the data subject or significantly affect him or her, shall be prohibited, unless authorised at law for preventing or combating a criminal offence and with appropriate safeguards for the rights and freedoms of the data subject, including at least the right to obtain human intervention.

ARTICLE 7

Onward transfer of the personal data received

(1) Brazil shall ensure that its competent authorities only transfer personal data received under this Agreement to other authorities of Brazil if:

(a) Europol has given its prior explicit authorisation;

(b) the purpose or purposes of the onward transfer is the same as the original purpose or purposes of the transfer by Europol; and

(c) the onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

www.parlament.gv.at

Without prejudice to Article 4(2), the requirement set out in point (a) of this paragraph does not need to be fulfilled when the receiving authority is itself a competent authority of Brazil.

(2) The Union shall ensure that Europol only transfers personal data received under this Agreement to authorities in the Union other than those listed in Annex III if:

(a) Brazil has given its prior explicit authorisation;

(b) the purpose or purposes of the onward transfer is the same as the original purpose or purposes of the transfer by Brazil; and

(c) the onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

Without prejudice to Article 4(2), the requirement set out in point (a) of this paragraph does not need to be fulfilled when the receiving authority is one of the bodies or authorities listed in Annex III.

(3) Brazil shall ensure that onward transfers of personal data received by its competent authorities under this Agreement to the authorities of a third country or to an international organisation are prohibited, unless the following conditions are fulfilled:

(a) Europol has given its prior explicit authorisation;

(b) the purpose or purposes of the onward transfer is the same as the original purpose or purposes of the transfer by Europol; and

(c) the onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

(4) Europol may only grant its authorisation under paragraph 3, point a, of this Article for an onward transfer to the authority of a third country or to an international organisation if and insofar as an adequacy decision, an international agreement providing appropriate safeguards with respect to the protection of the right to privacy and fundamental rights and freedoms of individuals, a cooperation agreement or any other legal ground for transfers of personal data within the meaning of the Europol Regulation covering the onward transfer is in place.

(5) The Union shall ensure that onward transfers of personal data received by Europol under this Agreement to authorities of third countries or an international organisation are prohibited, unless the following conditions are fulfilled:

(a) Brazil has given its prior explicit authorisation;

(b) the purpose or purposes of the onward transfer is the same as the original purpose of the transfer by Brazil; and

(c) the onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

(6) In the application of this Article, onward transfers of special categories of personal data referred to in Article 5 shall be allowed only if such onward transfers are strictly necessary and proportionate in individual cases concerning criminal offences.

www.parlament.gv.at

RIGHTS OF DATA SUBJECTS

ARTICLE 8

Right of access

(1) The Contracting Parties shall ensure that the data subject has the right, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed under this Agreement, and when that is the case, access to at least the following information:

(a) confirmation as to whether or not data related to him or her are being processed;

(b) information on at least the purpose or purposes of processing, the categories of data concerned, and where applicable the recipients or categories of recipients to whom the data are disclosed;

(c) the existence of the right to request from the competent authority rectification, erasure of personal data or restriction of processing of personal data concerning the data subject;

(d) an indication of the legal basis for the processing;

(e) the envisaged period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period;

(f) communication in an intelligible form of the personal data undergoing processing and of any available information as to its sources.

(2) In cases where the right of access pursuant to paragraph 1 is exercised, the transferring Contracting Party will be consulted in writing, on a non-binding basis before a final decision on the request for access is taken.

(3) The Contracting Parties may provide for the provision of information in response to any request under paragraph 1 to be delayed, refused or restricted if and as long as such delay, refusal or restriction constitutes a measure that is necessary and proportionate taking into account the fundamental rights and interests of the data subject, in order to:

(a) ensure that any criminal investigation and prosecution will not be jeopardised;

(b) protect the rights and freedoms of third parties; or

(c) protect national security and public order or prevent crime.

(4) The Contracting Parties shall ensure that the competent authority having received the request informs the data subject in writing of any delay, refusal or restriction of access and of the reasons for such delay, refusal or restriction of access. Those reasons may be omitted if and as long as this would undermine the purpose of the delay, refusal or restriction under paragraph 3. The competent authority shall inform the data subject of the possibility of lodging a complaint with the respective supervisory authorities and of other available means of administrative and judicial redress provided for in their respective legal frameworks.

