МЕМОРАНДУМ
про взаєморозуміння між Україною та Європейським поліцейським офісом стосовно конфіденційності та забезпечення збереження інформації

Україна

та

Європейський поліцейський офіс (Європол)

(далі – Сторони),

ураховуючи, що Сторони встановили відносини співробітництва з метою підтримки України та держав-членів Європейського Союзу в запобіганні та боротьбі з організованою злочинністю, тероризмом та іншими формами міжнародної злочинності шляхом укладення Угоди про оперативне та стратегічне співробітництво (далі – Угода),

усвідомлюючи необхідність захисту та охорони як інформації з обмеженим доступом, так і несекретної інформації, обмін якою здійснюється між Сторонами на підставі Угоди,

беручи до уваги статтю 19 Угоди, згідно з якою Сторони повинні дотримуватися визначених правил конфіденційності,

беручи до уваги статтю 20 Угоди, згідно з якою Сторони повинні реалізовувати принципи, викладені у статті 19 Угоди, шляхом укладення Меморандуму про взаєморозуміння, який повинен включати, зокрема, положення щодо організації системи безпеки Сторін, навчань і тренінгів, стандартів перевірки для секретної роботи, таблицю еквівалентності, процедуру обробки інформації з обмеженим доступом та оцінки забезпечення збереження інформації.

зважаючи, що обмін інформацією з обмеженим доступом є можливим лише за умови набрання чинності цим Меморандумом про взаєморозуміння стосовно конфіденційності,

домовилися про таке:

16

Стаття 1

Мета

Метою цього Меморандуму про взаєморозуміння є врегулювання процедури захисту інформації, обмін якою здійснюється між Сторонами, шляхом реалізації принципів, викладених у статті 19 Угоди.

Стаття 2

Визначення

Для цілей цього Меморандуму про взаєморозуміння:

a) «інформація» означає знання, яке може бути передано в будь-якій формі та яке може включати персональні й/або неперсональні дані;

b) «інформація з обмеженим доступом» означає будь-яку інформацію, визначену як така, що вимагає захисту від несанкціонованого розголошення, яку було визначено такою позначенням секретності;

c) «рівень секретності» означає захисне позначення, яке надається документу і яким зазначено заходи безпеки, які необхідно застосовувати до інформації;

d) «інформаційна система» означає цілісність інфраструктури, організації, кадрових та технічних компонентів для збору, обробки, зберігання, передачі, відтворення, поширення, розміщення і видалення інформації відповідно до цього Меморандуму про взаєморозуміння;

e) «оцінка ризику» означає структурований процес для вивчення загроз інформаційній безпеці, вразливості інформації та впливу на діяльність внаслідок порушення правил конфіденційності, цілісності та/або доступності інформації або інформаційної системи з метою визначення доцільності вжиття додаткових заходів безпеки;

f) «акредитація» означає процес, який здійснюється для гарантування реалізації всіх необхідних заходів безпеки і достатнього рівня захисту інформації з обмеженим доступом та інформаційної системи відповідно до цього Меморандуму про взаєморозуміння. Процес акредитації визначає максимальний рівень секретності інформації, яка може оброблятися в інформаційній системі, а також відповідні умови;

g) «випадок порушення системи безпеки» означає один або низку небажаних або несподіваних випадків у системі інформаційної безпеки, що мають значну ймовірність нанесення шкоди операційній діяльності та становлять загрозу інформаційній безпеці;

h) «аудит» означає структурований процес вивчення, розгляду, оцінки та звітування щодо використання інформації або інформаційної системи, який здійснюється однією або декількома компетентними особами, які є незалежними від ситуації, системи, процесу, посади тощо.

ГЛАВА 1
КОНФІДЕНЦІЙНІСТЬ

Стаття 3
Принципи

Кожна Сторона зобов'язується:

1. захищати та охороняти несекретну інформацію відповідно до Угоди та цього Меморандуму про взаєморозуміння, за винятком інформації, яка є явно позначена або чітко визначена як публічна, за допомогою різноманітних заходів, включаючи зобов'язання щодо обмеження доступу і конфіденційності інформації, обмеження доступу для уповноваженого персоналу та загальні технічні і процедурні заходи;

2. захищати і охороняти інформацію з обмеженим доступом відповідно до Угоди та цього Меморандуму про взаєморозуміння.

