Council of the European Union

Brussels, 4 May 2017
(OR. en)

8798/17

LIMITE

JAI 390
COPEN 125
DAPIX 166
ENFOPOL 206
CYBER 66
EUROJUST 59

NOTE

From:	Presidency
To:	Delegations
Subject:	Access criteria for competent authorities to retained communication data - Exchange of views

In its Judgment of 21 December 2016 [1] *Tele2*, the Court ruled that Article 15(1) of Directive 2002/58/EC (the ePrivacy Directive) [2], read in the light of the Charter of Fundamental Rights, must be interpreted as precluding national legislation that *"governs the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union".*

1 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.

2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ L 201, 31.7.2002, p. 37). This Directive is being thoroughly reviewed following the proposal submitted by the Commission in January 2017 to replace it by a Regulation (see Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), doc. 5358/17).

To provide a framework for the discussion, the Presidency would like to invite an exchange of views on the impact of the access criteria set out by the Court in paragraphs 113 to 125 of the Tele2 ruling at the next meeting of the DAPIX - FoP, organised around the questions below. Member States are invited to exchange views on these questions with a particular focus on the impact of the access criteria/conditions on the operational capabilities of law enforcement authorities (LEAs), including existing investigatory methods/techniques and to provide concrete examples where possible, in this respect.

I. Regarding the **scope of access** to retained communications data in terms of the **purposes** for which data are used and processed, paragraph 115 of the Tele2 ruling states that, in relation to the (exhaustive) list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58, "*it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, **only the objective of fighting serious crime** is capable of justifying such access to the retained data.*" [3]

Member States are invited to reply to / discuss the following questions:

1. What impact does/will this limitation have on the types of crime that LEAs are able to investigate compared to what is currently allowed under your legislation?
2. Is it possible to identify criminal offences that would be impacted in particular?

[3] It should be noted that there is a pending request for a preliminary ruling (C-207/16, Ministerio Fiscal) which deals with the notion of serious crime.

II. Regarding the **scope of access** in relation to the **persons** whose data can be accessed, paragraph 119 of the Tele2 ruling states: "*Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime,* ***only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime*** *[..]. However,* ***in particular situations,*** *where for example vital national security, defence or public security interests are threatened by terrorist activities,* ***access to the data of other persons*** *might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case make an effective contribution to combating such activities*."

Member States are invited to reply to / discuss the following questions:

1. What impact do/will the conditions set out in paragraphs 119 have on your relevant national legislation and on the current investigatory methods/techniques of LEAs?
2. Does your legislation provide for 'particular situations' such as the ones identified in paragraph 119 where access to data of other persons would be allowed? Are there any other particular situations that could justify access to the data of other persons ? What categories of persons should be considered in such circumstances?
3. Could you provide examples of 'objective evidence', as mentioned in paragraph 119?

III. Regarding **conditions** relating to access, paragraph 118 of the Tele2 ruling states: "national legislation must also lay down **substantive and procedural conditions** governing the access of the competent national authorities to the retained data". These conditions include **ex-ante review, oversight, individuals' rights and security and protection of retained data** (see paragraphs 120 to 123 of Tele2).

Member States are invited to reply to / discuss the following questions:

1. What impact do/will the requirements set out in paragraphs 120 to 123 have on your relevant national legislation and on the current investigatory methods/techniques of LEAs?
2. Does your legislation require prior review/authorisation of access by a court or independent administrative body? How could an operational system be put in practice (SPoC, fast track procedures)? On the basis of what criteria could "a validly established urgency" referred to in paragraph 120 be demonstrated?
3. Regarding the notification to the persons affected (paragraph 121) are there specific indicators that could be considered to establish that *"notification is no longer liable to jeopardise the investigations undertaken by […] authorities"* ?
4. Does your legislation require service providers to retain data within the European Union and to irreversibly destroy the data at the end of the retention period? Does/will this requirement raise issues of e.g. burden, cost, technical implications? How should the control for compliance with this obligations be ensured?
5. Are there other procedural conditions than the ones mentioned in paragraphs 120 to 123 that could be considered in this context?
6. Should a limitation of the types of authorities and/or staff/officers who can submit a request for access to a service provider and who can actually access and use the data once it has been handed over be envisaged?

IV. Are there any other conditions for access to retained data not referred to in the questions above that could be considered in this context?