The Hague, July 2014

Draft Memorandum of Understanding
on Confidentiality and Information Assurance
between the Republic of Moldova and the European Police Office

The Republic of Moldova

and

the European Police Office (hereafter referred to as "the Parties")

Considering that the Parties have established cooperative relations in order to support the Member States of the European Union and **the Republic of Moldova** in preventing and combating organised crime, terrorism and other forms of international crime by concluding an Agreement on Operational and Strategic Co-operation on XX.XX.XXXX (hereafter referred to as "the Agreement")

Aware of the necessity to protect and safeguard information, both classified and unclassified, exchanged between the Parties on the basis of the Agreement;

Having regard to Article 19 of the Agreement, which requires the Parties to adhere to specific standards of confidentiality;

Having regard to Article 20 of the Agreement which requires that the Parties shall implement the principles outlined in Article 19 of the Agreement by concluding a Memorandum of Understanding, which 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,

Bearing in mind that the exchange of classified information is conditional upon this Memorandum of Understanding on confidentiality and Information Assurance entering into force,

HAVE AGREED AS FOLLOWS:

Article 1
Purpose

The purpose of this Memorandum of Understanding is to regulate the protection of the information exchanged between the Parties by implementing the principles outlined in Article 19 of the Agreement.

Article 2
Definitions

For the purpose of this Annex:

a) "information" means knowledge that may be communicated in any form and which can include personal and/or non-personal data;
b) "classified information" means any information determined to require protection against unauthorised disclosure, which has been so designated by a classification marking;
c) "classification level" means a security marking assigned to a document indicating the security measures that need to be applied to the information;

d) "information system" means the entire infrastructure, organisation, personnel, and technical components for the collection, processing, storage, transmission, display, dissemination, disposition and deletion of information subject to this Memorandum of Understanding.
e) "risk assessment" means a structured process for examining information security threats, vulnerabilities and impacts to the business through the loss of Confidentiality, Integrity and/or Availability of information or an information system, in order to determine whether additional security controls are required.
f) "accreditation" means the process performed in order to obtain assurance that all appropriate security measures have been implemented and that a sufficient

level of protection of the classified information and of the information system has been achieved in accordance with this Memorandum of Understanding. The accreditation process determines the maximum classification level of the information that may be handled in an information system as well as the corresponding terms and conditions.

g) "security incident" means a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

h) "audit" means a structured process of examination, review, assessment and reporting on the use of information or information system by one or more competent people who are independent of the situation, system, process, function etc. being audited.

CHAPTER 1
Confidentiality

Article 3
Principles

Each Party shall:

1. protect and safeguard unclassified information subject to the Agreement and this Memorandum of Understanding, 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 the Agreement and this Memorandum of Understanding as outlined hereafter;

Article 4
Security Organisation

Each Party shall ensure that it has a security organisation, framework and measures in place. Parties shall ensure that:

1. the security organisation comprises roles defined with responsibility for security on various hierarchical layers;
2. information asset owners are identified;
3. a designated entity responsible for managing information risks is identified;
4. a designated entity responsible for accrediting information systems handling classified information subject is identified;
5. a designated entity responsible for the security of information in electronic form is identified;
6. a designated entity responsible for handling of cryptographic material, if used, is identified.

Article 5
Education, training and awareness

Each Party shall ensure that all staff processing information are familiar with the security framework in general and are aware of the procedures for reporting issues of security concern. They shall further ensure that staff who manage and maintain the secure configuration of information systems and those with access to information assets are appropriately trained and are aware of the incident reporting procedures.

Article 6
Security screenings and clearances

Each Party shall ensure that:

1. 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;
2. all persons who, in the conduct of their official duties require access or whose duties or functions may afford access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above or its equivalent in **the Republic of Moldova** in its registry, are appropriately security cleared before they are granted access to such information;
3. the security clearance procedures are designed to determine whether an individual can, taking into account his or her loyalty, trustworthiness and reliability, have access to classified information;
4. an individual's continuing eligibility for access to classified information is regularly reviewed.

Article 7
Choice of classification level

1. Each Party shall be responsible for the choice of the appropriate classification level for information supplied to the other Party.
2. If either Party – on the basis of information already in its possession – concludes that the choice of classification level needs amendment, it shall inform the other Party and attempt to agree on an appropriate classification level. Neither Party shall specify or change a classification level of information supplied by the other Party without its written consent.
3. Each Party may at any time request an amendment of the classification level related to the information it has supplied, including a possible removal of such a level. The other Party shall amend the classification level in accordance with such requests. Each Party shall, as soon as circumstances allow, request that the classification level be downgraded or removed altogether.
4. Each Party may specify the time period for which the choice of classification level related to the information it has supplied shall apply, and any possible amendments to the classification level after such period.
5. Where information of which the classification level is amended in accordance with this Article has been supplied to third parties, all recipients shall be informed of the change of classification level.

Article 8
Table of equivalence

The Parties determine that the following classification levels under the national legislation of **the Republic of Moldova** and classification levels used within Europol are equivalent and will provide equivalent protection to the information marked with such a classification level:

For the Republic of Moldova	**For Europol**
"Restricţionat"	"RESTREINT UE / EU RESTRICTED"
"Confidenţial"	"CONFIDENTIEL UE / EU CONFIDENTIAL"
"Secret"	"SECRET UE / EU SECRET"
"Strict secret"	"TRÈS SECRET UE / EU TOP SECRET"

Article 9
Registration

Each Party shall record all information classified CONFIDENTIEL UE / EU CONFIDENTIAL and above or its equivalent in **the Republic of Moldova** in its registry. The recorded information shall be at least the minimum required to uniquely identify the information in question, such as its reference number, subject, date and classification level.

