Council of the European Union
General Secretariat

Brussels, 29 April 2019

WK 5407/2019 INIT

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (17.12.2019)

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:	General Secretariat of the Council
To:	Delegations
Subject:	Council Conclusions on improving retention of data for the purpose of fighting crime effectively - Comments from FR, PL and COM

POLAND

Having regard the discussion which was held on FoP DAPIX data retention on 11th April, after consultations on national level, we would like to submit the following compromise proposition for the point 5 of draft council conclusions.

Instead of deleting the above mentioned paragraph we would like to propose as follows:

> *It should however be underlined that the existence of ~~different national legal regimes~~ **differences between solutions** for data retention may however ~~be counter-productive~~ **cause limitations** for cooperation and information exchange between competent authorities.*

FRANCE

ANNEX

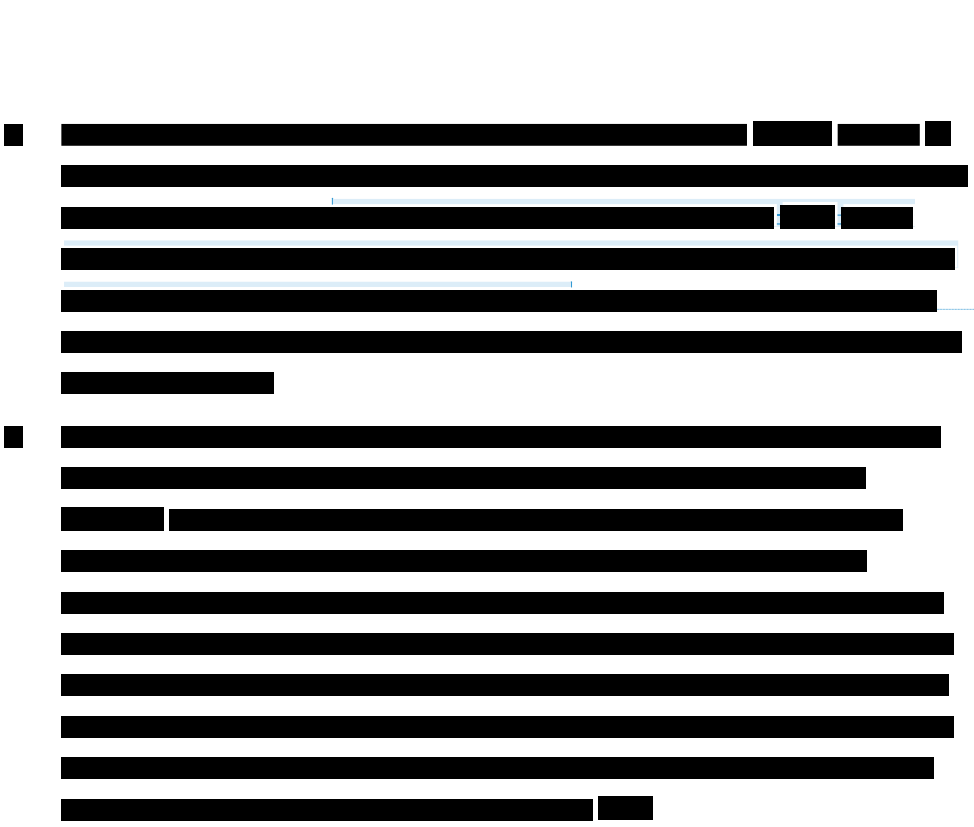
[redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]



[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

- [redacted]
- [redacted]

COMMISSION

ANNEX

DRAFT CONCLUSIONS OF THE COUNCIL OF THE EUROPEAN UNION ON ~~IMPROVING~~ RETENTION OF DATA FOR THE PURPOSE OF FIGHTING CRIME ~~EFFECTIVELY~~

Introduction

6. Data stemming from telecommunication operators and service providers ~~provides~~ is very important in order for law enforcement, judicial authorities and other competent authorities to successfully investigate criminal activities, such as terrorism and cyber crime, in the digital age.

