COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 29 May 2019

T-PD(2019)3

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Inclusion of data protection safeguards relating to law enforcement trans-border access to data in the Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185)

Prof. Dr. Gert Vermeulen

Senior Full Professor of (European and international) Criminal Law and Data Protection Law, Director of the Institute for International Research on Criminal Policy (IRCP) and Director of the Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement and Surveillance (PIXLES) at Ghent University, Belgium

Directorate General Human Rights and Rule of Law

1. Introduction

In the Fall 2017, the Cybercrime Convention Committee (T-CY) embarked with its work on the drafting of a Second Additional Protocol to the Cybercrime Convention, in view of rendering traditional MLA under the Convention more effective (including through emergency MLA procedures) and introducing the possibility of *direct cooperation* with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests. Such direct law enforcement trans-border access to data poses new challenges, implying that data protection safeguards inserted in the Protocol must *also* adequately cover the scenario of direct cooperation, in addition to traditional MLA scenarios.

In accordance with the ToRs for the preparation of the Protocol, the T-CY Protocol Drafting Plenary, meeting back-to-back with the regular T-CY Plenary, is assisted by a T-CY Protocol Drafting Group, meeting back-to-back with the T-CY Bureau. The Consultative Committee of Convention 108 (T-PD) has observer status in the meetings of the Protocol Drafting Plenary, but not in those of the Protocol Drafting Group. Combined with the scarce public release of information by T-CY, T-PD is largely left in the dark. Hence, the 38th Plenary can only have an exchange of views based solely on this report on the issues at stake regarding the ongoing Protocol drafting activities. Only following release of actual draft Protocol provisions, T-PD will be enabled to scrutinise them from a data protection perspective and adopt a definite and formal position.

For the time being, it bears relevance to recap that, leading up to the 2018 Octopus Conference, the 36th T-PD Plenary, held in June 2018, has adopted Provisional Answers to the Discussion paper for the Octopus Conference. In addition, the available preparatory documents for the 38th T-PD Plenary are a T-CY discussion paper on conditions for obtaining subscriber information in relation to dynamic versus static IP addresses and a T-CY discussion note for the consultation with data protection experts, held in Strasbourg on 26 November 2018, in which both the T-PD Secretariat and the T-PD expert participated. The above documents have all been joined with the agenda for the 38th T-PD Plenary.

2. Direct cooperation: Voluntary disclosure of subscriber data+

Based on informal information received during the expert consultation meeting of November 2018 (supra), it seems that the envisaged Protocol provision on direct cooperation between competent (law enforcement) authorities and providers would likely:

- be voluntary in nature, i.e. not compelling for service providers, whilst it will be necessary to create sufficient legal certainty for the latter. This would prompt the necessity of making sure providers can lawfully provide data to requesting competent authorities;

- be limited to only subscriber data+, i.e. inclusive of both static and dynamic IP addresses, excluding (other) traffic data or content data. In principle, this scoping *ratione informationis* could be supported, thus recognising that access to both static and dynamic IP addresses may be required in order to establish the information as meant in Article 18.3 of the Budapest Convention. In line with its provisional answers to the discussion paper for last year's Octopus Conference, T-PD would like to scrutinise the envisaged definition (in the Protocol or the explanatory memorandum to it) of subscriber data+, so as to make sure it is not inclusive of any (other) traffic data or content data. T-PD's would equally like to scrutinize any corresponding adaptation (for the sake of the Protocol) of the definition of 'traffic data' (currently defined in Article 1.d of

the Budapest Convention as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"), so as to make sure that all traffic data which are not necessary to establish the information as meant in Article 18.3 of the Budapest Convention (such as static or dynamic IP addresses) remain properly labelled as 'traffic data', falling outside of the scope of the envisaged direct cooperation mechanism.

