Council of the European Union

Brussels, 14 February 2019
(OR. en)

6358/19

Interinstitutional File: 2017/0003(COD)

LIMITE

JAI 133
COPEN 56
DAPIX 59
ENFOPOL 69
CYBER 41
EUROJUST 25
TELECOM 63
COMPET 129
MI 145
DATAPROTECT 43
CONSOM 57
DIGIT 33
FREMP 21

NOTE

From:	Belgium, Estonia, the Netherlands, Austria, Latvia, Denmark, France and UK delegations
To:	Delegations
Subject:	The issue of data retention in the proposal for ePrivacy Regulation - discussion paper

Delegation will find in Annex a discussion paper on the issue of data retention in the proposal for ePrivacy Regulation supported by Belgium, Estonia, the Netherlands, Austria, Latvia, Denmark, France and UK.

Non paper

E-privacy Regulation – Discussion paper on the impact on the data retention issue

The aim of this non-paper is to provide food for thought for the joint DAPIX / Telecom working party which is to be held on the 19 February and will assess the impact of the draft ePrivacy Regulation on the issue of data retention.

While it is clear that no comprehensive solution would be found within the ePrivacy Regulation (such comprehensive solution would require the adoption of a legislative instrument at European level containing necessary conditions and safeguards for a data retention system), there is a clear link between the ePrivacy legal framework as it was highlighted by the Tele2 ruling.

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. This call has been reiterated several times by the Justice and Home Affairs Ministers since the Télé2 ruling.

Considering possible future developments of the case-law of the Court of Justice, it should be ensured that the ePrivacy future framework maintains the possibility for existing and future data retention regimes compliant with the requirements of the Court of Justice (‘leaving the door open’).

The current version of the ePrivacy Regulation appears stricter than the former directive 2002/58/EU. As a consequence, there is a serious risk that the ePrivacy Regulation once applicable will further limit the possibilities of retaining data for law enforcement purposes in criminal proceedings.

Against this background, it should be ensured that the draft ePrivacy Regulation provides sufficient legal bases for existing and future data retention regimes compliant with the requirements of the Court of Justice.

The issue of general, targeted or restricted retention is not addressed in this document. After two years of work in the DAPIX Working Party, no solution has yet been found on how to implement a targeted/restricted retention. New preliminary references have been introduced, and it is to be expected that the Court of Justice will refine its case-law on that issue. This issue falls under the requirements of necessity and proportionality which are clearly set out in each proposal mentioned hereafter.

The proposals mentioned hereafter might be taken on board all-together or alternatively. **They do not reflect positions of Member States**, and only aim at facilitating the discussions in the Joint Telecom / DAPIX Working party.

I. Article 6. Permitted processing

Article 6 enumerates the grounds for which processing of electronic communication data or metadata is permissible. By virtue of to the *lex generalis - lex specialis* relationship between the GDPR and the ePrivacy Regulation, it means that, for matters specifically governed by the ePrivacy Regulation, it should apply instead of the GDPR provisions (consequently, Art 6 GDPR does not apply).

Article 6 of the ePrivacy Regulation would remain the only ground for processing of data by telecommunication providers. This means that if the provider does not collect certain types of data for one of the purposes listed in Article 6, it would be impossible to ensure the availability of those types data, while it is to be expected that with the development of flat rate packages, less data would be necessary for billing purposes.

Therefore, in order to maintain the possibility for data retention, it could be suggested to foresee an additional ground for processing based on European or national law.

*Article 6 (2), new point g : '**it is necessary for compliance with a legal obligation'***

The wording comes from article 6 of the GDPR ('*processing is necessary for compliance with a legal obligation to which the controller is subject'*). Conditions related to necessity and proportionality of such legislation could be added:

New article 6(2oa): ***Legal obligations set in accordance with point g) of this article shall be necessary and proportionate in a democratic society and subject to appropriate safeguards, be purpose limited, and subject to effective judicial remedy.***

Besides, it is to be noted that further processing (for purposes other than those for which the data have been initially collected) on basis of European or national legislations is recognized in Article 6(2a). It means that once the data have been collected for one of the legal grounds (consent, billing purposes,..), the data could be further processed on the basis of a legal obligation stemming from European or national legislations.

II. Article 7. Storage and erasure

Article 7 requires that the provider erases or anonymizes the data when it is no longer needed for the purposes they have been collected for. In order to ensure the availability of metadata for criminal investigations purposes, it may be necessary to retain them longer.

Yet, as it is currently drafted, Article 11 only enables to restrict the obligations contained in Article 7, which is unclear and could lead to different interpretations. As a result, the restrictions contained in Article 11 do not provide for a clear and sufficient legal basis for a general data retention regime.

Therefore, it could be considered to add a new sentence in paragraph 2, as follows:

Article 7 New (2a): '***Union or national law may impose an obligation on the providers of the electronic communication services to retain metadata for a longer period of time, where such an obligation respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences'.***

Such an amendment would require the deletion of the reference to Article 23(1)(d) from Article 11.

III. Article 11. Restrictions

Article 11 contains the rules on possible restrictions to Articles 5 to 8 of the Regulation. The scope and broad possibilities for restrictions could lead to very different and contradictory interpretations; indeed, it could be understood as allowing the limitation of the application of all these provisions by national law, which is not the intention of the legislator.

Thus, several amendments, either complementary or alternate, could be considered in this provision:

- the word restrict could be replaced by more suitable wording such as "derogate", "adapt the application" or "limit the application";
- the provision could be divided into several subparagraphs in order to adapt the wording to the different types of provisions; for instance, Article 6 contains the grounds for processing while Article 7 is a legal obligation to erase data;
- the goal of the provision could be completed by the addition of a possibility to extend the permitted processing.

In any case, Article 11 should contain a specific reference to data retention, as Article 15 of the ePrivacy Directive does.

'*Union or Member State law may* ~~***restrict***~~ ***derogate/adapt the application/ limit the application*** *by way of a legislative measure the scope of the obligations and rights,* ***or extend the permitted processing*** *provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) (c) to (e), (i) and (j) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.* ***To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph'***