Council of the European Union
General Secretariat

Brussels, 12 April 2018

WK 3974/2018 INIT

LIMITE

CYBER
COPEN
DAPIX
ENFOPOL
JAI

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:	DAPIX (Friends of the Presidency - Data Retention)
Subject:	Renewable retention warrants = initial exchange of views

Delegations will find in Annex a discussion paper on renewable retention warrants.

ANNEX I

I. INTRODUCTION

A common reflection process on data retention was launched under the MT Presidency[1] to assist Member States in analysing the requirements of the ECJ TELE2 judgement and to explore options for ensuring the availability of data for the purposes of prevention and prosecution of crime. The results of the active work pursued by the EE Presidency were presented to the December 2017 Council.

That report[2] presented the state-of-play and provided details on the 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 the recent jurisprudence. To further substantiate the **concept of restricted data retention** (first level of interference) certain issues such as limiting the data categories, limiting the data retention periods and using renewable retention warrants were specified in the report for further exploration.

The current note looks at different aspects, elements and options concerning the renewable retention warrant (RRW) which are intended to ensure the law enforcement needs to have certain data categories being retained by the electronic service providers[3] and provide additional safeguard that the data retention regime would comply with the strict necessity principle as prescribed by the ECJ.

For the purpose of the present discussion RRW would be provisionally described as a *warrant issued by a competent national authority addressed to (an) electronic service provider(s) (ESPs) operating in the territory of a Member State requesting the provider to retain (certain categories of) data which is valid for a specific period of time during which it can be renewed if it fulfils the specific conditions prescribed by national law for its renewal, including that its proportionality and necessity are justified by a prior and confirmed by a subsequent threat assessment.*

---

1 As confirmed by CATS on 8 March 2017 (doc. 6713/17).
2 14480/1/17.
3 See Para 106 of the *TELE 2* Judgement and para 59 of the *Digital Rights* Judgement.

The Presidency invites delegations to express their views and relevant national experience that can bring further clarity on the concept above and its minimum elements described below as well as on any other aspects they deem relevant in this regard.

To illustrate the matter the Presidency has prepared a mindmap that is attached to this document.

II. MINIMUM ELEMENTS FOR THE RRW

1. Legal basis

The legal basis for issuing a RRW would normally derive from provisions regulated in the national law as no EU legal basis is currently in place. Such national regimes would allow to better take into account national specificities. On the other hand the absence of harmonised rules at EU level might pose some challenges for the ESPs that could be confronted with different national legal regimes regulating RRW.

It would be important also to analyse whether the legal base should include a technologically neutral reference to the data categories needed by LEAs for prevention, detection and prosecution of crimes.

2. Justification (prior threat assessment for the initial RRW or subsequent threat assessment in case of RRW renewal)

As specified by the ECJ, a link between the data retention and the purpose pursued - to prevent and prosecute crimes, i.e. to counteract the threats to public security - should be established. Thus the necessity for issuing a RRW should derive from a prior threat assessment reflecting the specific circumstances in that MS or region (i.e. technological developments, a newly emerging crime trend or significant increase of specific type of crimes, etc.) which justify the needs of the competent authorities in that MS or region to have (certain categories of) data available for their investigations and prosecutions.

2.1. Substantive scope of the threat assessment (type of crimes):

The TELE2 judgement refers on several occasions to the fight against serious crime. Therefore, the scope of the threat assessment could be limited only to such crime. A matter to be considered in that regard is lack of common understanding at EU level what constitutes a serious crime. However, in order to ensure the right to security of persons as provided in Article 6 of the EU Charter of fundamental rights, the scope of the threat assessment could be broadened to encompass some specific type of crimes such as cybercrime, cyber-enabled crime and cases of life-threatening or urgent situation (missing persons, online stalking, terrorist attacks) that might not fulfil the national threshold for a serious crime.

2.2. Geographical scope of the threat assessment

Threat assessments can be conducted either at national level, i.e. a country specific assessment of the criminality situation, or at EU level, such as SOCTA and i-OCTA, i.e. providing a more comprehensive EU-wide picture. In case of parallel national and EU threat assessments they would need to be synchronised with respect to (type of) crimes and periods analysed (frequency). The possibility of sharing the results of the national and/or EU threat assessment among the MS could be considered in this regard.