7. In order to ensure that information necessary to conduct investigations effectively is available to law enforcement, judicial and other competent authorities, ~~it may not be sufficient to rely on~~ data retained by telecommunications operators and service providers for business purposes may not be sufficient for those authorities' purposes. Indeed, ~~such business purposes are~~there is no guarantee that operators will retain the data necessary for law enforcement~~will be retained~~, and if data is retained, the period of retention time would not be predictable. ~~Neither is there any guarantee that the telecommunications operators and service providers retain such specific data which may be required by law enforcement, judicial and other competent authorities.~~

8. It is ~~therefore appears~~ an objective of general interest to maintain public security, prevent and fight crime and ensure security of persons. ~~as well as a necessaryprerequisite for ensuring fundamental rights, includingsuch as the security of persons,~~ It is therefore appropriate to lay down ~~additional~~ proportionate, necessary and transparent data retention obligations for telecommunications operators and service providers to meet law enforcement operational needs, while providing for sufficient safeguards ~~also~~ for ~~other~~ fundamental rights, as enshrined in the Charter, in particular the rights to privacy and protection of personal data.

Commented [A8]: This paragraph seems to repeat similar ideas. For instance, the last sentence is redundant with the rest of the paragraph and in our view can be deleted. We propose to edit the text as indicated.

Commented [A9]: Laying down rules is a means to achieve an objective of general interest, not an objective of general interest in itself. We have therefore reformulated this para in a way that first sets out what the objective is and then say that to achieve this objective we need to have (necessary and proportionate) data retention rules.

Commented [A10]: Security of persons is not a fundamental right as such. However, given that states have a duty (of care) to protect their citizens, we propose to include the reference to 'ensure security of persons' in the first sentence.
By contrast, the rights of privacy and data protection are fundamental rights. The words 'also' and 'other', are thus redundant also in light of the preceding changes.

9. The rulings of the European Court of Justice in the cases *Digital Rights Ireland*[19] and *Tele 2*[20], which set out the criteria for the lawful retention of data and access thereof are of fundamental importance ~~in this context~~. In this context, Member States expressed their view[21] 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. ~~It should also be noted that it has been argued that the findings of the Court in those cases apply only to traffic and location data, and not to subscriber data.~~

10. The conclusions of the European Council of 23 June 2017 stress the importance of securing availability of data for the effectiveness of the fight against serious crime, including terrorism[22]. It should ~~however~~ be underlined that the existence of different national legal rules~~egimes for~~ in the area of data retention may ~~however~~ be counter-productive for cooperation and information exchange between competent authorities in cross-border cases. In this sense, the conclusions of the European Council of 18 October 2018 calls 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[23].

---

19 C-293/12
20 C-203/15
21 14319/18
22 EUCO 8/17
23 EUCO 13/18

11. In April 2017 the Council ~~has~~ launched a reflection process on data retention for the purpose of ~~prevention and prosecution of~~ preventing and fighting crime. The results of this process will assist Member States in 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 effectively in light of that~~e~~ case-law ~~of the Court of Justice~~, which is evolving as new cases have been brought before the European Court of Justice following the *Tele 2* ruling. Important progress of the reflection process includes:

    - The Council taking note of the progress in December 2017[24];
    - The compilation from Member States on the use of retained data in criminal investigations[25];
    - The outcome of data retention workshops at expert level held at Europol[26].

12. At ~~the Council (Justice and Home Affairs)~~its meeting of~~n~~ 6 and 7 December 2018, the ~~Austrian Presidency informed Ministers about~~ Council took note of the state of play of this reflection process, including some key directions for further work[27]. I~~and, i~~n the subsequent exchange of views, several Ministers called upon the Commission to conduct a comprehensive study on the possible solutions for retaining data, including a legislative initiative, taking into account the development of national and EU case-law.

13. Relevant case law at national and EU level must therefore be followed closely, in particular ~~as~~ regarding~~s~~ the most recent requests for a preliminary ruling by the Investigatory Powers Tribunal in the UK[28], the Constitutional Court in Belgium[29], the *Conseil d'Etat* in France[30], and the Supreme Court of Estonia[31], to the European Court of Justice.

Commented [A11]: We believe that it is important to maintain the element of prevention: in Union law the term "fighting" (or combating) crime is usually clearly distinguished from crime prevention. We do not think that MS would want to exclude this important aspect of data retention.

---

24 14480/1/17 REV 1

25 WK 5296/2017 REV 1

26 WK 5900 2018 INIT

27 14319/18

28 C-623/17. The request for a preliminary ruling is concerned with the scope of Union Law in relation to measures taken at national level for the purpose of protecting national security.

29 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 fighting other forms of crime or guaranteeing the national security and the defence of the territory or (ii) fulfilling the positive obligations as set out in Articles 4 and 8 of the Charter (prohibition of torture and protection of personal data).

30 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

14. The report of the Special Committee on Terrorism of the European Parliament notes that the necessity of an appropriate data retention regime was consistently raised during the work of the Committee. 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.

15. It should be recalled that the rules in the currently applicable ePrivacy Directive[32], the reformed legislative framework of the European Union, in particular the General Data Protection Regulation[33] and the Law Enforcement Directive[34], as well as the ongoing negotiations on the Commission proposal for a new ePrivacy Regulation[35] are of particular importance for the purpose of data retention.

Considerations of the Council

16. Data retention constitutes an essential tool for law enforcement, judicial and other competent authorities to effectively investigate serious crime, as defined by national law, including terrorism and cyber crime.

17. The use of data retention and similar investigative measures should be guided by the protection of fundamental rights and freedoms as enshrined by the Charter and the principles of purpose limitation, necessity and proportionality.

---

case (C623/17), the *Conseil d'Etat* asks the European Court of Justice whether the data retention regime is justified given the existing terrorist threat.

31 Case C-746/18 regarding access to retained data.

32 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.

33 OJ L 119, 27.04.2016, p. 1

34 OJ L 119, 27.04.2016, p. 89

35 2017/0003(COD)

18. Legislative reforms at national or European level, including the new e-Privacy Regulation, should maintain the legal possibility for schemes for retention of data at EU and national level~~ - that take into account f~~Future developments ~~and that are~~should be compliant with the requirements set out by the European Court of Justice and the Charter of Fundamental Rights.

Conclusions

1. Work should continue in the DAPIX Friends of Presidency Working Party on data retention.

2. The Commission is

   – ~~requested~~invited to take the appropriate steps to gather information from the Member States regarding ~~evaluate~~ the needs of competent authorities to have available data that are strictly necessary with a view to fighting crime, including terrorism, effectively;

   – invited, at an initial stage, to have a number of targeted ~~targeted~~ consultations with relevant stakeholders to complement the work being carried out in the DAPIX-Friends of the Presidency Working Party and periodically update the Working Party on its findings from these consultations;

   – invited to subsequently ~~prepare a comprehensive study, taking~~take into account these consultations, with a view to exploring ~~on~~ possible solutions for retaining data, ~~including the consideration of a future legislative initiative~~. Besides the outcome of the consultations, ~~such study~~the following should also be taken 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 in the Council[36];

Commented [A12]: We would like to remove the reference to the comprehensive study and legislation for the reasons we have outlined on previous occasions (i.e. it not feasible at the current moment due to pending CJEU court cases, EP elections and a new Commission later this year). We therefore propose to reformulate the para as indicated.

Commented [A13]: We would like to reiterate our understanding of the reference to national case law whereby 'take into account' does not imply an obligation for us to follow national jurisprudence, but simply that we may follow and be informed about national developments. National court rulings only bind the particular MS where the ruling was made (not the Commission or other MS).

[36] As set out in particular in the Presidency Notes 14480/1/17 REV1 and 14319/18.

– ~~invited to further substantiate~~ assess ~~in the study, *inter alia*, the concepts of general, targeted and 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 possible limitations at both interference~~vention ~~levels could assist in mitigating the overall impact of retaining those data to protect the fundamental rights of the Charter, while ensuring the effectiveness of the investigations, in particular when it is ensured that access is solely given to specific data needed for a specific investigation~~;

– requested to report on the state-of-play of its work on data retention by the end of 2019.

Commented [A14]: We appreciate the Presidency's change from 'substantiate' to 'assess', following our intervention at the last DAPIX meeting.
However, we maintain our position to delete this indent given our concerns about specifying the options we should look into, in particular general and restricted retention in light of the current state of play of CJEU case law.

If, on the other hand, the text is maintained, 'substantiate' should be changed to 'assess' as this is more accurate. The reference to the study should also be deleted to be consistent with our proposal to delete it from the previous indent.