



**Навчальним закладам та
неурядовим організаціям
(за списком)**

Щодо практичного семінару CyberEast

15-16.04.2021 проєкт CyberEast проводитиме робочий практичний семінар щодо довіри та співпраці у контексті боротьби з кіберзлочинністю та роботи з електронними доказами (інформація про захід додається).

Метою заходу є обговорення особливостей публічно-приватного партнерства та довіри між ними у контексті виконання зобов'язань ст. 15 Будапештської конвенції про кіберзлочинність, а також стандартів захисту персональних даних.

Захід проводитиметься онлайн англійською мовою з послідовним перекладом українською, кількість учасників необмежена.

У зв'язку із вищевикладеним, просимо опрацювати можливість залучення представників установи до практичного семінару і зареєструватися за посиланням:

https://docs.google.com/forms/d/e/1FAIpQLSeyYvNpQ1JKMlPHUdJLJK_KOisDU_ZUrUXwSF93VnYBxC_Phg/viewform.

Додаток: на 4 арк.

**Директор Департаменту
Європейського Союзу і НАТО**

Марина МИХАЙЛЕНКО

Вик. Б. Мартинюк, 279 78 97
bogdana.martyniuk@mfa.gov.ua



ДОКУМЕНТ СЕД МЗС АСКОД

Підписувач Михайленко Марина Юріївна
Сертифікат 58E2D9E7F900307B040000095622D0082C27C00
Дійсний з 17.12.2019 0:00:00 по 17.12.2021 0:00:00



МЗС

311/17-690-19044 від 25.03.2021

Вхід. № 46
29" 03 2021

Funded
by the European Union
and the Council of Europe



COUNCIL OF EUROPE



Implemented
by the Council of Europe

February 2021

Activity Code 2.3.4 / PMM 96791

2088_109 Workshop with personal data protection authorities and national communications regulators on trust and cooperation in relation to cybercrime and electronic evidence action

15-16 April 2021, Kyiv, Ukraine (online)

**Organized by the European Union and Council of Europe
CyberEast project**

Outline

Background

As societies rely increasingly on the use of information technology, cybercrime and the use of electronic evidence become challenges for criminal justice authorities and to the rule of law. With offences involving computers and electronic evidence evolving rapidly both in number and in sophistication, the necessity to effectively combat criminal offences by facilitating their detection, investigation and prosecution should be counterbalanced by the equally important needs of protecting fundamental human rights and freedoms - most importantly, right to private and family life, home and correspondence.

Article 15 of the Budapest Convention seeks to ensure protection of fundamental rights and freedoms by mandating that each party to the Convention establishes in its domestic law that certain conditions and safeguards are to be applied in relation to the abovementioned procedural powers. Beyond practical implications for the use procedural powers under the Convention, it is also a provision that helps to build trust between criminal justice authorities and the society as a whole, requiring balanced approach between the interests of investigation and the individual rights involved.

As part of safeguards and guarantees provided by Article 15, the issue of the protection of personal data in law enforcement operations has become more prominent in recent years as the number of cybercrime investigations, including cross-border ones, has increased exponentially. On the other hand, newer standards of personal data protection (GDPR, modernized Council of Europe Convention 108, etc.) have provided for further guarantees to data protection oversight of law enforcement operations in cyberspace, including criminal investigations. The aspects of human rights and data protection have been highly relevant in the implementation of the [CyberEast project](#), as attested by specialized regional studies on [Article 15](#) and [Data Protection](#) in the Eastern Partnership, respectively.

On the other hand, cooperation between public and private sector and in particular between law enforcement authorities (LEA) and Internet Service Providers (ISP) has always been important in order to ensure effective criminal justice response and fight against cybercrime. In this context, the CyberEast project aims to support the countries of the Eastern Partnership in building and



ДОКУМЕНТ СЕД МЗС АСКОД

МЗС

Підписувач [Михайленко Марина Юріївна](#)
Сертифікат [58E2D9E7F900307B040000095622D0082C27C00](#)
Дійсний з [17.12.2019 0:00:00](#) по [17.12.2021 0:00:00](#)



311/17-690-19044 від 25.03.2021

maintaining partnerships with private sector entities, primarily Internet Service Providers (ISPs), for reinforcing mechanisms for trusted cooperation between the private sector, citizens and criminal justice authorities. In particular, partnerships with already established platforms for public-private dialogue on IT and security are sought to maximize impact and visibility.

