Provisional Answers from the Committee of Convention 108 to the Discussion paper for Octopus Conference, 11-13 July 2018

a. **What are the implications of these developments for work on the Protocol?**

On 17 April 2018, the European Commission published the e-Evidence Initiative, aimed at establishing a new framework for European Union Member States to access content data and metadata across national borders, which needs to be taken into account considering its possible impact on the drafting of the second additional Protocol to the Budapest Convention and its interplay with the international data protection regime that Convention 108+ (Convention 108 as modernised by the amending Protocol CETS n°223) provides[1].

The Committee of Convention 108 furthermore notes that the US CLOUD Act (enacted one month before the e-Evidence Initiative of the European Union) makes reference to "applicable international human rights obligations and commitments or demonstrates respect for international universal human rights", leaving the room for Convention 108+ to get recognised as an important reference in this matter, in addition to possible further guarantees that the US will seek.

In terms of possible implications, also the following issues need to be addressed:

- the establishment by the Protocol of a new regime, allowing and regulating the conditions for voluntary disclosure of data by service providers, should by no means legitimise, induce or promote national or regional data retention schemes or practices;

- reassurance that any different regime and safeguards for differentiating among types of personal data (subscriber information, metadata, content) does not lead to lowering of standards of protection of the right to privacy and of personal data;

- the subsequent use and onwards transfer of data acquired through such regime, in terms of purpose limitation and data protection standards of recipients of onward transfers, must be strictly regulated;

- any trans-border flow of data under such regime should be conditional to an appropriate level of data protection as foreseen by the Convention 108+;

- implications due to the difference in the level of human rights protection and rule of law guarantees in national or regional regimes.

b. Would civil society, data protection or industry organisations have any comments on such proposals?

The Committee of Convention 108 wishes to provide comments on all proposals having privacy and data protection relevance and to offer its expertise in putting in place the necessary privacy and data protection guarantees, notably with regard to this round of negotiations in relation with emergency mutual legal assistance and cooperation in joint investigations teams.

c. Can current practices by US providers be generalised in a Protocol?

[1] The Committee of Convention 108 took note of the Statement of the Article 29 Working Party of 29 November 2017 on "*Data protection and privacy aspects of cross-border access to electronic evidence*"

Only if after careful assessment the necessity for such practices is proven and if they contain all the necessary privacy and data protection guarantees, preferably by the binding application of the provisions of Convention 108+.

i. With regard to subscriber information?

Only if the level of data protection as foreseen by Convention 108+ is guaranteed and if no data retention schemes or "back-door" measures are envisaged. The Committee of Convention 108, bearing in mind the risks the re-opening of the definition of subscriber information could represent for the synergies, well-functioning of different cooperation regimes and for the level of protection they afford, would also like to scrutinise the envisaged definition of "subscriber information", especially to see to it that it is non-inclusive of any "traffic" or "content" data (current acquis of Article 18.3 of the Budapest Convention) nor of any "transactional" data or "content" data (in the sense of the definitions used in the EU e-Evidence proposals, which put subscriber data and access data on the same footing, whilst also allowing for a certain degree of cross-over between transactional and access data, which the Committee of Convention 108 questions). The Committee of Convention 108 noted with interest the European Court of Human Rights case Benedik v. Slovenia (application no. 62357/14) and its possible implications on the definition of "subscriber information" and on the safeguards required before accessing such information. Its assessment will also include clarifying if a simplified regime for accessing metadata is necessary and proportionate and whether it does not imply the lowering of the protection of individuals against arbitrary and/or abusive intrusion.

Question (linked to h.i, *infra*): does the Committee need to explicitly address the issue of access data (new category in the EU proposals), taking position as to whether it either or not supports a possible widening of subscriber data to access data?

ii. For disclosure of other data in emergency situations?

No. In data protection terms it is already possible with the information of the competent authority and ex-post validation/subpoena/court order.

d. What rules/regulations or other factors prevent providers from voluntarily disclosing subscriber information to criminal justice authorities from other jurisdictions?