Стаття 4
Організація щодо безпеки

Кожна Сторона забезпечує у себе наявність організації, системи і заходів щодо безпеки. Кожна Сторона гарантує:

1. організацію щодо безпеки, якою визначаються посадові функції з відповідальністю за забезпечення безпеки на різних ієрархічних рівнях;

2. визначення власників інформаційних активів;

3. визначення суб'єкта, призначеного відповідальним за управління інформаційними ризиками;

4. визначення суб'єкта, призначеного відповідальним за акредитацію інформаційних систем, які здійснюють обробку інформації з обмеженим доступом відповідно до цього Меморандуму про взаєморозуміння;

5. визначення суб'єкта, призначеного відповідальним за безпеку інформації в електронному вигляді;

6. визначення суб'єкта, призначеного відповідальним за обробку криптографічного матеріалу, якщо такий використовується.

Стаття 5
Навчання, тренінги та інформування

Кожна Сторона гарантує, що всі співробітники, які здійснюють

обробку інформації відповідно до цього Меморандуму про взаєморозуміння, ознайомлені із системою безпеки в цілому та поінформовані щодо процедури повідомлення з питань безпеки. Сторони також гарантують, що співробітники, які управляють і підтримують конфігурацію інформаційних систем безпеки, і співробітники, які мають доступ до інформаційних активів, належним чином навчені і поінформовані щодо процедури повідомлення про випадки порушення системи безпеки.

Стаття 6
Перевірка для секретної роботи й дозвіл на доступ

Кожна Сторона забезпечує:

1. щоб усі особи, яким під час виконання їхніх службових обов'язків необхідний доступ до інформації з обмеженим досвідом, або чиї обов'язки або функції можуть дозволити доступ до інформації з обмеженим доступом на рівні «Для службового користування»/«RESTREINT UE/EU RESTRICTED», пройшли необхідну перевірку для секретної роботи з метою визначення того, чи може особа, ураховуючи її лояльність, довіру до неї та надійність, мати доступ до такої інформації;

2. регулярний перегляд тривалого права особи на доступ до інформації з обмеженим доступом.

Стаття 7
Вибір рівня секретності

1.Кожна Сторона відповідає за вибір відповідного рівня секретності інформації, що надається іншій Стороні.

2. Якщо будь-яка зі Сторін – на основі інформації, якою вона вже володіє, – доходить висновку, що вибір рівня секретності потребує внесення змін, вона інформує іншу Сторону й намагається погодити відповідний рівень секретності. Жодна зі Сторін не може скасувати або змінити рівень секретності інформації, який надається іншою Стороною, без її письмової згоди.

3. Кожна Сторона може в будь-який час зробити запит про внесення змін до рівня секретності стосовно наданої нею інформації, зокрема про можливе скасування такого рівня. Відповідно до таких запитів інша Сторона вносить зміни до рівня секретності. Кожна Сторона, як тільки дозволять обставини, звертається з проханням стосовно зниження або повного скасування рівня секретності.

4. Кожна Сторона може визначити строк, протягом якого застосовується вибраний рівень секретності стосовно наданої нею

інформації, а також будь-які можливі зміни рівня секретності після закінчення цього строку.

5. У випадках, коли інформацію, до рівня секретності якої внесено зміни згідно із цією статтею, уже надано третім сторонам, усі отримувачі інформуються про зміни рівня секретності.

Стаття 8
Таблиця еквівалентності

Сторони визначають, що наведені нижче рівні секретності згідно з національним законодавством України й рівні секретності, що застосовуються в Європолі, є еквівалентними й забезпечуватимуть еквівалентний захист інформації, позначеної таким рівнем секретності:

Україна	Європол
Для службового користування	RESTREINT UE / EU RESTRICTED

Стаття 9
Позначення

Кожна Сторона гарантує, що інформація з обмеженим доступом відповідно до цього Меморандуму про взаєморозуміння завжди чітко позначається, як це зазначено у статті 8, для визначення рівня секретності.