ARTICLE 9

www.parlament.gv.at

Right to rectification, erasure and restriction

(1) The Contracting Parties shall ensure that the data subject has the right to have inaccurate personal data transferred under this Agreement rectified by the competent authorities. Taking into account the purpose or purposes of the processing, this includes the right to have incomplete personal data transferred under this Agreement completed.

(1) Rectification shall include erasure of personal data that are no longer necessary for the purpose or purposes for which they are processed.

(2) The Contracting Parties may provide for the restriction of processing rather than the erasure of personal data if there are reasonable grounds to believe that such erasure could affect the legitimate interests of the data subject.

(3) The competent authorities shall inform each other of measures taken pursuant to paragraphs 1, 2 and 3. The receiving competent authority shall rectify, erase or restrict the processing in accordance with the action taken by the transferring competent authority.

(4) The Contracting Parties shall provide for the competent authority which has received the request to inform the data subject in writing without undue delay, and in any case within three months of receipt of a request in accordance with paragraph 1 or 2, that data concerning the data subject have been rectified, erased or the processing has been restricted.

(5) The Contracting Parties shall provide for the competent authority which has received the request to inform the data subject in writing, without undue delay and in any case within three months of receipt of a request of any refusal of rectification, erasure or restriction of processing, of the reasons for such a refusal and of the possibility of lodging a complaint with the respective supervisory authorities and other available means of administrative and judicial redress provided for in their respective legal frameworks.

ARTICLE 10

Notification of a personal data breach to the authorities concerned

(1) The Contracting Parties shall ensure, in the event of a personal data breach affecting personal data transferred under this Agreement, that the respective competent authorities notify each other as well as their respective supervisory authority of that personal data breach without delay, and to take measures to mitigate its possible adverse effects.

(2) The notification shall at least:

(a) describe the nature of the personal data breach including, where possible, the categories and number of data subjects concerned and the categories and number of personal data records concerned;

(b) describe the likely consequences of the personal data breach;

(c) describe the measures taken or proposed to be taken by the competent authority to address the personal data breach, including the measures taken to mitigate its possible adverse effects.

www.parlament.gv.at

(3) To the extent that it is not possible to provide all the required information at the same time, it may be provided in phases. Outstanding information shall be provided without undue further delay.

(4) The Contracting Parties shall ensure that their respective competent authorities document any personal data breaches affecting personal data transferred under this Agreement, including the facts relating to the personal data breach, its effects and the remedial action taken, thereby enabling their respective supervisory authority to verify compliance with applicable legal requirements.

ARTICLE 11

Communication of a personal data breach to the data subject

(1) The Contracting Parties shall, where a personal data breach as referred to in Article 10 is likely to severely and adversely affect the rights and freedoms of the data subject, provide for their respective competent authorities to communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject pursuant to paragraph 1 shall describe, where possible, the nature of the personal data breach, recommend measures to mitigate the possible adverse effects of the personal data breach, and provide the name and contact details of the contact point where more information can be obtained.

(3) The communication to the data subject pursuant to paragraph 1 shall not be required if:

(a) the personal data concerned by the breach were subject to appropriate technological protection measures that render the data unintelligible to any person who is not authorised to have access to that data;

(b) subsequent measures have been taken which ensure that the rights and freedoms of the data subject are no longer likely to be severely affected; or

(c) communication to the data subject pursuant to paragraph 1 would involve disproportionate effort, in particular owing to the number of cases involved; in such a case, there shall instead be a public communication or similar measure whereby the data subject is informed in an equally effective manner.

(4) The communication to the data subject pursuant to paragraph 1 may be delayed, restricted or omitted where such communication would be likely to:

(a) obstruct official or legal inquiries, investigations or procedures;

(b) prejudice the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties, public order or national security;

(c) affect the rights and freedoms of third parties;

where this constitutes a necessary and proportionate measure with due regard for the legitimate interests of the data subject concerned.

www.parlament.gv.at

ARTICLE 12

Storage, review, correction and deletion of personal data

(1) The Contracting Parties shall provide for appropriate time limits to be established for the storage of personal data received under this Agreement or for a periodic review of the need for the storage of personal data, so that personal data are stored only as long as is necessary for the purpose or purposes for which they are transferred.

