Council of the European Union
General Secretariat

Brussels, 10 October 2017

WK 11127/2017 INIT

DOCUMENT PARTIALLY ACCESSIBLE
TO THE PUBLIC (12.01.2018)

LIMITE

JAI
COPEN
DAPIX
ENFOPOL
CYBER
TELECOM

WORKING DOCUMENT

From:	Presidency
To:	DAPIX (Friends of the Presidency - Data Retention)
Subject:	Availability of data and issues related to data retention - elements relevant in the context of e-Privacy = Exchange of views

Delegations will find attached in the Annex a Presidency paper that will serve as a basis for the discussion at the joint meeting of the DAPIX - FoP on data retention and the WP TELE on 16 October 2017.

Availability of data and issues related to data retention - elements relevant in the context of e-Privacy

= <u>Exchange of views</u>

I. Introduction

Electronic communications data is a valuable source of information for the law enforcement authorities, providing information on possible links between suspects and enabling recreation of the communication patterns of different individuals, such as suspects or victims. Electronic communications data can also provide important information on the location of the victims or link the suspect to the crime scene, as well as help to eliminate suspects from enquiries. It has to be noted that the discussion on the retention of electronic communications data only concerns communications metadata and is not related to the content of the communication. The focus of the discussion is the retention of certain electronic communications metadata to ensure availability of such data for law enforcement purposes. The definition of "metadata" will be subject to further discussions in this context, though any content-related information is always excluded. However, it should be noted that the definition of "metadata" in e-Privacy Regulation is broader than it was stipulated in EU legislation on data retention (Directive 2006/24/EC, the Data Retention Directive).

The e-Privacy Directive (Directive 2002/58/EC) was adopted in 2002 and remains in force until the new e-Privacy Regulation, currently being negotiated by the Council, will enter into force. The e-Privacy Directive provides for strict rules in order to ensure a high level of protection of electronic communication data. Article 15(1) of the Directive allows Member States to adopt national legislative measures to restrict the scope of certain rights and obligations provided for in the Directive when such restrictions constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. Article 15 (1) also allows Member States to adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in that paragraph. All the measures referred to in 15(1) shall be in accordance with the general principles of EU law.

In 2006, a specific EU legislation on data retention was adopted (Directive 2006/24/EC, the Data Retention Directive), laying down specific rules to harmonise retention measures throughout the EU. However, in 2014 the European Court of Justice (ECJ) in its Judgment of 8 April *2014 Digital Rights Ireland*[1] invalidated the Data Retention Directive *ab initio*, i.e. from the date it took effect in 2006.

Another case was brought before the ECJ to assess conformity of national legislation adopted on the basis of Article 15 (1) of the e-Privacy Directive with the Charter of Fundamental Rights. In its Judgment of 21 December 2016 *Tele2*[2], the ECJ ruled that Article

[1] Judgement 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

[2] Judgement 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.

15(1) of the e-Privacy Directive, read in the light of the Charter, must be interpreted as precluding national legislation *"which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication"*[3].

The ECJ has stated that general data retention cannot become a rule. Therefore, in order to be compliant with the Charter, the retention of data has to be limited to what is strictly necessary. There should always be a link between the retained data and the purpose pursued. Therefore, it is necessary to assess what kind of data can potentially be relevant to retain for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including safeguarding against and prevention of threats to public security. Additionally, the ECJ requires access to the retained data to be targeted and include additional safeguards such as limited storage period, differentiated access rules, adequate supervision etc.

The referred case law resulted in direct implications for the operational capacities of the competent law enforcement and judicial authorities in terms of ensuring the availability and subsequent use of retained data for the purposes of prevention, investigation and prosecution of crime. It also raised the necessity to address the scattered picture of data retention rules currently applicable across the EU.

II. State of play

Following the *Digital Rights Ireland* judgement, the Justice and Home Affairs (JHA) Council has called upon finding a solution to ensure that retained communications data remain available for the law enforcement purposes, in line with the ECJ requirements. On 22 June 2017, the European Council also highlighted the importance of the availability of data[4]. At the informal meeting of Justice and Home Affairs Ministers in Tallinn on 6-7 July 2017, Ministers confirmed that the DAPIX - Friends of Presidency on Data Retention should examine any legislative and non-legislative options, including in the context of the proposed e-Privacy Regulation, to address the issues arising from the recent ECJ case law on data retention.

The objective and main features of the draft e-Privacy Regulation were presented by the Commission at the DAPIX - FoP meeting on 17 July 2017. Delegations agreed that alongside developing specific legislation on data retention for the purposes of fighting crime, a complementary approach could be considered in the context of the e-Privacy Regulation. The aim of such an approach would be to ensure the availability of communications metadata processed for business purposes, while not imposing a specific storage obligation on providers for the purposes of prevention and prosecution of crime as such in the draft Regulation. Delegations expressed an interest to examine relevant elements of the e-Privacy Regulation proposal to that end.

[3] See Information Note by the Legal Service to COREPER (doc. 5884/17)
[4] European Council conclusions on security and defence, 22.06.2017. Available: http://www.consilium.europa.eu/en/press/press-releases/2017/06/22-euco-security-defence/

The Presidency has analysed the input provided by delegations to DAPIX - FoP and has decided to put on the basis of that input under discussion a selected number of issues at the joint meeting of the DAPIX - FoP on Data Retention and the WP on Telecommunications and Information Society. The Presidency would like therefore to invite an exchange of views on the specific issues listed below, with a view to assessing the feasibility of each of them from a multidisciplinary point of view and using the input for future work on issues related to data retention.

In view of the above, the purpose of the joint meeting is to explore the extent to which the issues related to the availability of data could be addressed in the context of the e-Privacy Regulation and the margin for further specification of the scope of the Regulation insofar as the activities of competent authorities are concerned, taking into account the case law by the ECJ.

III. Framework of the discussion

It is important to highlight, that two different aspects of the data retention have been assessed by the ECJ against the requirements of the Charter:

- retention and availability of data

- rules on access to the retained data.

Based on the discussions in the DAPIX-FoP, the Presidency is of the opinion that the e-Privacy Regulation is not the instrument to lay down criteria for law enforcement access.

The issue of the availability and retention of the data is, however, linked to the e-Privacy Regulation. As the e-Privacy Regulation will apply to all processing of electronic communications metadata, data availability, resulting from the processing activities of providers could currently fall under the rules of e-Privacy.

Concept of confidentiality of communications. Article 5 of the e-Privacy Directive (as well as Article 5 of the draft e-Privacy Regulation) provides for confidentiality of communications. The principle of secrecy of communications derives directly from article 8 ECHR and has been clearly asserted by the European Court of Human Rights. The right to the confidentiality of communications is a fundamental right protected under Article 7 of the Charter of Fundamental Rights of the European Union (the Charter). It is embedded in the European constitutional traditions, where the majority of EU Member States also recognise it as a distinct constitutional right. The underlining principle of confidentiality of communications prohibits any interference with the communications, unless it is provided for by law and fulfils certain predefined criteria, e.g. necessity in democratic society, meeting the objectives of general public interest etc, as recognised by the jurisprudence.

DELETED FROM THIS POINT UNTIL THE END OF THE DOCUMENT (page 6)