Agreement
on Strategic Co-operation
between the European Union Agency for Network and Information Security and the European Police Office

The European Union Agency for Network and Information Security (hereafter referred to as "ENISA")

and

the European Police Office (hereafter referred to as "Europol"),

Hereafter jointly referred to as "the Parties" or individually referred to as "the Party"

Whereas Europol, as an entity responsible for the law enforcement co-operation at the European Union level that pursuant to the Europol Council Decision of 6 April 2009 aims to support and strengthen action by the competent authorities of the Member States in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States;

Whereas ENISA, as a body of expertise that pursuant to the Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security and repealing Regulation (EC) No 460/2004 assists the Member States, the Commission and other Stakeholders to prevent, address and respond to network and information security problems, thereby ensuring the smooth functioning of the internal market;

Whereas it is in the common interest of Europol and ENISA to exchange information and contribute to the safer cyber space through learning, awareness raising, strengthening capacity building and undertaking other activities to safeguard network and information security at the European Union level;

Aware of the urgent problems arising from international organised crime, especially terrorism, and other forms of serious crime;

Considering Article 22 of the Europol Council Decision, allowing for Europol to establish and maintain co-operative relations with the institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on the European Union and the Treaties establishing the European Communities;

Considering that the Management Board of Europol on 1 December 2011 authorised the start of negotiations between Europol and ENISA;

Considering that the Management Board of Europol has on 22 May 2013 given Europol the authorisation to agree to the present Agreement between ENISA and Europol;

Considering that the Management Board of ENISA has on 3 March 2014 given ENISA the endorsement to the present Agreement between Europol and ENISA;

Respectful of Europol's obligations under the Charter of Fundamental Rights of the European Union;

Have agreed as follows:

Article 1
Definitions

For the purpose of this Agreement:

a) "Europol Council Decision" shall mean the Council Decision of 6 April 2009 establishing the European Police Office (Europol)[1];

b) "ENISA Regulation" shall mean the Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security and repealing Regulation (EC) No 460/2004[2];

c) "Personal data" means any data relating to an identified or identifiable natural person: 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 physical, physiological, mental, economic, cultural or social identity.

Chapter I- Purpose and Scope

Article 2
Purpose of co-operation

The purpose of this Agreement is to establish co-operative relations between Europol and ENISA in order to support the Member States of the European Union and its Institutions in preventing and combating cybercrime and other forms of related crime with a view to ensuring a high and effective level of network and information security. The co-operation between the Parties will not extend or go beyond their respective mandates. This Agreement does not cover the exchange of personal data.

Article 3
Areas of co-operation

The areas of co-operation shall cover tasks within Europol's mandate as provided for in Article 3 of the Europol Council Decision and in the Annex thereto. ENISA shall operate within its mandate as provided for in the ENISA Regulation.

---

[1] OJ L 121, 15.5.2009
[2] OJ L 165/41 18.6.2013

The co-operation may in particular include the exchange of specialist knowledge and expertise, general situation reports, results of strategic analyses and best practices, as well as building capacity through training and awareness raising.

Chapter II – Mode of Co-operation

Article 4
Contact point

The Parties shall, for the purpose of information exchange, designate their contact points by means of an exchange of letters between the Director of Europol and the Executive Director of ENISA.

Article 5
Consultations and Closer Co-operation

1. The Parties agree that to further the co-operation and the enhancement as well as the monitoring of the development of the provisions of this Agreement, the regular exchanges, as appropriate, are integral. Specifically:

    a. High level meetings between Europol and ENISA shall take place regularly to discuss issues relating to this Agreement and co-operation in general.

    b. Representatives of ENISA and Europol shall consult each other regularly on policy issues and matters of common interest for the purpose of realising their objectives and co-ordinating their respective activities.

2. When appropriate, consultation shall be arranged at the required level between representatives of ENISA and Europol to agree upon and periodically review the most effective way in which to organise their particular activities.

Chapter III - Information exchange

Article 6
General Provisions

1. Exchange of information between the Parties shall only take place for the purpose of and in accordance with the other provisions of this Agreement.

2. Parties shall only supply information to each other which was collected, stored and transmitted in accordance with their respective legal frameworks.

3. Requests for public access by individuals to information transmitted on the basis of the present Agreement shall be submitted to the transmitting Party for their advice as soon as possible. The concerned information shall not be disclosed should the transmitting Party object to it.

Article 7
Use of the information

1. Information if transmitted with a purpose may be used only for the purpose for which it was transmitted and any restriction on its use, deletion or destruction, including possible access restrictions in general or specific terms must be respected by the Parties.

2. Use of information for a different purpose than the purpose for which the information was transmitted must be authorised by the transmitting Party.

Article 8
Onward transmission of the information received

Any information received by either Party under this Agreement may only be transmitted onward to a third party with the prior consent of the transmitting Party and subject to any conditions or restrictions indicated by that Party. Such consent may only be given when allowed under the applicable legal framework of the transmitting Party.

Article 9
Assessment of the source and of the information

1. When information is supplied by the Parties on the basis of this Agreement, the source of the information shall be indicated as far as possible on the basis of the following criteria:

    a. Where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances;

b. Source from whom information received has in most instances proved to be reliable;
c. Source from whom information received has in most instances proved to be unreliable;
X. The reliability of the source cannot be assessed.

