



Council of the
European Union

Brussels, 5 April 2017
(OR. en)

7597/17

LIMITE

**JAI 276
COPEN 90
DAPIX 110
ENFOPOL 149
CYBER 45
EUROJUST 48
TELECOM 80
DATAPROTECT 64**

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	6713/17
Subject:	Reflection process on data retention issues - Issues to be discussed

1. As confirmed at CATS on 8 March 2017, the Working party on information exchange and data protection (DAPIX) will meet in a Friends of the Presidency format to facilitate a common reflection process at EU level regarding issues related to retention of electronic communication data in light of the recent case law of the Court of Justice of the EU.
2. In order to structure the work of the group and to enable it to gradually take a comprehensive view on the various working strands, the Presidency has identified a certain issues to be discussed, as presented in the Annex. The issues identified set only the general framework for the future work of the group providing a possibility for approaching data retention from different angles. This approach is based on feedback from delegations. The Annex is intended to be a living document that should take into account further developments and new issues arising in the course of the reflection process.
3. Delegations are invited to exchange views on the issues identified and to propose any other issues that they think should be considered.

DAPIX (Friends of the Presidency - Data retention)

Issues to be discussed

The scope and general impact of the CJEU Judgment of 21 December 2016 (Tele 2)¹ on data retention for the purposes of prevention, prosecution and investigation of crime (also with reference to the Digital Rights Ireland ruling of 8 April 2014)², as well as the principles of necessity and proportionality for the collection and use of data, the general framework of necessary safeguards and guarantees and data protection and other fundamental rights considerations.

1. Exchange of information

Regular updates by Member States on relevant legislative and other developments, and on operational experience, in particular the consequences for law enforcement of a loss of data.

2. Targeted data retention criteria

What limitation factors e.g. geographical, technical, or other could be considered regarding:

- categories of data
- the means of electronic communications
- persons concerned
- type of serious crime
- period of retention

3. Access criteria for competent authorities

What kind of measures could satisfy the Court's criteria on access to data to meet the requirement of limiting the intervention of competent authorities to what is *"strictly necessary and justified within a democratic society"*?

1 Judgment of the Court of Justice of the EU (Grand Chamber) *"Tele 2 and Watson"* of 21 December 2016 in joined Cases C-203/15 and C-698/15.

2 Judgment of the Court of Justice of the EU (Grand Chamber) *"Digital Rights Ireland and Seitlinger and others"* of 8 April 2014 in joined Cases C-293/12 and C-594/12

4. Other criteria

- What measures could be taken with regard to:
 - Data localisation
 - Investigative techniques that could meet the criterion of targeted data retention
 - Technical measures for targeted data retention
 - Data security
 - Independent oversight
 - Individuals' rights (e.g. information, redress)

5. Data retention for other purposes (in the context of the E-privacy reform)

Purpose (billing purposes or in the context of consumer protection), scope of such retention, impact on new types of services (free of charge or flat rates), technical possibilities, ISPs perspective

6. Data retention by public authorities

Scope (what data and what authorities), technical requirements, necessary safeguards

7. Other measures

Exploring the possibility to compensate availability of data by other measures, e.g. ensuring availability of necessary data through fast track direct cooperation with ISPs.

What framework for cooperation, possible scope, conditions, etc.