(2) In any case, the need for continued storage of personal data shall be reviewed no later than three years after the personal data has been transferred, and if no justified and documented decision is taken on the continued storage of personal data, personal data shall be erased automatically after three years.

(3) Where a competent authority has reason to believe that personal data previously transferred by it are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the receiving competent authority, which shall correct or delete that data, and provide notification thereof to the transferring competent authority.

(4) Where a competent authority has reason to believe that personal data previously received are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the transferring competent authority, which shall provide its position on the matter. Where the transferring competent authority concludes that the personal data are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the receiving competent authority, which shall correct or delete that data, and provide notification thereof to the transferring competent authority.

ARTICLE 13

Logging and documentation

(1) The Contracting Parties shall provide for the keeping of logs or documentation of the collection, alteration, access, disclosure including onward transfers, combination and erasure of personal data.

(2) Logs or documentation referred to in paragraph 1 shall be made available to the respective supervisory authority upon request for the purpose of verification of the lawfulness of processing, self-monitoring and ensuring proper data integrity and security.

ARTICLE 14

Supervisory authority

(1) Each Contracting Party shall ensure that there is a public authority responsible for data protection (supervisory authority) to independently oversee matters affecting the right to privacy of individuals, including the domestic rules relevant under this Agreement, in order to protect the fundamental rights and freedoms of natural

www.parlament.gv.at

persons in relation to the processing of personal data. The Contracting Parties shall notify each other of the authority that each of them designates as the supervisory authority.

(2) The Contracting Parties shall ensure that each supervisory authority:

(a) acts with complete independence in performing its tasks and exercising its powers; it shall act free from external influence and neither seek nor accept instructions; its members shall have a secure term of office, including safeguards against arbitrary removal;

(b) has the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers;

(c) has effective powers of investigation and intervention to exercise oversight over the bodies it supervises and to engage in legal proceedings;

(d) has powers to hear complaints from individuals about the use of their personal data by the competent authorities under its supervision.

ARTICLE 15

Administrative and judicial redress

(1) Data subjects shall have the right to effective administrative and judicial redress for violations of the rights and safeguards recognised in this Agreement resulting from the processing of their personal data. The Contracting Parties shall notify each other of the domestic legislation that each of them considers as providing for the rights guaranteed under this Article.

(2) This shall include the right to compensation for any damage caused to the data subject.

CHAPTER III

EXCHANGE OF NON-PERSONAL DATA

ARTICLE 16

Data protection principles for non-personal data

(1) Each Contracting Party shall provide for the non-personal data exchanged under this Agreement to be processed fairly and lawfully, and in a manner that ensures appropriate security of the non-personal data.

(2) The transferring competent authority, at the moment of transferring non-personal data, may indicate any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its onward transfer, erasure or destruction after a certain period of time, or the further processing of it. Where the need for such restrictions becomes apparent after the data has been provided, the transferring competent authority shall inform the receiving authority accordingly.

www.parlament.gv.at

(3) Each Contracting Party shall ensure that the receiving competent authority complies with any restriction on access or further use of the non- personal data indicated by the transferring competent authority as described in paragraph 2.

(4) Each Contracting Party shall ensure that its competent authorities do not transfer non-personal data which have been obtained in a manifest violation of human rights recognised by the norms of international law binding on the Contracting Parties. Each Contracting Party shall ensure that the non-personal data received are not used to request, hand down or execute the death penalty or any form of torture and other cruel, inhuman or degrading treatment or punishment.

ARTICLE 17

Onward transfer of the non-personal data received

(1) Brazil shall ensure that its competent authorities only transfer non-personal data received under this Agreement to other authorities of Brazil or to the authorities of a third country or to an international organization, if:

(a) Europol has given its prior explicit authorisation;

(b) the onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

Without prejudice to Article 16(2), the requirement set out in point (a) of this paragraph does not need to be fulfilled when the receiving authority is itself a competent authority of Brazil.