This question needs to be turned around. The issue is not to know whether there are factors preventing providers to voluntarily disclose subscriber information, but to provide the conditions under which such disclosure is legitimate. Through its international open instruments, notably the Convention on Cybercrime and the Convention 108+, the Council of Europe can provide a widely accepted international legal framework for law enforcement cooperation in the field of fight against cybercrime while equally ensuring an appropriate level of protection of personal data as is necessary for such cooperation. The Committee of Convention 108 supports the organisation in promoting the two instruments and calls for Parties to do the same in their relation with countries around the world. In order, however, to directly access personal data held by private companies based in non-Convention 108+ jurisdictions, a new program would need to be set up, based on voluntary participation of accredited private and public partners and containing the safeguards and guarantees foreseen by Convention 108+, in particular the easily accessible procedures to exercise data subjects' rights towards private entities and participating public authorities as well as the effective oversight of such a program.

For systematic, large-volume, frequent disclosures, one would have to develop a new scheme or to require as a precondition for the use of such regime the application of Convention 108+. The convention in its integrity ensures the appropriate level of protection in its various dimensions (starting from the legitimacy of the data processing and the quality of data as laid down in Chapter II, the set up and functioning of a supervisory authority, etc.), which is required for such systematic transfers.

On an ad hoc, case-by-case basis, voluntary disclosure is already possible under Convention 108+:

Personal data can be processed for a pre-determined, specific and legitimate purpose (~ scope of the Budapest Convention and the list of specific crimes in appendix) and on a valid legal basis (for the time being, art 18.) So that, if the request is compliant with the provisions of the Budapest Convention and is detailed and specific enough, respects the procedures foreseen for data requested, respects Convention 108+ requirements (such as necessary, proportionality, purpose bound data processing, etc.), it may be considered as lawful.

The basic requirements for actual transfer of data are the same: legitimate purpose, valid legal ground (necessity, proportionality, etc.) and an appropriate level of data protection if data is sent to a non-Convention 108+ party. To guarantee this appropriate level of data protection one has different options: national law or ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing (Article 14.3.b of Convention 108+).

Moreover, even where there are no assurances for an appropriate level of data protection, transfer to a non-Convention 108+ country will still be possible based on either consent (Article 14.4.a of Convention 108+)[2] or specific interests of the data subject; prevailing legitimate interests of the data controller, in particular important public interests given that those are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society, or where it constitutes a necessary and proportionate measure in a democratic society for freedom of expression (Article 14.4.b-d of Convention 108+).

To guarantee the appropriate level of data protection, the most straightforward, sustainable and widely acceptable way would be to require accession to Convention 108+. If the envisaged new regime will not meet the criteria set by Convention 108+, it will pose problems for at least 53 countries (Cabo Verde will become the 52nd Party and Mexico the 53rd Party as of 1 October 2018), some of them also Parties to the Budapest Convention.

e. Questions: Connecting factors: in what circumstances may service providers be subject to a domestic production order?

i. "Real and substantial connection" to a Party?
ii. Offering a service in the territory of a Party?
iii. Or otherwise "established" in the Party?

If a new regime is created and it respects the criteria cited above: all of the three, provided that the production order is issued by the domestic competent authorities in a Convention 108+ state. Otherwise a specific program should be set up with proper scrutiny of the participating states and data controllers, and which will guarantee the appropriate level of protection as described by Convention 108+.

f. Questions regarding data protection and other safeguards for voluntary disclosure:

i. Which data protection and other safeguards apply:

- **Legal framework of country of service provider?**
- **Legal framework of country of requesting criminal justice authority?**
- **Legal framework of country where data is stored?**

[2] Which cannot be seen as a valid legal basis in criminal investigations for transfer of personal data as in no cases it can be freely given. Particular situations however could exist where the data subject consents to the transfer of her/his personal data in her/his own interests.

- **Legal framework of country of data subject? What if several countries are involved?**

Notwithstanding the fact that data storage constitutes data processing (so that, obviously, relevant data protection standards apply to it), in times of 'loss of location' data location seems the least relevant criterion to govern the data protection and procedural rights safeguards that should apply to a voluntary disclosure regime.