Стаття 10
Зберігання

Уся інформація з обмеженим доступом відповідно до цього Меморандуму про взаєморозуміння підлягає зберіганню в безпечний спосіб, згідно з відповідним законодавством Сторони.

Стаття 11
Репродукція та переклад

1. Кожна Сторона гарантує, що кількість репродукцій інформації з обмеженим доступом обмежується кількістю, що є чітко необхідною для задоволення основних потреб. Заходи безпеки, які застосовуються до оригінальної інформації, також застосовуються до її репродукцій.

2. Усі переклади інформації з обмеженим доступом для цілей цього Меморандуму про взаєморозуміння вважаються репродукціями оригінальної інформації.

Стаття 12
Передача

1. Інформація з обмеженим доступом повинна передаватися в безпечний спосіб відповідно до законодавства Сторони, яка передає таку інформацію.

2. Отримання інформації з обмеженим доступом повинно підтверджуватися.

Стаття 13
Знищення

1. Кожна Сторона гарантує, що інформація з обмеженим доступом, яка більше не є потрібною, знищується у спосіб, у який буде дотримано відповідні стандарти з метою запобігання відновленню такої інформації в цілому або частково.

2. Відходи, що утворюються після підготовки інформації з обмеженим доступом, знищуються з такою самою ретельністю та у такий самий спосіб, що використовується для знищення інформації з обмеженим доступом.

Стаття 14
Оцінки

Кожна Сторона дозволяє іншій Стороні відвідати свою територію або приміщення після отримання письмового дозволу для оцінки її процедур і об'єктів для захисту інформації з обмеженим доступом, отриманої від іншої Сторони. Домовленість про такий візит повинна бути погоджена у двосторонньому порядку. Кожна Сторона надає допомогу іншій Стороні в установленні того, чи належним чином захищено інформацію з обмеженим доступом, яку надано іншою Стороною.

Стаття 15
Несанкціоноване розголошення інформації з обмеженим доступом

1. Уповноважений орган з безпеки інформації кожної Сторони негайно повідомляє уповноваженому органу з безпеки інформації іншої Сторони про будь-яке можливе несанкціоноване розголошення інформації з обмеженим доступом.

2. У випадках, коли відбулося несанкціоноване розголошення, обидві Сторони співробітничають належним чином у проведенні розслідування та інформують одна одну про результати.

ГЛАВА 2
ЗАБЕЗПЕЧЕННЯ ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ

Стаття 16
Політика інформаційної безпеки

Кожна Сторона повинна мати, як складову своєї комплексної політики безпеки, політику інформаційної безпеки, якою визначається те, як Сторони та їхні партнери з передачі інформації дотримуються мінімальних вимог, установлених у цьому Меморандумі про взаєморозуміння.

Стаття 17
Управління інформаційними ризиками

Кожна Сторона проводить оцінку інформаційного ризику на регулярній основі та у випадках, коли існують істотні зміни у ризиковій складовій (загроза, вразливість, вплив тощо) в існуючих в експлуатації інформаційних системах. Рішення з оцінки та управління ризиками фіксуються у відповідній документації з управління ризиками.

Стаття 18
Акредитація

Кожна Сторона гарантує, що інформаційні системи, які обробляють інформацію з обмеженим доступом відповідно до цього Меморандуму про взаєморозуміння, є акредитованими. Стан акредитації підлягає перегляду на регулярній основі з метою оцінки того, чи відбулися істотні зміни, які можуть змінити початкове рішення про акредитацію.

Стаття 19
Аудит

Кожна Сторона має проводити аудит з безпеки стосовно інформаційних систем, що обробляють інформацію з обмеженим доступом відповідно до цього Меморандуму про взаєморозуміння.

Стаття 20
Управління ідентифікацією і доступом

Кожна Сторона повинна здійснювати належний контроль ідентифікації та автентифікації інформаційних систем, які обробляють інформацію з обмеженим доступом відповідно до цього Меморандуму про взаєморозуміння.

Стаття 21
Криптографія

Кожна Сторона повинна використовувати криптографічні засоби управління для безпечного обміну інформацією з обмеженим доступом відповідно до цього Меморандуму про взаєморозуміння. Криптографічні пристрої повинні бути затверджені відповідно до законодавства Сторони, що передає інформацію.

