COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Strasbourg, 7 June 2016 T-CY (2016)21

Cybercrime Convention Committee (T-CY)

Cloud Evidence Group

Exchange of views with data protection organisations

Strasbourg, France, 23 May 2016

Informal summary[1]

The Cloud Evidence Working Group of the Cybercrime Convention Committee (T-CY) organised this meeting on 23 May 2016[2] to seek 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[3] with new European data protection regulations.

Representatives of the European Commission, the Secretariat of the EU Council, EUROPOL, the European Data Protection Supervisor, Working Party 29, Experts and members of the Secretariat of the Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) as well as members and observers of the T-CY participated in this exchange of views held prior to the 15th Plenary Session of the T-CY. The gathering was also addressed by Mr. Philippe De Backer, Secretary of State for Social fraud, Privacy and the North Sea, Belgium.

Following adoption by the European Union of the new data protection "package" (consisting of a General Data Protection Regulation (GDPR) and a Directive on data protection in the criminal justice sector) and the imminent finalisation of the Amending Protocol to modernise the Council of Europe's data protection "Convention 108", the meeting was timely.

Discussion focused on a set of specific questions (see appendix) regarding (1) the implications of new European data protection standards on the Budapest Convention, (2) the disclosure of personal data by a criminal justice authority to a service provider in another jurisdiction when submitting a lawful request directly within a specific criminal investigation, (3) and conversely, the disclosure of information by a service provider to a criminal justice authority in another jurisdiction in response to such a request, as well as (4) finally, the question of customer notification by service providers of such requests.

Parties to the Budapest Convention other than the USA – including in particular European States – reportedly send more than 100,000 requests per year directly to major US service providers.[4] These contain at least minimal personal information so that the providers can act. The question of disclosing data – in particular subscriber information – by service providers located or offering a

[1] This summary does not necessarily represent the views of participants in the Exchange of Views.
[2] http://www.coe.int/en/web/cybercrime/exchange-of-views
[3] For an informal summary of current issues and options under consideration see https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8
[4] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d

service in the territory of a Party to criminal justice authorities and of the legal basis for such direct "asymmetric" cooperation is therefore highly relevant.

Discussions suggest the following:

Question 1: Implications of the European Union's new data protection package and of the Council of Europe's draft Amending Protocol to Convention 108 on the Budapest Convention

Given that the Budapest Convention stipulates specific procedural powers that are subject to conditions and safeguards and that are to be implemented in the domestic law of Parties, these powers should not pose data protection concerns in principle.

The same seems to apply to the provisions on international cooperation of the Budapest Convention. This treaty represents an international legal basis for criminal justice cooperation, including the transmission of personal data within specific criminal investigations.

Some participants raised possible concerns in relation to Article 32 (transborder access to data) and the question of whether a service provider could consent to disclose data. However, others pointed at the Guidance Note on Article 32b which states that "Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32".[5]

Moreover, following earlier discussions with data protection organisations, it is understood that the concept of consent in a data protection context is not the same as consent in a criminal justice context.

Question 2: Direct disclosure of personal data by a criminal justice authority to a service provider in another jurisdiction in specific criminal investigations

To make a request on which a provider can act, a criminal justice authority must provide at least minimal personal information. For EU member States, such disclosures would fall under the new EU Directive on data protection in the criminal justice sector. If disclosed to a service provider within the European Union it would be considered a "transmission" and not a "transfer" and the general rules of the Directive apply. In principle, this should not cause problems. Among other things, such transmissions would need to have a basis in domestic law. Proper implementation of Article 18 Budapest Convention could represent such a legal basis.

For disclosures by a criminal justice authority within the EU to a service provider in a "third" country, Chapter V of the Directive applies, according to which transfers are possible under the conditions of Article 39 regarding "transfers of personal data to recipients established in third countries".

These conditions are without "prejudice to any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation".

In this connection, Article 18 Budapest Convention could represent a relevant provision and legal basis in an international agreement, in that production orders for subscriber information may be transmitted to service providers located in another jurisdiction but that are offering a service in the territory of the requesting Party.

Given that a Guidance Note on Article 18 Budapest Convention is still under negotiation within the T-CY, the consideration of whether Article 18 can represent a legal basis for the transmission of

[5] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a

personal data to a service provider in a third country as part of a production order would need to be continued.

Clarification would also be needed as to when a US service provider is considered to be located within the European Union and which rules apply for requests to such providers for different types of data by criminal justice authorities from within the EU and from "third" countries.