2. When information is supplied by the Parties on the basis of this Agreement, the reliability of the information shall be indicated as far as possible on the basis of the following criteria:

1. Information whose accuracy is not in doubt;
2. Information known personally to the source but not known personally to the official passing it on;
3. Information not known personally to the source but corroborated by other information already recorded;
4. Information which is not known personally to the source and cannot be corroborated.

3. If either of the Parties - on the basis of information already in its possession - comes to the conclusion that the assessment of information supplied by the other Party needs correction, it shall inform the other Party and attempt to agree on an amendment to the assessment. Neither of the Parties shall change the assessment of information received without such agreement.

4. If a Party receives information without an assessment, it shall attempt as far as possible and in agreement with the transmitting Party to assess the reliability of the source or the information on the basis of information already in its possession.

5. The Parties may agree in general terms on the assessment of specified types of information and specified sources, which shall be laid down in a Memorandum of Understanding between ENISA and Europol. If information has been supplied on the basis of such general agreements, this shall be noted with the information.

6. If no reliable assessment can be made, or no agreement in general terms exists, the information shall be evaluated as at paragraph 1 (X) and paragraph 2 (4) above.

Chapter IV – Confidentiality of information

Article 10
Principles of security and confidentiality

Each Party shall:

1. protect and safeguard unclassified information subject to this Agreement and the Memorandum of Understanding referred to in Article 11, with the exception of information which is expressly marked or is clearly recognisable as being public information, by various measures including the obligation of discretion and confidentiality, limiting access to authorised personnel and general technical and procedural measures;

2. protect and safeguard classified information subject to this Agreement and the Memorandum of Understanding referred to in Article 11;

3. ensure that it has a security organisation, framework and measures in place. The Parties mutually accept and apply the basic principles and minimum standards implemented in their respective security systems and procedures to ensure that at least an equivalent level of protection is granted for classified information subject to this Agreement;

4. ensure that the premises where information subject to this Agreement is kept have an appropriate level of physical security in accordance with the respective legal framework of the Party;

5. ensure that access to and possession of information is restricted to those persons who by reason of their duties or obligations need to be acquainted with such information or need to handle it;

6. ensure that all persons who, in the conduct of their official duties require access or whose duties or functions may afford access to classified information shall be subject to a basic security screening in accordance with the respective legal framework of the Party;

7. be responsible for the choice of the appropriate classification level for information supplied to the other Party;

8. ensure that classified information subject to this Agreement keeps the classification level given to it by the originating Party. The receiving Party shall protect and safeguard the classified information according to its legal framework for the protection of classified information holding an equivalent classification level;

9. not use or permit the use of classified information subject to this Agreement except for the purposes and within any limitations stated by or on behalf of the originator, without the written consent of the originator;

10. not disclose or permit the disclosure of classified information subject to this Agreement to third parties, without the prior written consent of the originator.

Article 11
Memorandum of Understanding on Confidentiality and Information Assurance

The protection of the information exchanged between the Parties, shall be regulated in a Memorandum of Understanding on Confidentiality and Information Assurance agreed between the Parties implementing the principles outlined in this Chapter. Such Memorandum shall include in particular provisions on the Parties' security organisation, education and training, standards of security screening, table of equivalence, handling of classified information and values of information assurance. Exchange of classified information is conditional upon the conclusion of the Memorandum of Understanding on Confidentiality and Information Assurance.

Chapter V - Disputes and Liability

Article 12
Liability

1. The Parties shall be liable, in accordance with their respective legal frameworks, for any damage caused to an individual as a result of legal or factual errors in information exchanged. In order to avoid its liability under their respective legal frameworks vis-à-vis an injured party, neither Party may plead that the other had transmitted inaccurate information.

2. If these legal or factual errors occurred as a result of information erroneously communicated or of failure on the part of the other Party to comply with their obligations, they shall be bound to repay, on request, any amounts paid as compensation under paragraph 1 above, unless the information was used by the other Party in breach of this Agreement.

3. The Parties shall not require each other to pay for punitive or non-compensatory damages under paragraphs 1 and 2 above.

Article 13
Settlement of Disputes

1. All disputes which may emerge in connection with the interpretation or application of the present Agreement shall be settled by means of consultations and negotiations between representatives of the Parties.

2. In the event of serious failures of either Party to comply with the provisions of this Agreement, or a Party is of the view that such a failure may occur in the near future, either Party may suspend the application of this Agreement temporarily, pending the application of paragraph 1. Obligations inherent upon the Parties under the Agreement will nonetheless remain in force.

Chapter VI - Final Provisions

Article 14
Expenses

The Parties shall bear their own expenses which arise in the course of implementation of the present Agreement, unless otherwise stipulated in this Agreement.

Article 15
Amendments and Supplements

1. This Agreement may be amended in writing, at any time by mutual consent between the Parties. Any amendments must receive the prior endorsement or approval of the respective Management Board.

2. The Parties shall enter into consultations with respect to the amendment of this Agreement at the request of either of them.

Article 16
Entry into force and validity

This Agreement shall enter into force on the date of the last signature.

Article 17

Termination of the Agreement

1. This Agreement may be terminated in writing by either of the Parties with three months' notice.

2. In case of termination, the Parties shall reach agreement on the continued use and storage of the information that has already been communicated between them. If no agreement is reached, either of the two Parties is entitled to require that the information which it has communicated be destroyed or returned to the transmitting Party.

3. Without prejudice to paragraph 1, the legal effects of this Agreement remain in force

Done at The Hague, on the 26/06/2014 in duplicate in the English language.

For **ENISA**

Udo Helmbrecht
Executive Director

For **Europol**

Rob Wainwright
Director