(2) The Union shall ensure that Europol only transfers non-personal data received under this Agreement to other Union bodies or authorities of third countries or an international organisation, if:

(a) Brazil has given its prior explicit authorisation;

(b) the onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

Without prejudice to Article 16(2), the requirement set out in point (a) of this paragraph does not need to be fulfilled when the receiving authority is one of the bodies or authorities listed in Annex III.

CHAPTER IV

COMMON PROVISIONS FOR THE EXCHANGE OF PERSONAL AND NON-PERSONAL DATA

ARTICLE 18

www.parlament.gv.at

Assessment of reliability of the source of and accuracy of data

(1) The competent authorities shall indicate as far as possible, at the latest at the moment of transferring data, the reliability of the source of the data exchanged under this Agreement on the basis of one or more of the following criteria:

(a) "(A)" where there is no doubt about the authenticity, trustworthiness and competence of the source, or if the data is supplied by a source who, in the past, has proved to be reliable in all instances;

(b) "(B)" where the data is provided by a source from whom information received has in most instances proved to be reliable;

(c) "(C)" where the data is provided by a source from whom information received has in most instances proved to be unreliable;

(d) "(X)" where the reliability of the source cannot be assessed.

(2) The competent authorities shall indicate as far as possible, at the latest at the moment of transferring data, the accuracy of the data on the basis of one or more of the following criteria:

(a) "(1)" for data the accuracy of which is not in doubt at the time of transfer;

(b) "(2)" for data known personally to the source but not known personally to the official passing it on;

(c) "(3)" for data not known personally to the source but corroborated by other information already recorded;

(d) "(4)" for data which is not known personally to the source and cannot be corroborated.

(3) Where the receiving competent authority, on the basis of information already in its possession, comes to the conclusion that the assessment of data supplied by the transferring competent authority or of its source carried out in accordance with paragraphs 1 and 2 needs correction, it shall inform that competent authority and shall attempt to agree on an amendment to the assessment. The receiving competent authority shall not change the assessment of data received or of its source without such an agreement.

(4) If a competent authority receives data without an assessment, it shall attempt as far as possible and where possible in agreement with the transferring competent authority to assess the reliability of the source or the accuracy of the data on the basis of information already in its possession.

(5) If no reliable assessment can be made, the data shall be evaluated in accordance with paragraph 1, point d, and paragraph 2, point (d), as applicable.

ARTICLE 19

www.parlament.gv.at

Data security

(1) The Contracting Parties shall ensure that data transferred under this Agreement are processed in a manner that ensures appropriate data security.

(2) The Contracting Parties shall ensure the implementation of technical and organisational measures to protect data exchanged under this Agreement. The modalities for the implementation of such measures shall be laid down between Europol and the competent authorities of Brazil.

(3) In respect of automated data processing, the Contracting Parties shall ensure the implementation of measures designed to:

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

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

(e) ensure that persons authorised to use an automated 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 data may be or have been transmitted using data communication equipment (communication control);

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

(h) ensure that it is possible to verify and establish what data have been accessed by which member of personnel and at what time (access log);

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

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

(k) 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).

CHAPTER V

DISPUTES

www.parlament.gv.at

ARTICLE 20

Settlement of disputes

All disputes which may emerge in connection with the interpretation, application or implementation of this Agreement and any matters related thereto shall give rise to consultations and negotiations between representatives of the Contracting Parties with a view to reaching a mutually agreeable solution.

ARTICLE 21

Suspension clause

(1) In the event of non-fulfilment of obligations stemming from this Agreement, either Contracting Party may suspend this Agreement temporarily in part or in whole by written notification to the other Contracting Party through diplomatic channels. Such written notification shall not be made until after the Contracting Parties have engaged in a reasonable period of consultation without reaching a resolution and suspension shall take effect twenty days from the date of receipt of such notification. Such suspension may be lifted by the suspending Contracting Party upon written notification to the other Contracting Party. The suspension shall be lifted immediately upon receipt of such notification.

(2) Notwithstanding any suspension of this Agreement, personal and non-personal data falling within the scope of this Agreement and transferred prior to the suspension of this Agreement shall continue to be processed in accordance with this Agreement.