As a minimum requirement, the Committee of Convention 108 suggests to work with the combined data protection and procedural rights obligations (double *locus* regime) of at least:

- as far as the new regime only envisages disclosure of *subscriber data*: the country of the requesting competent authority and the country where the service provider is located;

- in case where a new regime would also pertain to *traffic or content data* (which the Committee of Convention 108 does not support *(supra)*): the country of the requesting competent authority and the country where the data subject was present whilst using the targeted service.

ii. On the part of the service provider as the data controller under European legal frameworks:

- **What conditions precisely have to be met to permit disclosure and which are the applicable provisions of the GDPR or Convention 108?**

  The Committee of Convention 108 underlines that the following provisions of Convention 108+ are applicable:

  - Legitimate purpose (art 5.1)
  - Valid legal basis (art 5.2)
  - Principle of necessity, proportionality, purpose bound data processing, data which are processed shall be adequate, relevant, not excessive, accurate, up to date, preserved in a form which permits identification for no longer than is necessary (art 5.3, 5.4.)
  - For the processing of special categories of data complementary safeguards have to be put in place (art 6)
  - Data processing shall be secure (art 7)
  - Transparency obligations (art 8)
  - The exercise of the data subject rights have to be ensured (art 9)
  - Additional obligations imply accountability, data protection impact assessment, privacy by design and by default (art 10)
  - Data shall only be transferred abroad where the appropriate level of protection is guaranteed (art 14)
  - Data processing shall be subject to independent external oversight (art 15)

- **What would be considered a sufficient legal basis under the GDPR or Convention 108?**

  For Parties to Convention 108+: international law and national law (having the criteria established by the ECtHR: accessible, understandable, foreseeable, etc.)

- **[What constitutes a "legitimate interest" (Article 6.1.(f) GDPR) of a service provider in this context?]**

- **What are requirements for disclosure/transfers of subscriber information to "third countries"?**

Supra: appropriate level of protection.

- **[Would the derogations of Article 49 GDPR – such as Article 49.1 (f) – apply if data is required in a specific criminal investigation?]**

- **[What is the meaning of Article 48 GDPR?]**

iii. In the requesting country (that is, in the country of destination of data):

- **What conditions precisely have to be met to permit transfer to this country and which are the applicable provisions of the GDPR or Convention 108?**

  From a Convention 108+ perspective, idem as above.

iv. What data protection and other safeguards must be met for the voluntary disclosure of data in other jurisdictions?

Idem as above, plus:

- the setup of a program based on voluntary participation of accredited partners containing the safeguards and guarantees foreseen by Convention 108+, in particular the easily accessible procedures to exercise data subject's rights towards private entities and participating public authorities as well as effective oversight of such a program;

g. Can current practices by US-providers be generalised in a Protocol?

Only if additional agreements, accreditation, monitoring, review, etc. are put in place.

h. Could such a mandatory regime be envisaged for non-EU countries?

i. For what type of data? Subscriber information only?
ii. What limitations and connecting factors?
iii. Role of competent authorities in requested country?
iv. Enforcement in case of non-compliance with order?
v. Safeguards and data protection requirements?

No, the Council of Europe is not an internal market as the European Union.

In addition, in relation to point i: only without additional conditions for subscriber information in the sense of Article 18.3 of the Budapest Convention (in e-Evidence Initiative : subscriber and access data), i.e. not for traffic or content data (in e-Evidence Initiative: not for transactional or content data). For traffic or content data (e-Evidence Initiative: transactional or content data), higher, additional standards would need to be in place, such as a judge or court order, offence thresholds, external oversight, revision, stricter data retention periods, etc.

i. What may be relevant factors to determine jurisdiction to enforce (location of data or equipment in the territory of a State, and/or access by a person in the territory of a State who has "possession or control" of data)?

Supra.

j. What is "trans-border"?

A transfer which goes across jurisdictions.

k. Is further clarification needed on the scope of Article 32?

To the extent that any new regime envisages linking in with Article 32 of the Budapest Convention: yes, definitely.

l. What other scenarios could be envisaged?

If any, the Committee of Convention 108 would like to scrutinise them and check the conditions and safeguards from a data protection perspective.