- We would like to thank the Presidency for keeping the discussions going and the Commission for their comprehensive non-paper.
- Thus far, Finland does not have an official position on a potential new EU initiative on data retention and its most suitable form. However, we would like to make the following preliminary remarks.
- Our approach has been that data retention can still be legislated at national level as long as legitimate objectives as referred to in Directive 2002/58/EC are pursued, the retention is not general and indiscriminate, it is strictly necessary and there are adequate safeguards in place.
- While common rules have their advantages, they can have drawbacks too. The situations vary in Member States, and their authorities might have different needs. Member States need at least some margin of appreciation in deciding on how to target retained data and for which purposes the data can be accessed. As stated before, e.g. defining the concept of "serious crime" should be left to Member States. Therefore, the possibility of no intervention or a non-legislative intervention should not be excluded.
- Furthermore, given the recent Court cases and the fact that the discussions on this topic have lasted quite some time already, interinstitutional negotiations on a legislative proposal would presumably be quite difficult or inconclusive, or there can be a risk that a possible outcome of these negotiations quickly contradicts the Court's assessment. If e.g. in the approach 3(a) the proposal would only codify the Court's ruling, the benefit of all that work could be quite limited. In addition, the Court could still develop or even change its previous position in its forthcoming cases which could further complicate assessing best possible options to legislate at this point.
- Regarding targeted retention (3b), using only categories of persons or geographical areas as a criterion is difficult in practice and legally. We do not see how it is possible to use them as criteria for targeted retention without them being discriminatory in practice - a precondition for the use of such criteria set out by the Court too. Thus, such criteria should not be exclusive and there is a need to be able to use other targeting criteria as well.
- The "quick freeze" (3c) provision can be one tool but it might not be enough. To our knowledge, some telecom companies in Finland will delete communication data after a month or so. In many cases that timeframe is too short for authorities' needs. In addition, the expedited retention of traffic and location data does not, by any means, replace or complement a data retention regime where data is stored for future use of the law enforcement and the judiciary without a concrete or a direct link to an actual offence or a criminal act at the time when the data is initially retained as opposed to a mechanism for the expedited preservation of traffic and location data that requires, as a prerequisite for undertaking such a preservation a concrete link to offences or acts that have already been established or reasonably suspected.
- Regarding "civil identity data" (3e), it is somewhat unclear what the concept as used by the Court exactly means or does it indeed just mean "subscriber data" as the Commission points out.
- Finally, we would like to stress that be it EU-level legislation or national law, the data retention regime must be in line with the Human Rights Convention and with the Charter of Fundamental Rights. The latter has been quite extensively interpreted by the Court of Justice. The Court's jurisprudence is something that must be carefully evaluated and taken into account.

Policy approach 1: no EU initiative

Do Member States see merits or drawbacks in maintaining a national approach to data retention legislative measures?

Policy approach 2: Non-regulatory initiative on data retention (a guidance document)

Question: Do Member States consider this a viable way forward?

Policy approach 3: regulatory initiative on data retention

Could Member States consider a 'mixed' approach of both national and EU measures? If so, what aspects should be regulated at which level (EU or national)?

Approach 3(a): generalised retention of traffic and location data for national security purposes

In light of the delineation of national and EU competences, what are Member States' views on a legislative initiative that would harmonise certain criteria relating to the retention of traffic and location data and related access conditions for national security purposes, for situations that involve private actors (for storage, transmission and providing access to data to relevant competent authorities)?

Approach 3(b): targeted data retention of traffic and location data for serious crime and serious threats to public security (and, a fortiori, safeguarding national security)

What are the legal challenges for Member States and the technical challenges for providers to comply with a targeted retention obligation and how could they be overcome? Please be as specific and concrete as possible in your responses.

What is the 'objective evidence' (in the case of persons) and what are the 'objective and non-discriminatory factors' (in the case of geographical areas) or other objective criteria that Member States could consider in drawing up a targeted retention framework?

Do Member States consider there is merit in revisiting the 'data matrix' exercise initiated by Europol in 2018 to try to find ways to devise a targeted retention system that fulfils the Court's requirements?

Do Member States consider there is merit in devising a targeted retention system by developing criteria to limit the means of communication or the number or type of electronic communications service providers subject to retention obligations (e.g. based on size, geographical coverage, number of subscribers, cross-border presence)?

Can Member States share their views of what serious threats to public security entails?

Approach 3(c): expedited retention (quick-freeze) of traffic and location data for serious crime and the safeguarding of national security

Given that a "quick freeze" provision can apply only if there is metadata available to "freeze", can Member States share any experience relating to the normal period of availability of metadata, absent a general retention obligation? Can Member States point to any ideas stemming from that experience that may be helpful in this context?

Can Member States share any experience relating to the use of expedited retention in their current legislation?

Which options do Member States see for operationalising this mechanism to meet its objective to support investigations into serious crime and protection of national security?

Approach 3(d): generalised retention of IP addresses assigned to the source of an Internet connection for serious crime and serious threats to public security

Do Member States see the benefits of this approach? Do they see any drawbacks in this approach e.g. that the IP address of the destination of a communication is not retained? Is there a lawful way to overcome this limitation?

Are there other technical identifiers that could, in line with the jurisprudence, be captured in such legislation for example time stamps and source-port numbers to allow for identification of individuals where IP addresses are shared across multiple users, as may be the case e.g. in mobile communications?

What cybercrimes are not currently covered by the notion of 'serious crime' in Member States' legislation?

Approach 3(e): generalised retention of civil identity data to fight crime and public security threats in general

Is retention of 'civil identity data' effective to fight crimes?

What specific elements should be included in this data category?