3. Two-directional data protection, including for asymmetrical transfers, optional or mandatory?

a. The importance of making sure, at least, that data protection conditions and safeguards in the Protocol may apply in two directions has to be underlined, since the receiving entity may be:

- either a competent authority:
  - in the case of traditional MLA: both the requesting and requested authority being the recipient of personal data, i.e. of the personal data provided in the request or of the personal data transferred as a result of the execution of a request;
  - in the case of direct, asymmetrical transfers: the requesting authority being the recipient of personal data transferred by a private data controller (service provider);
- or a private data controller (service provider), which, in the case of direct, asymmetrical transfers is the recipient of personal data provided in the request.

b. As outlined in the provisional answers to the discussion paper for last year's Octopus Conference, the most straightforward, sustainable and widely acceptable way to guarantee an appropriate level of data protection under the Protocol would be to require accession by the Protocol Parties to Convention 108+. As a result, adequate data protection would be generically guaranteed by all Parties to the Protocol and indirectly become a default standard also for the application amongst them of the Budapest Convention itself.

c. If not feasible, the key questions seem to be the following:

- whether to phrase the data protection conditions and safeguards in the protocol as mandatory, i.e. applicable to all Parties, or as optional conditions, i.e. leaving it to the competent authority or data controller of a Party to make the transfer of personal data conditional upon an appropriate level of data protection:

  To the extent that the option to require accession by the Protocol Parties to Convention 108+ (supra) does not prove feasible, it is suggested to take Article 26 (pertaining to "Data protection") of the Second Additional Protocol to the Convention on MLA in criminal matters (ETS 182) as a point of departure, thus ensuring consistency with at least the Council of Europe's data protection acquis in the context of judicial cooperation in criminal matters. This would imply an optional regime, comparable with that of Article 26.3, 2nd indent ("Any Party may refuse to transfer personal data obtained as a result of the execution of a request made under the Convention or any of its Protocols where […] the Party to which the data should be transferred is not bound by [Convention 108], unless the latter Party undertakes to afford such protection to the data as is required by the former Party"), but rephrased so as to enable tow-directional applicability, including for asymmetrical

transfers (infra).

- in the latter (optional) scenario: how to enable and ensure (and if necessary: enforce) compliance by private data controllers (service providers) with the data protection conditions and safeguards in the Protocol, given that they cannot not themselves be directly bound by the Protocol, being a public international law instrument:

  It is suggested to stipulate in the Protocol that if a data controller or competent authority of a Party requires an appropriate level of data protection in the receiving Party, such condition shall be considered to be met if "the receiving competent authority or data controller of the latter Party **undertakes** to process the personal data transferred subject to the conditions and safeguards under the domestic law of the former Party [i.e. the **Party from where personal data would be transferred**], including obligations the latter has undertaken under [Convention 108 and its Protocol] and/or other applicable bilateral or international data protection agreements guaranteeing the protection of individuals by the implementation of at least the following principles [list as included infra, under 4]";

  In doing so, as a minimum requirement, also mentioned in the provisional answers to the discussion paper for last year's Octopus Conference a Protocol regime for disclosure of subscriber data should allow for the combined data protection obligations of at least the Party of the requesting competent authority and the Party where the service provider [or executing competent authority] is located.

  Since an undertaking as above lacks the "legally-binding and enforceable" character of safeguards as required under Article 14.3.b of Convention 108+, it is further suggested to introduce an additional obligation in the Protocol for Parties to stipulate in their domestic legislation that violations of such undertaking by a receiving competent authority or data controller in their territory may give rise to all judicial and non-judicial sanctions and remedies available under their laws.

- whether the application of data protection conditions and safeguards in the Protocol should be limited to cooperation under the Protocol or also extend to MLA under the Budapest Convention itself:

  As it may be difficult for Parties to the Budapest Convention to accept generic or optional data protection restrictions on the level of the Budapest Convention itself, Parties could choose to confine their commitment by limiting the application of data protection conditions and safeguards to data transfers in the context of requests and the execution thereof under only the Protocol, even where this would lead to incoherence in the (possible) application of data protection rules, depending on whether MLA or cooperation is happening under the mother Convention or under the Protocol.

