Council of the European Union

Brussels, 8 May 2019
(OR. en)

7833/3/19
REV 3

LIMITE

JAI 328
COPEN 127
DAPIX 115
ENFOPOL 136
CYBER 104
EUROJUST 59
DATAPROTECT 106
CATS 68

NOTE

From:	Presidency
To:	CATS
No. prev. doc.:	WK 3113/2019
Subject:	Council Conclusions on retention of data for the purpose of fighting crime - Final text

Delegations will find in Annex the final text of the Council Conclusions on retention of data for the purpose of fighting crime as adapted following the last meeting of the DAPIX Working Party on 8 May 2019 that the Presidency intends to submit to COREPER for approval on 22 May before their adoption by the June Council.

The new changes in comparison to the previous version are marked as follows: new text - with bold and underlined where the deleted text - with ~~underlined and strikethrough~~.

ANNEX

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

Introduction

1. Data stemming from telecommunication operators and service provide**r**s is very important in order for law enforcement, judicial authorities and other competent authorities to successfully investigate criminal activities, such as terrorism ~~and~~ **or** cyber crime, in the digital age.

2. 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 no guarantee that data 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.~~

3. It is ~~therefore~~ ~~appears~~ an objective of general interest **to ~~maintain public security~~ fight crime in order to maintain public security and to ensure security of persons** as well as a ~~necessary~~ prerequisite for ensuring fundamental rights, including ~~such as~~ **non-discrimination and presumption of innocence** ~~the security of persons.~~ **It is therefore appropriate** to lay down ~~additional~~ proportional, 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.

4. The rulings of the ~~European~~ Court of Justice **of the European Union (the 'Court of Justice')** in the cases *Digital Rights Ireland*[1] and *Tele 2*[2], 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[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.~~ 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[4].

5. 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[5]. It should ~~however~~ be underlined that the existence of different ~~national~~ legal rules ~~regimes for~~ in the area of data retention may ~~however be counter-productive~~ **cause limitations** 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[6].

---

1 C-293/12
2 C-203/15
3 ~~14319/18~~
4 14319/18
5 EUCO 8/17
6 EUCO 13/18

6. In April 2017 ~~the Council has launched~~ a reflection process on data retention **was launched** for the purpose of ~~prevention and prosecution of~~ 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[7];

– The compilation from Member States on the use of retained data in criminal investigations[8];

– The outcome of data retention workshops at expert level held at Europol[9].

7. 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[10]. 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.

---

7 14480/1/17 REV 1
8 WK 5296/2017 REV 1
9 WK 5900 2018 INIT
10 14319/18

8. 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[11], the Constitutional Court in Belgium[12], the *Conseil d'Etat* in France[13], and the Supreme Court of Estonia[14], to the ~~European~~ Court of Justice.

9. 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.

---

11 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.

12 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).

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

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

10. It should be recalled that the rules in the currently applicable ePrivacy Directive[15], the reformed legislative framework of the European Union, in particular the General Data Protection Regulation[16] and the Law Enforcement Directive[17], as well as the ongoing negotiations on the Commission proposal for a new ePrivacy Regulation[18] are of particular importance for the purpose of data retention.

Considerations of the Council

1. 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~~ **or** cyber crime.

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

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

---

15 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.

16 OJ L 119, 27.04.2016, p. 1

17 OJ L 119, 27.04.2016, p. 89

18 2017/0003(COD)

Conclusions

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

2. The Commission is

– invited to take the appropriate steps to gather information regarding ~~evaluate~~ the needs of **Member States** 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~~ **requested** to subsequently prepare a comprehensive study **in accordance with Art. 241 TFEU,** taking into account these consultations, on possible solutions for retaining data, including the consideration of a future legislative initiative. 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 in the Council[19];

---

[19] 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.
