Council of the European Union
General Secretariat

Brussels, 29 January 2019

WK 870/2019 INIT

LIMITE

COPEN
CYBER
DAPIX
ENFOPOL
JAI

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Delegations
Subject:	Outline of key political messages on improving retention of data for the purpose of fighting crime and terrorism effectively

In order to progress the discussions on data retention for the purpose of effectively fighting crime and terrorism, the Presidency would like to examine with delegations their views on the way forward and more specifically on the possible preparation of Council conclusions on data retention to be submitted for adoption by the Justice and Home Affairs Council on 6/7 June 2019. These conclusions would contribute to moving from the current reflection stage into a stage of examination and assessment of the various options for addressing the challenges stemming from the lack of a general legal framework at EU level.

With a view to drawing up a first draft of such Council conclusions on data retention, the Presidency would like to present to delegations an outline of key political messages which is set out in ANNEX to this document.

The Presidency invites delegations to give their comments on the outline either orally in the DAPIX Friends of Presidency- Data retention Working Party that will take place on 4 February 2019 and/or in writing.

ANNEX

Outline of key political messages on improving retention of data for the purpose of fighting crime and terrorism effectively

1. Indication of the current situation.

1.1. In the digital age law enforcement and judicial authorities as well as intelligence services rely heavily on data to successfully investigate criminal and/or terrorist activities.

1.2. Law enforcement, judicial and other competent authorities consider that the data normally retained by telecommunications operators and service providers for business purposes are not enough to ensure that they have the necessary information available to conduct their investigations of crime and terrorism effectively. Therefore, it has been considered necessary to impose additional data retention obligations on those providers to meet law enforcement operational needs. However, such retention of data could infringe upon individual fundamental rights, in particular the rights to privacy and protection of personal data.

1.3 The rulings of the European Court of Justice in the cases *Digital Rights Ireland*[1] and *Tele 2*[2] set out the criteria for the lawful retention of data and access thereof.

1.4. In this context, Member States expressed their view[3] that the findings of the European Court of Justice in *Digital Rights Ireland* and *Tele 2* do not apply to subscriber data, but only to traffic and location data.

1.5. [The existence of different national legal regimes for data retention may be counter-productive for cooperation and information exchange between competent authorities.]

1 C-293/12
2 C-203/15
3 See 14319/18.

2. Relevant events to be taken into consideration

2.1. The conclusions of the European Council of 18 October 2018 that call for measures to provide Member States' law enforcement authorities and Europol with adequate resources to face new challenges posed by technological developments and the evolving security threat landscape, including through pooling of equipment, enhanced partnerships with the private sector, interagency cooperation and improved access to data[4].

2.2 The common reflection process launched by the Council on data retention for the purpose of prevention and prosecution of crime and terrorism assisted Member States analysing the requirements of the relevant case-law of the Court of Justice of the EU and in exploring possible options for ensuring the availability of data needed to fight crime and terrorism effectively in light of the case-law of the Court of Justice.

2.3. The exchange of views in the Justice and Home Affairs Council on 6/7 December 2018. In this Council meeting, the Austrian Presidency informed Ministers about the state of play of this reflection process. In reaction, several Ministers called upon the Commission to conduct a comprehensive study on the possible solutions for retaining data, including a legislative initiative one, taking into account the development of national and EU case law.

2.4. The relevant case law at national and EU level, in particular the most recent requests for a preliminary ruling by the Constitutional Court in Belgium[5] and by the *Conseil d'Etat* in France[6] to the European Court of Justice.

---

4 EUCO 13/18

5 C-520/18. The request for a preliminary ruling by the Belgian Constitutional court concerns the questions whether a general data retention scheme would be justified in case of (i) a broader purpose than fighting serious crime (such as guaranteeing national security and defence of the territory and (ii) fulfilling the positive obligations as set out in Articles 4 - 8 of the Charter (right to life and freedom).

6 Case 511/18. One of the requests for a preliminary ruling of the French *Conseil d'Etat* concerns the legal framework for data retention for criminal investigations whereby the *Conseil d'Etat* poses a similar question as the Belgian Constitutional court, namely whether a general retention of data can be justified in light of the right to security. Case 512/18 concerns the legal framework for data retention for intelligence services. Similar to the UK case (C-623/17), the *Conseil d'Etat* asks the European Court of Justice whether the data retention regime is justified given the existing terrorist threat.

2.5. The report of the Special Committee on Terrorism of the European Parliament which notes that the necessity of an appropriate data retention regime was consistently raised during the work of the Committee and that the rapporteurs believe it is necessary to provide for an EU regime on data retention, in line with the requirements stemming from the case-law of the Court of Justice of the EU, while taking into account the needs of the competent authorities and the specificities of the counter-terrorism field.

2.6. The currently applicable ePrivacy Directive[7], the reformed legislative framework of the European Union, in particular the General Data Protection Regulation[8] and the Law Enforcement Directive[9], as well as the ongoing negotiations on the Commission proposal for a new ePrivacy Regulation[10].

3. Suggested way forward

3.1. The use of investigative measures should be guided by the protection of fundamental rights and freedoms and the principles of purpose limitation, necessity and proportionality.

3.2. Legislative reforms at national or European level, including the new e-Privacy Regulation, should not prevent future developments as regards retention of data.

3.3. Council should continue the work in the DAPIX Friends of Presidency Working Party on data retention.

3.4. The Council invites the Commission to take the appropriate steps to address the needs of competent authorities to have certain data available with a view to fighting crime and terrorism effectively.

3.5. At a first stage, such steps could include a number of targeted consultations with relevant stakeholders to complement the work being carried out in the DAPIX-Friends of Presidency Working Party. The Council invites the Commission to regularly report to the Working Party about its findings from to these consultations.

---

7 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/1369/EC of 25 November 2009.

8 OJ L 119, 27.04.2016, p. 1

9 OJ L 119, 27.04.2016, p. 89

10 2017/0003(COD)

3.6. At a second stage, the outcome of these consultations should feed into a comprehensive study on possible solutions for retaining data, including the consideration for a future legislative initiative one. Besides the outcome of the consultations, such study should also take into account:

- the evolving case-law of the European Court of Justice and of national courts relevant for data retention; and
- the outcomes of the common reflection process as set out in particular in the Presidency Notes 14480/1/17 REV1 and 14329/18.

3.7. The study should *inter alia* further substantiate the concept of restricted data retention (first level of interference) and the concept of targeted access to retained data (second level of interference), and explore to what extent the cumulative effect of strong safeguards and limitations at both intervention levels could assist in mitigating the overall impact of retaining those data [, in particular when it is ensured that access is solely given to specific data needed for a specific investigation.]

3.8. The Council invites the Commission to report on the state-of-play of its work on data retention by the end of 2019.