Стаття 22
Інформування про випадки порушення системи захисту

Кожна Сторона повинна мати чітку політику та процедури щодо інформування, управління та вирішення випадків порушення системи захисту.

Стаття 23
Знімні носії інформації

Кожна Сторона повинна мати політику і процедури щодо належного використання і захисту знімних носіїв інформації, що використовуються для зберігання інформації з обмеженим доступом відповідно до цього Меморандуму про взаєморозуміння.

Стаття 24
Безпечна утилізація

Кожна Сторона гарантує, що всі носії інформації, використовувані для зберігання або обробки інформації з обмеженим доступом, будуть безпечно утилізовані або стерті відповідно до відповідного законодавства Сторони.

ГЛАВА 3
ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Стаття 25
Набрання чинності

Цей Меморандум набирає чинності з дати надіслання Європолом дипломатичними каналами письмового повідомлення Україні про отримання та прийняття повідомлення України про завершення нею внутрішньодержавних ратифікаційних процедур, необхідних для набрання ним чинності.

Обмін інформацією з обмеженим доступом здійснюється лише після набрання чинності цим Меморандумом про взаєморозуміння.

Стаття 26
Внесення змін та припинення дії

1. До цього Меморандуму про взаєморозуміння в будь-який час може бути внесено зміни за взаємною згодою Сторін у письмовій формі.

2. Дію цього Меморандуму про взаєморозуміння може бути припинено будь-якою зі Сторін шляхом надіслання за три місяці до цього письмового повідомлення. У такому випадку юридичні наслідки застосування цього Меморандуму про взаєморозуміння зберігаються.

3. Дія цього Меморандуму про взаєморозуміння автоматично припиняється у день припинення дії Угоди.

Учинено в м. Київ, 03 липня 2017 року у двох примірниках українською та англійською мовами. У разі виникнення розбіжностей щодо тлумачення положень цього Меморандуму про взаєморозуміння перевага надається тексту англійською мовою.

За Україну
Арсен Аваков
Міністр внутрішніх справ

За Європол
Роб Уейнрайт
Директор

EUROPOL

Memorandum of Understanding
on Confidentiality and Information Assurance
between Ukraine and the European Police Office

Ukraine
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 Ukraine in preventing and combating organised crime, terrorism and other forms of international crime by concluding an Agreement on operational and strategic cooperation (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 the entry into force of this Memorandum of Understanding on confidentiality,

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 Memorandum of Understanding:

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 classified information and of 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 to this Memorandum of Understanding 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 subject to this Memorandum of Understanding 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 at the level Для_службового_користування/RESTREINT UE/EU RESTRICTED shall be subject to an appropriate security screening to determine whether an individual can, taking into account his or her loyalty, trustworthiness and reliability, have access to such information;
2. an individual's continuing eligibility for access to such 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 remove 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 Ukraine and classification levels used within Europol are equivalent and will provide equivalent protection to the information marked with such a classification level:

Ukraine	Europol
Для_службового_користування_	RESTREINT UE / EU RESTRICTED

Article 9
Marking

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

Article 10
Storage

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

Article 11
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. All translations of classified information shall be, for the purposes of this Memorandum of Understanding, considered to be reproductions of the original information.

Article 12
Dispatch

1. Classified information shall be dispatched in a secure manner in accordance with the legal framework of the transmitting Party
2. Receipt of classified information shall be confirmed.

Article 13
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.

Article 14
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 15
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 16
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 17
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 18
Accreditation

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

Article 19
Audit

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

Article 20
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 21
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 22
Reporting incidents

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

Article 23
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 24
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 25
Entry into force

This Memorandum of Understanding shall enter into force on the date on which Europol notifies Ukraine in writing through diplomatic channels that it has received and accepted notification of Ukraine that its internal ratification procedures have been completed.

The exchange of classified information shall only take place after the entry into force of this Memorandum of Understanding.

Article 26
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 Kiev, on the 3rd of July in duplicate in the Ukrainian and English languages. In case of any divergences in interpretation of this Memorandum of Understanding, the English text shall prevail.

For Ukraine

Arsen Avakov
Minister of Internal Affairs

For Europol

Rob Wainwright
Director