Council of the European Union
General Secretariat

Brussels, 02 August 2018

WK 9459/2018 INIT

LIMITE

DAPIX
CODEC
COMPET
CONSOM
COPEN
CYBER
DATAPROTECT
DIGIT
ENFOPOL
EUROJUST
FREMP
JAI
MI
TELECOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Delegations
Subject:	Procedural legal requirements for access to retained data - Exchange of views

Delegations will find in Annex a discussion paper of the Presidency on procedural legal requirements for access to retained data.

1. Introduction

A common reflection process on data retention for the purposes of prevention and prosecution of crime in the light of ECJ judgements *Digital Rights Ireland* and *Tele2* was launched under the MT Presidency and has been continued by the EE and BG Presidencies.

The December 2017 Council decided to focus on three main elements for the future work, namely: ensuring availability of data (coherence with the draft e-Privacy Regulation); setting access safeguards and restricting the scope of the data retention framework in view of recent jurisprudence[1]. The EE Presidency has already made several proposals to further substantiate the concept of targeted access to retained data (second level of interference) in doc. 13845/17. The current note looks at different aspects, elements and options concerning the **procedural legal requirements** for access to retained data.

In this context, the ECJ rulings *Digital Rights* and *Tele2* both contain criticism of the lack of rules regulating the procedural criteria under which retained data can be accessed. In *Digital Rights* the ECJ states:

> *"Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits."* [2]

As a general rule the ECJ reasoning in *Tele2* is as follows:

> *"In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse."*[3]

---

1 14480/1/17.
2 *Digital Rights*, para 62.
3 *Tele2*, para 109.

Before *Tele2*, the ECJ complained about the lack of clear and precise procedural rules in *Digital Rights*:

> *"Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use."*[4]

2. Procedural criteria for access to retained data

2.1. Review by a court or by an independent administrative body

The EJC rulings *Tele2* and *Digital Rights* both make clear the necessity of safeguards throughout all procedural steps taken in relation to data retention. The prior review carried out by either a court or an independent administrative body is cited as an important safeguard:

> *"In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should [...] be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime."*[5]

Delegations are invited to give their opinions on and share their experiences of the following questions:

- **Do you deem the prior review by a court and/or an independent administrative body to be necessary?**
- **Does your legal system provide safeguards such as a prior review by a court and/or an independent administrative body? If not, what other safeguards does it provide?**

---

4 *Digital Rights*, para 61.

5 *Tele2*, para 120 (by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 62).

2.2. Exceptions to the general rules in cases of urgency

In *Tele2* the ECJ states that there should be a system of prior review in place with the exception of cases of validly established urgency.[6] The ECJ does not set out the grounds on which these exceptions can be made and in which cases the general rules of a reasoned request, which is reviewed before allowing to access the data, need not be complied with.

Delegations are invited to give their opinions on and share their experiences of this issue, especially the following questions:

- **What is your opinion on providing / attaching such exceptions to the general rule on prior review?**
- **In your opinion, in which cases should such exceptions be applicable?**
- **Which exceptions could be compatible with ECJ case law?**

2.3. Installation of a legal protection commissioner / independent supervisory body

In *Tele2* the ECJ states, that not only must

> *"the Member States […] ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law".*

The ECJ also specifies that if this protection of individuals in relation to the processing of personal data was not guaranteed,

> *"persons whose personal data was retained would be deprived of the right to lodge with the national supervisory authorities a claim seeking the protection of their data."*[7]

6 *Tele2*, para 120.
7 *Tele2*, para 123.

Delegations are invited to give their opinions and share their experiences on this issue, especially on the following questions:

- **Would you consider an additional safeguard such as a legal protection commissioner[8] or a supervisory body necessary in order to give individuals the possibility to protect their fundamental rights? If yes:**

1) Which duties should such a legal protection commissioner or supervisory authority cover?

2) When should this review take place in the proceedings (before or after the approval? both?)

3. Special rules for access to retained data of certain groups of persons

3.1. Exemptions for persons subject to professional secrecy

In the DAPIX WP meeting of 6 November 2017 several delegations have made remarks that they did not deem exemptions at the retention level for persons subject to professional secrecy to be feasible, but wanted the topic to be discussed at the access level.

Concerning the lack of exemptions in Directive 2006/24 for this group the ECJ in *Digital Rights* stated that:

> *"[I]t does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy."*[9]

The reasoning in *Tele2* is similar[10]. Therefore, procedural rules which would prevent the retained data of groups of persons subject to professional secrecy (doctors, lawyers, etc.) from being accessed could be considered.

---

8 In order to exercise the special legal protection afforded by (e.g. data retention) measures, an independent legal protection commissioner can be appointed as an additional safeguard.

9 *Digital Rights*, para 58.

10 see *Tele 2*, para 105.

Delegations are invited to give their opinions and share their experiences, especially as regards the following questions:

- **In your national law, are there any exemptions or other restrictions concerning access to the retained data of persons subject to professional secrecy?**
- **Do you think a data retention regime should provide exemptions for persons subject to professional secrecy, or would such a regime be too complicated and harm investigations?**
- **Do you think a data retention regime without exemptions for persons subject to professional secrecy would be compatible with Union law/your national constitutional law?**

3.2. Access to the data of persons that are not suspects or accused persons

There are situations in which having access to the data of victims and other persons, who are not suspects or accused, helps to advance the criminal investigation and prosecution of crimes. However, for obvious reasons accessing the retained data of persons that are not suspects or accused persons is even more sensitive than accessing the retained data of a suspect or accused persons.

The ECJ reasons that in the case of suspects or accused persons:

> *"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"*[11].

[11] *Tele2*, para 119.

However, the ECJ sets the threshold for access to the retained data of persons who are not suspects or accused persons even higher:

> *"[I]n 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."*[12]

Delegations are invited to give their opinions and share their experiences, especially as regards the following questions:

- **Do you think a data retention regime in which access to retained data is not limited 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 would generally be compatible with Union Law? Could specific objective criteria justify the access to the data of non-suspects? If so which ones?**
- **- Should access to the retained data of non-suspects be limited to particular situations, where vital national security, defence or public security interests are threatened or should it also be possible in cases of very serious crime (for example murder, rape, armed robbery, etc.)?**

4. Notification of the persons affected

As a prerequisite for giving the affected individuals the possibility to take further steps, they must first be informed of the fact that their retained data has been accessed. In *Tele2* the ECJ states:

> *"... the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities."*[13]

12 *Tele2*, para 119.
13 *Tele2*, para 121.

Delegations are invited to give their opinions and share their experiences as regards the following question: Do your legal systems experience any issues with regard to notifying the persons affected of the access to their retained data?

5. Legal remedies

In view of the comments expressed under point 3, above, notifications that the data of a data subject have been accessed subsequently pave the way for taking steps towards an ex-post review of the decision granting access to retained data. In *Tele2*, the ECJ states that it is necessary that these decisions are subject to judicial review, as follows:

> "*That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy*"[14].

Delegations are invited to give their opinions on and share their experiences in relation to the possibility of data subjects having the right to a legal remedy (which right is often exercised following a notification that their, data have been accessed), especially as regards the following question:

Can you think of any reasons why affected persons should not have the right to a legal remedy in these cases?

Finally, delegations are kindly invited to share any other suggestions or experiences with regard to the procedural legal requirements for access to retained data.

---

[14] *Tele2*, para 121.