3. Prior and ex-post judicial oversight

The provision of prior and ex-post judicial oversight for the issuance and respectively the renewal of a RRW would serve as a strong safeguard. In this regard it would be useful to consider: **who** should be entitled to appeal a RRW, i.e. should this possibility be provided/limited to the ESPs that are addressees of the RRW; on **what grounds** the appeal could be based, i.e. procedural ones or such related to the technical feasibility of the warranted retention by the ESPs; what would be the **legal effect** of an appealed RRW addressed to a number of ESPs, but appealed by one of them, i.e. if the RRW is repealed would this have an effect only for this ESP or for all, would the appeal postpone the execution of the RRW and thus extend its validity period; and whether the oversight should be **entrusted to a specifically designated national judicial authority**.

4. ESP(s) to whom a RRW is addressed defined by either type of provider or service offered

A starting point could be the case where all electronic service providers operating on the territory of the issuing Member State are subject to RRW otherwise the latter could be rendered ineffective for law enforcement purposes (if some ESPs are not subject to RRWs, communication data essential for some cases could not be subject to the data retention regime). The ESPs covered are the providers of "publicly available electronic communication services or of public communications networks" (e.g. fixed network telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony, OTTs).

However, a differentiated approach based on the ESPs' size and/or service offered could be considered in certain cases, where certain ESPs could be excluded from the scope of the RRW either on the basis of their size (possible criteria to be used the number of their active users) or on the basis of the fact that they provide very specialised services. In the case where a differentiated approach is used, the RRW should be sufficiently precise in order not to leave doubts as to which ESPs are covered. Such approach could benefit SMEs providers as it would take into account the administrative burden and additional costs to be born by the ESPs in relation to the execution of a RRW.

In order to avoid doubts regarding the ESPs that are covered, a specific RRW for each single ESP operating on the territory of the issuing MS could be also considered. This could simplify the judicial oversight on one side and on the other take into account the specific technologies used by the respective ESP.

5. Data to be retained

The respective national (or EU) legislation could envisage that a RRW would be issued by a competent national authority if a certain type of crime as demonstrated by the prior threat assessment justifies the retention of [specific categories of] data. However, it should be borne in mind that different data retained in different MS could hamper investigations involving two or more MS. This could also create an additional administrative and financial burden for ESPs. Large-scale global ESPs might be confronted with requests for retention of different data in different MS. Another issue to be considered is whether RRWs are to use technically neutral language only or could specify the concrete elements that are to be retained.

A more general issue that should be explored is how the RRW would relate to the data matrix, which MS are elaborating with Europol assistance, i.e. whether they compliment or contradict each other. In the latter case, a solution should be envisaged to deal with that.

Finally, a RRW would be expected to cover data at rest and will depend on the results of the threat assessment conducted either at national or EU level allowing thus the establishment of a direct link between the data to be retained and the committed crimes.

6. Retention period

Different retention periods could hamper the investigations involving two or more MS. Given the importance, the matter should be discussed separately. For consistency reasons it is kept in the list of the RRW minimum elements.

7. Issuing authorities

RRW would be issued by the national authorities competent to issue warrants under the applicable national law. It could be the authority which conducted the threat assessment or, given the RRW nature, a specific body could be entrusted with this function.

8. Validity period

The RRW should be valid for a certain period of time whose duration can vary, for example three or six months depending on the frequency of conducting national threat assessments, or one year with the argument that SOCTA and I-OCTA threat assessments are conducted on yearly basis at EU level or any other period that can be reasonably justified given the level of interference.

9. Conditions for renewal

The RRW should provide for the possibility to be renewed within its period of validity should the conditions that justified its necessity and proportionality in the first place are fulfilled by a subsequent follow-up threat assessment performed by the MS or EU. The same elements foreseen above with regard to the prior threat assessment should be applicable here.

ANNEX II

RENEWABLE RETENTION WARRANTS