Therefore, the Workshop organized under the CyberEast project intends to facilitate discussion with national counterparts about aspects of trust and cooperation between criminal justice authorities, personal data protection authorities and national communications regulators in the context of Budapest Convention Article 15 guarantees, personal data protection and public-private cooperation.

Expected outcome

Organized by joint EU/Council of Europe CyberEast project, the event contributes directly to output 2.3 of the CyberEast project (*Internal and external accountability and oversight including role of civil society organisations reinforced*); more specifically, the event is a part of series of national discussions in the Eastern Partnership states on aspects of trust and cooperation between criminal justice authorities, personal data protection authorities and national communications regulators in the context of Budapest Convention Article 15 guarantees, personal data protection and public-private cooperation.

By the end of the event, the participants are expected to agree on the ways in which the CyberEast project, in cooperation with other entities of the Council of Europe, could support improvement of trust and cooperation between respective stakeholders in Ukraine, with a further view to continue these discussions on a regional level.

Participants

As the event is conducted virtually with simultaneous interpretation into Ukrainian language, there is no limitation on the number of interested participants. The only requirement for participants is to undergo registration at the following link: [Registration Form](#), which also includes a short survey/questions related to the event.

Overall, the following participants will benefit the most from taking part in the Workshop:

- Representatives of Cyber Police, Security Service, Prosecutor General's Office and judiciary/judges, working and/or interested in cybercrime and electronic evidence matters;
- Representatives of the Data Protection Authority under the Ombudsman's Office;
- Representatives of National Communications Regulatory Commission;
- Internet service providers/companies' and associations' representatives (INAU, Telecom Association and others);
- Civil society organizations active on matters covered by the Workshop.

Administrative arrangements and location

The event will be conducted virtually, on Council of Europe's KUDO platform to address the needs of virtual meetings with interpretation.

Simultaneous interpretation between Ukrainian and English will be available throughout the event.

Unless specified otherwise, all times indicated in the programme correspond to Kyiv local time.

Programme

Day I - Thursday, 15 April 2021

11h00	Opening session <ul style="list-style-type: none"> • EU Delegation Ukraine • Council of Europe
11h10	Introduction: Budapest Convention on Cybercrime and its Human Rights mandate <ul style="list-style-type: none"> • Giorgi Jokhadze, Cybercrime Programme Office of the Council of Europe • Experts of the Council of Europe
11h40	Budapest Convention: Scope and application of Article 15 <ul style="list-style-type: none"> • Experts of the Council of Europe
13h00	<i>Lunch break</i>
14h00	Connection between the Budapest Convention and personal data protection safeguards <ul style="list-style-type: none"> • Experts of the Council of Europe
15h00	Retention of traffic data: balancing fight against cybercrime with personal data protection standards <ul style="list-style-type: none"> • Open discussion moderated by experts of the Council of Europe
16h00	<i>End of day I</i>

Day II - Friday, 16 April 2021

11h00	Public-private cooperation: elements of trust between law enforcement and private (Internet) industry <ul style="list-style-type: none"> • Giorgi Jokhadze, Cybercrime Programme Office of the Council of Europe • Experts of the Council of Europe
12h00	Internet service providers: Role of private industry in fighting and preventing cybercrime <ul style="list-style-type: none"> • Experts of the Council of Europe
13h00	<ul style="list-style-type: none"> • <i>Lunch break</i>
14h00	Communications regulators: Role of regulatory authorities in ensuring trust and security in cyberspace <ul style="list-style-type: none"> • Experts of the Council of Europe
15h00	Way forward for Ukraine: how can Council of Europe support long-term trust and cooperation? <ul style="list-style-type: none"> • Open discussion moderated by experts of the Council of Europe
15h50	Closing remarks <ul style="list-style-type: none"> • Council of Europe • Experts • Project counterparts
16h00	<i>End of event</i>

Contacts

Council of Europe:

Giorgi JOKHADZE
CyberEast Project Manager
Cybercrime Programme Office
Tel: +40-21-201-784
Giorgi.Jokhadze@coe.int

Cybercrime Programme Office of the
Council of Europe (C-PROC)
Bucharest, Romania
www.coe.int/cybercrime

Ukraine:

Bogdana MARTYNIUK
Attaché
Political, security and defence cooperation
Directorate General for the EU and NATO
Ministry of Foreign Affairs of Ukraine
bogdana.martyniuk@mfa.gov.ua