Article 10
Marking

Each Party shall ensure that classified information is always clearly marked by the designations specified in Article **8** to allow recognition of the classification level.

Article 11
Storage

All classified information shall be stored in a secure manner corresponding to the respective legal framework of the Party.

Article 12
Reproduction and translation

1. Each Party shall ensure that the number of reproductions of classified information is limited to what is strictly necessary to meet essential requirements. The security measures applicable to the original information shall also be applicable to reproductions thereof.
2. Each Party shall ensure that all individual reproductions of information classified CONFIDENTIEL UE / EU CONFIDENTIAL and above or its equivalent in **the Republic of Moldova** bear a unique number allowing the identification of each individual reproduction of the information.
3. Reproductions in whole or in part of information classified TRÈS SECRET UE / EU TOP SECRET or its equivalent in **the Republic of Moldova** shall not be made without the prior written consent of the originator, who may specify other restrictions.
4. All translations of classified information shall be considered to be reproductions of the original information.

Article 13
Dispatch

1. Classified information shall be dispatched in a secure manner in accordance with the legal framework of the transmitting Party to prevent unauthorised disclosure.

2. Information classified CONFIDENTIEL UE / EU CONFIDENTIAL and above or its equivalent in **the Republic of Moldova** is to be exchanged between the responsible registries of the Parties.

3. Dispatch of information classified CONFIDENTIEL UE / EU CONFIDENTIAL or its equivalent in the Republic of Moldova shall be documented by the responsible registries.

4. Receipt of classified information shall be confirmed.

Article 14
Destruction

1. Each Party shall ensure that classified information which is no longer required is destroyed by methods which meet relevant standards so as to prevent reconstruction in whole or in part.

2. Classified waste resulting from the preparation of classified information shall be destroyed using the same care and methods that are used to destroy the classified information.

3. For classified information CONFIDENTIEL UE / EU CONFIDENTIAL and above or its equivalent in **the Republic of Moldova,** the destruction shall be recorded by the registry in accordance with the respective legal framework of the Party.

Article 15
Assessments

Each Party shall allow the other Party to visit its territory or premises, upon receipt of a written permit, in order to assess its procedures and facilities for the protection of classified information received from the other Party. The arrangements for such visit will be agreed bilaterally. Each Party shall assist the other Party in ascertaining whether classified information which has been made available by the other Party is adequately protected.

Article 16
Compromise of classified information

1. The Security Authority of either Party shall notify immediately the Security Authority of the other Party of any potential compromise of classified information.
2. When an unauthorized disclosure has occurred, both Parties shall cooperate duly in the investigation and inform each other on the results.

CHAPTER 2
INFORMATION ASSURANCE

Article 17
Information security policy

Each Party shall have, as a component of their overarching security policy, an information security policy setting out how they, and their delivery partners, comply with the minimum requirements set out in this Memorandum of Understanding.

Article 18
Managing information risk

Each Party shall conduct information risk assessments on a regular basis and when there is a significant change in a risk component (Threat, Vulnerability, Impact etc.) to existing information systems in operation. The assessment and the risk management decisions made shall be recorded in relevant Risk Management documentation.

Article 19
Accreditation

Each Party shall ensure that information systems processing classified information subject to this Memorandum of Understanding are accredited at the appropriate level. The accreditation status shall be reviewed at regular intervals to judge whether material changes have occurred which could alter the original accreditation decision.

Article 20
Audit

Each Party shall conduct security audits to information systems that process classified information subject to this Memorandum of Understanding.

Article 21
Identity and Access Management

Each Party shall have suitable identification and authentication controls for information systems that process classified information subject to this Memorandum of Understanding.

Article 22
Cryptography

Each Party shall use cryptographic controls for the secure exchange of classified information subject to this Memorandum of Understanding. Cryptographic devices shall be approved in accordance with the legal framework of the transmitting Party.

Article 23
Eavesdropping and Electro-Magnetic Countermeasures

Information systems handling information classified CONFIDENTIEL UE / EU CONFIDENTIAL and above or its equivalent in **the Republic of Moldova** shall be protected on the basis of a risk assessment in such a way that the information cannot be compromised by eavesdropping and/or electromagnetic emanations.

Article 24
Reporting incidents

Each Party shall have clear policies and procedures for reporting, managing and resolving security incidents and breaches.

Article 25
Removable media

Each Party shall have policies and procedures on the appropriate use and protection of removable media used to store classified information subject to this Memorandum of Understanding.

Article 26
Secure disposal

Each Party shall ensure that all media used for storing or processing classified information shall be securely disposed of or erased in accordance with the respective legal framework of the Party.

CHAPTER 3
FINAL PROVISIONS

Article 27
Entry into force

This Memorandum of Understanding shall enter into force on the first day of the month following signature by the last Party and, in any case, not before the Agreement has entered into force. The exchange of classified information shall only take place after the entry into force of this Memorandum of Understanding.

Article 28
Amendment and termination

1. This Memorandum of Understanding may be amended in writing, at any time by mutual consent between the Parties.
2. This Memorandum of Understanding may be terminated in writing by either of the Parties with three months' notice. In that case the legal effects of this Memorandum of Understanding remain in force.
3. This Memorandum of Understanding terminates automatically on the day the Agreement is terminated.

Done at _____ , on the _____ in duplicate in Romanian and English languages, each text being equally authentic.

For **the Republic of Moldova** For Europol