ARTICLE 22

Termination

(1) This Agreement may be terminated at any time by either of the Contracting Parties by written notification through diplomatic channels. The termination shall take effect three months after the date of receipt of the notification.

(2) If either Contracting Party gives notice of termination under this Article, the Contracting Parties shall decide what measures are needed to ensure that any cooperation initiated under this Agreement is concluded in an appropriate manner. In any event, with regard to all personal and all non-personal data obtained through cooperation under this Agreement before it ceases to be in force, the Contracting Parties shall ensure that the level of protection under which the personal and the non-personal data were transferred is maintained after the termination takes effect.

CHAPTER VI

FINAL PROVISIONS

www.parlament.gv.at

ARTICLE 23

Relation to other international instruments

This Agreement shall not prejudice or otherwise affect or impact the legal provisions with regard to the exchange of information provided for by any mutual legal assistance treaty, any other cooperation agreement or arrangement, or working law enforcement relationship for the exchange of information between Brazil and any Member State of the Union.

ARTICLE 24

Exchange of classified information

Where necessary under this Agreement, the modalities for the exchange of classified information shall be laid down between Europol and the competent authorities of Brazil.

ARTICLE 25

Requests for Public Access

Requests for public access to documents containing personal or non-personal data transferred pursuant to this Agreement shall be submitted to the transferring Contracting Party for consultation as soon as possible.

ARTICLE 26

National contact point and liaison officers

(1) Brazil shall designate a national contact point within the Brazilian Federal Police to act as the central point of contact between Europol and competent authorities of Brazil. Brazil shall notify the EU of its designated national contact point. Brazil shall ensure the continuous availability of the national contact point twenty-four hours a day, seven days a week. Any direct exchanges between Europol and other competent authorities of Brazil, which shall be limited to the context of specific operations, must receive prior and express authorisation by the national contact point.

(2) Europol and Brazil may enhance their cooperation as laid down in this Agreement through the deployment of one or more liaison officer(s) by Brazil. Europol may deploy one or more liaison officer(s) to Brazil. The liaison officers' tasks, their number, and the costs involved, shall be laid down between Europol and the Federal Police of Brazil.

ARTICLE 27

www.parlament.gv.at

Secure communication line

A secure communication line shall be established for the purpose of exchange of personal and non-personal data between Europol and the competent authorities of Brazil. The modalities for the establishment, implementation, costs and operation of the secure communication line shall be laid down between Europol and the Federal Police of Brazil.

ARTICLE 28

Expenses

The Contracting Parties shall ensure that the competent authorities bear their own expenses which arise in the course of the implementation of this Agreement, unless otherwise laid down between Europol and the Federal Police of Brazil.

ARTICLE 29

Notification of implementation

(1) Each Contracting Party shall provide for its competent authorities to make publicly available a document setting out in an intelligible form the provisions regarding the processing of personal data transferred under this Agreement, including the means available for the exercise of the rights of data subjects. Each Contracting Party shall notify a copy of that document to the other Contracting Party.

(2) Where not already in place, each Contracting Party shall ensure that the competent authorities shall adopt rules specifying how compliance with the provisions regarding the processing of personal data transferred under this Agreement will be enforced in practice. Each Contracting Party shall notify a copy of those rules to the other Contracting Party and the respective supervisory authorities.

(3) Notifications by a Contracting Party made pursuant to Articles 14(1), 15, 26(1), 29(1) and 29(2) of this Agreement shall be made through diplomatic channels, in a single note verbale.

ARTICLE 30

Entry into force and application

(1) This Agreement shall be approved by the Contracting Parties in accordance with their own procedures.

(2) This Agreement shall enter into force on the date of the receipt of the last written notification by which the Contracting Parties have notified each other through diplomatic channels that the procedures referred to in paragraph 1 have been completed.

(3) For this Agreement to enter into application, it is required that the notifications by a Contracting Party referred to in Article 29(3) are accepted by the other Contracting

www.parlament.gv.at

Party through diplomatic channels. This Agreement shall enter into application on the first day after the date of receiving the last acceptance of the notifications referred to in Article 29(3).

