www.coe.int/cybercrime

Strasbourg, 18 March 2016

Cloud Evidence Group (CEG)

Invitation to an

Exchange of views with data protection organisations

Monday, 23 May 2016, 11h00 - 17h00, Room 5, Palais de l'Europe
Council of Europe, Strasbourg, France

1 Participation

The meeting is open to representatives of:

1. T-PD / Council of Europe
2. Working Party 29
3. European Data Protection Supervisor (EDPS)
4. European Commission – DG Home and DG Justice
5. European Parliament – Committee on Civil Liberties, Justice and Home Affairs (LIBE)
6. Members and Observers in the Cybercrime Convention Committee (T-CY)

The meeting will be held on 23 May 2016, 11h00 - 17h00, Room 5, Palais de l'Europe, Council of Europe, Strasbourg, France.

Representatives are required to register beforehand in order to obtain badges for access to the building.

In order to facilitate and structure discussions, interested representatives are invited to submit written contributions addressing the issues listed in this note.

Deadline for registration and written comments: **1 May 2016**.

For registration, written comments and further information please contact:

Alexandru FRUNZA,
Programme Officer
Cybercrime Division
Tel +33 390215897
Alexandru.FRUNZA@coe.int

2 Background

The Cybercrime Convention Committee (T-CY), at its 12th plenary (2-3 December 2014), established a working group to explore solutions for access for criminal justice purposes to evidence in the cloud, including through mutual legal assistance ("Cloud Evidence Group").[1]

This decision was motivated by the recognition that in the light of the proliferation of cybercrime and other offences involving electronic evidence, and in the context of technological change and uncertainty regarding jurisdiction, additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence in specific criminal investigations.[2]

The Cloud Evidence Group is to submit a report to the T-CY with options and recommendations for further action by the end of 2016.

The Cloud Evidence Group has identified the challenges faced by criminal justice authorities in obtaining transborder electronic evidence[3] and is now preparing possible solutions.[4]

In November 2015, the Cloud Evidence Group held a hearing with service providers,[5] and would now like to continue discussions with data protection organisations.

3 Objectives

The Cloud Evidence Group is seeking the views of data protection organisations with respect to the compatibility of possible options and solutions on criminal justice access to evidence in the cloud or in foreign jurisdictions with European data protection regulations.

---

[1] Document T-CY(2014)16: Transborder Access to data and jurisdiction: Options for further action by the T-CY (report of the Transborder Group adopted by the 12th Plenary of the T-CY, December 2014).

[2] The need for solutions to allow for timely access to electronic evidence in view of protecting the rights of victims is also underlined by the European Union in http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf (February 2015). The EU Agenda on Security (April 2015) notes:
"*Cyber criminality requires competent judicial authorities to rethink the way they cooperate within their jurisdiction and applicable law to ensure swifter cross-border access to evidence and information, taking into account current and future technological developments such as cloud computing and Internet of Things. Gathering electronic evidence in real time from other jurisdictions on issues like owners of IP addresses or other e-evidence, and ensuring its admissibility in court, are key issues.*"
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
The T-CY in document T-CY(2014)16
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf stated:
"The Transborder Group believes that in the absence of an agreed upon international framework with safeguards, more and more countries will take unilateral action and extend law enforcement powers to remote transborder searches either formally or informally with unclear safeguards. Such unilateral or rogue assertions of jurisdiction will not be a satisfactory solution."

[3] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b5

[4] For an informal summary of current issues and options under consideration see https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680a53c8

[5] http://www.coe.int/en/web/cybercrime/hearing

4 Issues for discussions

The meeting will focus on the following questions:

Question 1:	In December 2015, the European Union reached agreement on the substance of a new General Regulation on Data Protection and a Directive on data protection in the criminal justice sector. The Amending Protocol to the Council of Europe data protection Convention 108 is about to be finalised. What are the implications of these instruments with regard to the Budapest Convention on Cybercrime in its current form?
Question 2:	Criminal justice authorities may need to disclose personal data directly to a service provider in another jurisdiction, for example, in situations of imminent danger or other exigent circumstances. This appears to be foreseen in Article 36aa of the future EU Directive:
a)	Does it make a difference if the service provider is in an EU Member State, or in another Party to Convention 108, or in a third country?
b)	Could a Protocol to the Budapest Convention provide a legal basis for such processing? If so, what would be the elements to be foreseen?
Question 3:	Criminal justice authorities increasingly send requests for subscriber information (and sometimes also for other data) directly to service providers in other jurisdictions, and often service provider respond positively to such requests. In emergency situations, including situations of child abuse, service providers are sometimes also prepared to disclose content information:
a)	What would be the basis or reasoning under European data protection instruments and/or domestic law permitting such disclosure directly transborder in non-emergency situations?
b)	What would be the basis or reasoning under European data protection instruments and/or domestic law permitting such disclosure, including of content, directly transborder in emergency situations?
c)	Does it make a difference if the receiving criminal justice authority is in an EU M/S or adequate country or territory, or in another Party to Convention 108 or in a 3rd country?
d)	Could a Protocol to the Budapest Convention provide a legal basis for such processing? If so, what would be the elements to be foreseen?
Question 4:	Service providers receiving requests for data from criminal justice authorities in another jurisdiction may notify their customer of such request. Customer notification may harm investigations or witnesses or threaten the safety of requesting law enforcement officials. Is customer notification a requirement under data protection instruments (e.g. under Article 14 of the future General Data Protection Regulation)?