- for which use purposes transferred personal data can be used by the receiving competent authority or private data controller (service provider):

  It is suggested to stay close to the provisions of Article 26 of ETS 185 (supra), amending them *mutatis mutandis* and extending them to also cover use limitations upon a private data controller (service provider) to which a request is transferred. This could translate in three provisions, in which it is stipulated respectively that:

  1. [*mutatis mutandis* adaptation of Article 26.1 ETS 185] personal data transferred by a competent authority or data controller of a Party as a result of the execution

of a request made under the Protocol by a competent authority of the receiving Party, may be used by the latter only:

a. for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence within the scope of articles 14.2 and 25.1 of the Budapest Convention;
b. for other judicial and administrative proceedings directly related to the proceedings mentioned under (a);
c. for preventing an immediate and serious threat to public security;

2. [*mutatis mutandis* adaptation of Article 26.2 ETS 185] such data may however be used by the competent authority for any other purpose if prior consent to that effect is given by either the Party from which the data had been transferred, or the data subject. In principle, from a narrow data protection perspective, the consent of the data subject ought to be avoided as a ground for data processing in the context of judicial and law enforcement cooperation in criminal matters. However, it should be stressed that the possibility of reliance on the consent of the person concerned is formally part of the contemporary acquis of MLA in criminal matters, both at Council of Europe (Article 26.2 ETS 185) and EU level (Article 23.1, under (d) of the EU MLA Convention of 29 May 2000, which was not abrogated from by the European Investigation Order Directive). It is actually the case that the possibility to rely on consent of the person concerned functions here as an extra guarantee for that person in the context of the so called specialty principle (which is the traditional correlative of the purpose limitation principle in data protection law). The specialty principle traditionally has a trust function: the requesting sate or authority ought not to use data for other purposes than the initial purposes, so as not to betray the trust put in it by the executing state or authority in sending the data concerned for those initial purposes. Since the requested state or authority might have refused cooperation or data transfer for other than the initial purposes, the specialty principle stipulates that additional consent of the executing state or authority must be sought in case of intended use beyond the initial purposes (comparable with the data owner principle in data protection law). It was only with the above 'new' generation of European MLA instruments that the person concerned was also given a possible say in further use of his or her personal data. It would be pitiful to rewind the clock, and to leave it only to the Party from which data have been transferred to decide on use of an individual's personal data beyond the initial purposes. Hence, to allow for consent of the data subject as a basis for further use could be supported;

3. [extension to cover use limitations for service providers] the request received and the information it contains can only be used by the receiving data controller for the purpose of the execution of a request made under this Protocol.

4. Substantive data protection conditions, safeguards or principles

To the extent that the option to require accession by the Protocol Parties to Convention 108+ (supra, under 3) does not prove feasible, it is of an utmost importance that, as a minimum, the Protocol allows data controllers or competent authorities to require, as a precondition before transferring any personal data, the receiving competent authority or data controller to undertake to process the personal data transferred subject to the conditions and safeguards under the domestic law of the Party from where personal data would be transferred, guaranteeing the protection of individuals by the implementation of at least the following principles [allowing flexibility as to possible re-ordering, clustering etc.]:

a. purpose legitimacy, purpose specificity and purpose limitation;
b. lawfulness;
c. fairness and transparency;
d. necessity for and proportionality to the legitimate purpose pursued;
e. non-excessive data processing and data minimisation;
f. adequacy, relevance and accuracy of data;
g. data retention limitation;
h. accountability of controllers and processors;
i. logging, data security and data breach notification duty;
j. specific, additional safeguards for special categories of sensitive data;
k. lawful use of exceptions and derogations;
l. enforceable data subjects' rights and effective administrative or judicial redress;
m. appropriate protection in (onward) data transfers;
n. free, specific and explicit consent where consent of the data subject is the legal basis*
o. effective independent oversight

* Supra, under 3, 4th indent, 2.

5. Derogations

It is to be considered that derogations are possible, when in line with Article 11 and 14.4 of Convention 108+. In any event, structural or systemic reliance on derogations, as a standardised means to allow for direct, asymmetrical transfers, must be plainly excluded.