Question 3: Direct disclosure of subscriber information – or of content data in emergency situations – by a service provider to a criminal justice authority in another jurisdiction

Under EU data protection legislation, the disclosure of personal data by service providers to criminal justice authorities in another jurisdiction in the future falls under the General Data Protection Regulation. One of the situations enumerated in Article 6 (GDPR) must apply to make such processing lawful. Disclosure by a service provider within the EU to a criminal justice authority within the EU could be possible under data protection rules.

The question of why service providers within EU member States do not disclose data – including subscriber information – directly to criminal justice authorities in other EU member States remained without answer. Some pointed at the confidentiality requirement of the E-Privacy Directive (2002/58/EC) as a possible explanation, and at the need to distinguish more clearly between traffic data and subscriber information should the E-Privacy Directive be revised.[6]

The disclosure of personal data by a service provider within the EU to a criminal justice authority in a third country seems to be possible by way of an adequacy decision (Article 45 GDPR), appropriate safeguards (Article 46) or derogations for specific situations (Article 49). These appear to be exceptions to Article 48 (Transfers or disclosures not authorized by Union Law).

Article 48 furthermore refers to international agreements as the basis for the transfer or disclosure of data to an authority in a third country. In this connection, Article 18 Budapest Convention could represent such a basis in that service providers offering a service in the territory of Party without being legally or physically present may respond to production orders for subscriber information.

As indicated above, given that a Guidance Note on Article 18 is still under negotiation within the T-CY, the consideration of whether Article 18 can represent a legal basis for the transmission of subscriber information by a service provider to a criminal justice authority in response to a production order would need to be continued.

Clarification would also be needed as to when a US service provider is considered to be located within the European Union and which rules apply for responses to requests for different types of data by criminal justice authorities from within the EU and from "third" countries

Question 4: Customer notification by service providers

The practice of US service providers to notify customers of lawful requests for data is of major concern to criminal justice authorities as it may compromise investigations and create risks to investigators, prosecutors and others.

It would seem that such notification is a decision of individual service providers and is not a requirement under European data protection rules. Confidentiality requirements may be imposed under domestic law, and appear to be foreseen in the criminal procedure laws of most European countries.

[6] https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data

Conclusion

The exchange of views was not intended to lead to specific conclusions and definite answers to the questions raised.

It provided participants with a better understanding of

- The Budapest Convention as an international legal basis for criminal justice cooperation between the Parties to this treaty, including the transmission of personal data within specific criminal investigations;
- The compatibility of data protection principles with the Budapest Convention in its present form;
- The potential of Article 18 as a legal basis for the cooperation between criminal justice authorities and service providers with respect to production orders for subscriber information;
- The need to consider data protection principles should an additional Protocol to the Budapest Convention be prepared.

Appendix: Questions discussed

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 39 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?
NEW c)	Could Article 18 Budapest Convention on Production Orders serve as the legal basis for such processing?
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?
NEW e)	Could Article 18 Budapest Convention on Production Orders serve as the legal basis for such processing?
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)?

Appendix: Agenda

11h00	Opening ▪ Jan Kleijssen, Director for Information Society and Action against Crime, DG1, Council of Europe ▪ Cristina Schulman, Vice-chair, T-CY, Ministry of Justice, Romania
11h15	Introductory presentations ▪ Summary of proposals under consideration by the Cloud Evidence Group[7] (Alexander Seger, Executive Secretary T-CY, Council of Europe) ▪ Summary of EU data protection package (Regulation and Directive)[8] (Juraj Sajfert, DG JUST, European Commission) ▪ Summary of modernization proposals related to Council of Europe Convention 108[9] and review of Recommendation R(1987)15[10] (Sophie Kwasny, Secretary, T-PD, Council of Europe)
12h00	Discussion of Question 1: Implications of the EU DP package and amendments to Convention 108 for Budapest Convention
13h00	Discussion of Question 2: Disclosure of personal data by criminal justice authorities to service providers in foreign jurisdictions Including new question 2 c) Could Article 18 Budapest Convention on Production Orders serve as the legal basis for such processing?
13h30-14h30	Coffee break
14h30	Intervention by Philippe De Backer, Secretary of State for Social fraud, Privacy and the North Sea, Belgium
14h45	Discussion of question 3: Disclosure of personal data by service providers to LEA in foreign jurisdictions Including new question 3 e) Could Article 18 Budapest Convention on Production Orders serve as the legal basis for such processing?
16h00	Discussion of question 4: Customer notification
16h45	Conclusions

[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016864b77c

[8] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

[9] http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2016)01_E.pdf

[10] http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf