



Brussels, 15 March 2019

WK 3113/2019 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:	Presidency
To:	Delegations
N° prev. doc.:	WK 870/2019 INIT
Subject:	Revised draft Outline of key political messages on improving retention of data for the purpose of fighting crime effectively

On 29 January 2019, the Presidency submitted a draft Outline of key political messages on improving retention of data for the purpose of fighting crime effectively (WK 870/2019 INIT). This draft Outline aims to provide the basis for conclusions that the Council could be invited to adopt at its meeting on 6/7 June 2019.

In light of the comments from delegations expressed in the DAPIX Working Party on 4 February and submitted as written contributions, the Presidency has revised the draft Outline. Delegations will find the revised draft Outline in Annex I. Changes to the previous text are indicated in underlined and underlined strike through. Delegations will find a synthesis of the written comments in Annex II.

The Presidency invites delegations to give their comments either orally, at the meeting of the DAPIX working Party on 11 April 2019, and/or in writing.

The Presidency intends to re-work the draft Outline into Council Conclusions format and send these draft Council Conclusions to delegations in advance of the meeting on 11 April 2019.

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

1. Indication of the current situation.
 - 1.1. In the digital age law enforcement, and judicial authorities and other competent authorities as well as intelligence services rely heavily on data to successfully investigate criminal and/or terrorist activities, such as terrorism for example.
 - 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. Business purposes are no guarantee that data will be retained at all and, if so, for what period of time. There is also no guarantee that the telecommunications operators and service providers retain such specific data as may be required by law enforcement, judicial and other competent authorities. Therefore, it has been considered necessary to require impose additional and transparent data retention obligations for on those providers to meet law enforcement operational needs. Such However, such retention of data should provide sufficient safeguards for guaranteeing infringe upon individual fundamental rights, as enshrined in the Charter, 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 view³ 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 data⁴.
 - 2.2 In its conclusions of 23 June 2017, the European Council stressed the importance of securing availability of data for the effectiveness of the fight against serious crime, including terrorism⁵. 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 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 ~~and terrorism~~ effectively in light of the 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.
 - 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 Belgium⁶, ~~and by~~ the *Conseil d'Etat* in France⁷ and the Supreme Court of Estonia⁸ to the European Court of Justice.

⁴ EUCO 13/18

⁵ EUCO 8/17

⁶ 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 ~~and~~ (ii) fulfilling the positive obligations as set out in Articles 4 and 8 of the Charter (prohibition of torture and protection of personal data ~~right to life and freedom~~).

⁷ 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.

⁸ Case C-746/18 regarding access to retained data.

- 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 Directive⁹, the reformed legislative framework of the European Union, in particular the General Data Protection Regulation¹⁰ and the Law Enforcement Directive¹¹, as well as the ongoing negotiations on the Commission proposal for a new ePrivacy Regulation¹².
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. At the same time, due account has to be taken that data retention constitutes an essential tool for law enforcement, judicial and other competent authorities to effectively investigate serious crime, including terrorism.
- 3.2. 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 ~~not prevent~~ future developments and that are compliant with the requirements of the European Court of Justice ~~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 evaluate ~~address~~ the needs of competent authorities to have ~~the certain~~ data available that are strictly necessary with a view to fighting crime, including ~~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 periodically update ~~regularly report~~ ~~to~~ the Working Party about its findings from ~~to~~ these consultations.

⁹ 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.

¹⁰ OJ L 119, 27.04.2016, p. 1

¹¹ OJ L 119, 27.04.2016, p. 89

¹² 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 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 intervention 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.
- 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.
-

ANNEX II

Outline of key political messages on improving retention of data for the purpose of fighting crime, 1. ~~and including~~ [BE] ██████████ terrorism effectively

*This document gathers the comments of Member States and the Commission on the draft outline. The comments are indicated by ~~strike through~~ and **bold**. In the text, for each comment, the relevant delegation is put between brackets. If several delegations suggested different changes to the same sentence/paragraph, these changes are separated by numbers.*

1. Indication of the current situation.
 - 1.1. In the digital age law enforcement and judicial authorities ~~as well as intelligence services~~ [BE] rely heavily on data to successfully investigate criminal ~~and/or terrorist~~ activities **such as terrorism for example** ██████.
 - 1.2. Law enforcement, judicial and other competent authorities consider that the data ~~normally~~ [BE/DE] ██████ 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, **including and** [BE] terrorism effectively. Therefore, it has been considered necessary to ~~impose~~ **require** [BE] additional **and transparent** [BE] data retention obligations ~~on~~ **for** [BE] those providers to meet law enforcement operational needs. 1. ~~However, Such~~ [BE] retention of data 2. However, **general and indiscriminate** [MT] retention of data 1. **should provide sufficient safeguards for guaranteeing the could** ~~infringe upon individual~~ [BE] fundamental rights / 2. could **conflict with some** ██████ individual fundamental rights **as enshrined in the Charter**[BE], 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 **provide an interpretation of the relevant EU legal acts regulating set out the criteria for the lawful** [PL] retention of data and access thereof.
 - 1.4. In this context, Member States expressed their view³ that the findings of the European Court of Justice in *Digital Rights Ireland* and *Tele* do not apply to subscriber data, but only to traffic and location data.

Commented [A1]: BE : As mentioned during the DAPIX-meeting on the 4th of February, terrorism should be presented as a form of crime.
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████

Commented [A2]: BE : As mentioned during the DAPIX-meeting on the 4th of February, we believe we should be rather cautious with references to the work of the intelligence services. This is outside the scope of the competences of the EU and it could unnecessarily complicate the debate in this stage.

████████████████████ ██████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████

████████████████████ ██████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████

Commented [A5]: BE : A more positive wording seems more appropriate.

Commented [A6]: MT : Justification: It must be emphasised that only general and indiscriminate retention of data is unlawful.

████████████████████ ██████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████
████████████████████

¹ C-293/12
² C-203/15
³ See 14319/18.

- 1.5. 1. ~~[The existence of different national legal regimes for data retention may be counter-productive for cooperation and information exchange between competent authorities.] [PL]~~
 2. [The existence of different national legal regimes **lack of a common legislative framework on** for data retention ~~may be~~ **is** counter-productive for cooperation and information exchange between competent authorities] [MT].

Commented [A8]: MT : The existence of different national legal regimes is a result of the lack of common European legislative framework following the annulment of Directive 2006/24/EC.

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 data⁴.
- 2.2. **In its conclusions of 23 June 2017, the European Council stressed the importance of ensuring availability of data for the effectiveness of fight against serious crime, including terrorism [BE].** The common reflection process launched by the Council on data retention for the purpose of prevention and prosecution of crime 1. ~~and including [BE]~~ terrorism 2. [REDACTED] 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 1. ~~and including [BE]~~ terrorism [REDACTED] effectively in light of the case-law of the Court of Justice **which is not settled yet, new cases having been brought before the ECJ [REDACTED]**
- 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~~ [COM], 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 Belgium⁵ ~~and~~ , [COM] by the *Conseil d'Etat* in France⁶ **and the Supreme Court of Estonia**⁷ [COM] to the European Court of Justice.

[REDACTED]

[REDACTED]

[REDACTED]

⁴ EUCO 13/18

⁵ C-520/18. The request for a preliminary ruling by the Belgian Constitutional ~~court~~ **Court [BE]** 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 [BE]** guaranteeing **the [BE]** national security and **the [BE]** 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~~ **prohibition of torture and protection of personal data [BE]**).

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.

⁷ **Case C-746/18 regarding access to retained data [COM]**

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, **in the light of the fundamental rights of the Charter**, [DE/] while taking into account the needs of the competent authorities and the specificities of the counter-terrorism field.

[REDACTED]

2.6. The currently applicable ePrivacy Directive⁸, the reformed legislative framework of the European Union, in particular the General Data Protection Regulation⁹ and the Law Enforcement Directive¹⁰, as well as the ongoing negotiations on the Commission proposal for a new ePrivacy Regulation¹¹.

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., **whereas due account has to be taken of the fact that data retention constitutes an essential tool for law enforcement, judicial authorities and intelligence services carrying out their statutory tasks in order to protect national security or public order and to successfully investigate serious crimes, including terrorism.** [PL]

3.2. 1. Legislative reforms at national or European level, including the new e-Privacy Regulation, should **maintain the legal possibility for not prevent** future developments as regards the **schemes for retention of data at EU or national level**[BE] **and should maintain the possibility for existing and future data retention regimes, compliant with the requirements of the Court of Justice** [REDACTED]

[REDACTED]

[REDACTED] Future developments as regards retention of data **should be consistent with legislative reforms at European level, including the future e-Privacy Regulation.** [COM] 1. **Furthermore, the further endorsement of data retention should be made clear/highlighted in the new e-Privacy regulation.** [BE]

⁸ 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.

⁹ OJ L 119, 27.04.2016, p. 1

¹⁰ OJ L 119, 27.04.2016, p. 89

¹¹ 2017/0003(COD)

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~~ **evaluate** [COM] the needs of competent authorities to have ~~certain~~ [MT] data available **which is strictly necessary** [MT] with a view to fighting crime, **1. including and** [BE] terrorism **2. and terrorism** [FR] effectively.

3.5. ~~At a first stage, s~~Such [COM] steps could include a number of targeted **technical** [COM] 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~~ **periodically update to** [COM] the Working Party about its findings from ~~to~~ [COM] these consultations.

3.6. **1.** 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~~ [BE].. Besides the outcome of the consultations, such study should also take into account:

~~2. 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~~ **The way forward** should also take into ~~also~~ account [COM] :

- the evolving case-law of the European Court of Justice ~~and of national courts relevant for data retention~~ [COM] ; 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. **1.** The study should *inter alia* further substantiate the concepts of **general, targeted and** [BE] 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** [BE] limitations at both intervention levels could assist in mitigating the overall impact of retaining those data **while ensuring effectiveness of the investigation** [BE] **to protect the fundamental rights of the Charta** [DE/FR] [, in particular when it is ensured that access is solely given to specific data needed for a specific investigation.]

2. Entire para 3.7 suppressed [COM]

3.8. The Council invites the Commission to report **regularly** [MT] on the state-of-play of its work on data retention ~~by the end of 2019~~ [MT]-

Commented [A14]: MT : The words 'certain data' is too vague. The text used in both rulings refer to 'what is strictly necessary'.

Commented [A15]:

COM : NOTE TO THE PRESIDENCY:

As we stated during the DAPIX-FoP meeting of 04/02/19, the Commission considers that given the legal and political uncertainty (EP elections, new Commission, ECJ rulings), launching a comprehensive study is currently not an appropriate way forward. Such a study could be rapidly rendered obsolete notably by the expected Court decisions. Moreover, were we to consider a study in the future, the Commission would need to keep an open mind by weighing all the possible options, analyzing them in an objective and comprehensive manner. It cannot be restricted to studying and substantiating only one particular scenario for the way forward (as in pt. 3.7).

Commented [A16]: MT : This contradicts the wording used in 3.5, whereby the text states that the "Council invites the Commission to regularly report to the Working Party about its findings".