(4) From the time it enters into application, the Contracting Parties shall ensure that any other legal instruments governing cooperation between Europol and the competent authorities of Brazil are promptly repealed.

ARTICLE 31

Amendments and supplements

(1) This Agreement may be amended in writing, at any time by mutual consent between the Contracting Parties by written notification exchanged through diplomatic channels. The amendments to this Agreement shall enter into force in accordance with the legal procedure provided for in Article 30(1) and (2).

(2) The Annexes to this Agreement may be updated, as necessary, by exchange of diplomatic notes. Such updates shall enter into force in accordance with the legal procedure provided for in Article 30(1) and (2).

(3) The Contracting Parties shall enter into consultations with respect to the amendment to this Agreement or its Annexes at the request of either Contracting Party.

ARTICLE 32

Review and evaluation

(1) The Contracting Parties shall jointly review the implementation of this Agreement one year after its entry into force, and at regular intervals thereafter, and additionally if requested by either Contracting Party and jointly decided.

(2) The Contracting Parties shall jointly evaluate this Agreement four years after the date of its application.

(3) The Contracting Parties shall decide in advance on the modalities of the review of the implementation of this Agreement and shall communicate to each other the composition of their respective teams. The teams shall include relevant experts on data protection and law enforcement. Subject to applicable laws, any participants in a review shall be required to respect the confidentiality of the discussions and have appropriate security clearances. For the purposes of any review, the Union and Brazil shall ensure access to relevant documentation, systems and personnel.

ARTICLE 33

This Agreement shall be drawn up in duplicate in the Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish, each text being equally authentic. In the event of any divergence between the texts of this Agreement, the English text shall prevail.

www.parlament.gv.at

ANNEX I

AREAS OF CRIME

Criminal offences are:

– terrorism,
– organised crime,
– drug trafficking,
– money-laundering activities,
– crime connected with nuclear and radioactive substances,
– immigrant smuggling,
– trafficking in human beings,
– motor vehicle crime,
– murder, grievous bodily injury,
– illicit trade in human organs and tissue,
– kidnapping, illegal restraint and hostage taking,
– racism and xenophobia,
– robbery and aggravated theft,
– illicit trafficking in cultural goods, including antiquities and works of art,
– swindling and fraud,
– crime against the financial interests of the Union,
– insider dealing and financial market manipulation,
– racketeering and extortion,
– counterfeiting and product piracy,
– forgery of administrative documents and trafficking therein,
– forgery of money and means of payment,
– computer crime,
– corruption,
– illicit trafficking in arms, ammunition and explosives,
– illicit trafficking in endangered animal species,
– illicit trafficking in endangered plant species and varieties,
– environmental crime, including ship-source pollution,
– illicit trafficking in hormonal substances and other growth promoters,
– sexual abuse and sexual exploitation, including child abuse material and solicitation of children for sexual purposes,
– genocide, crimes against humanity and war crimes.

www.parlament.gv.at

The forms of crime referred to in this Annex shall be assessed by the competent authorities of Brazil in accordance with the law of Brazil and by Europol in accordance with the applicable laws of the European Union and its Member States.

www.parlament.gv.at

ANNEX II

COMPETENT AUTHORITIES OF BRAZIL

The competent authorities of Brazil are:

The Federal Police of Brazil, and

The Civil Polices of the States and the Federal District, and

The units of the Ministry of Justice and Public Security responsible for preventing and fighting criminal offences in accordance with Brazilian law.

www.parlament.gv.at

ANNEX III

UNION BODIES AND EU MEMBER STATE AUTHORITIES

(a) Union Bodies:

Common Security and Defence Policy Missions/Operations, limited to law enforcement activities

European Anti-Fraud Office (OLAF)

European Border and Coast Guard Agency (Frontex)

European Central Bank (ECB)

European Public Prosecutor's Office (EPPO)

European Union Agency for Criminal Justice Cooperation (Eurojust)

European Union Intellectual Property Office (EUIPO)

(b) the authorities responsible in the EU Member States for preventing and fighting criminal offences, in accordance with Article 2(a) and Article 7 of the Europol Regulation.

www.parlament.gv.at