Council of the European Union
General Secretariat

Brussels, 15 September 2017

WK 9699/2017 INIT

LIMITE

JAI
COPEN
DAPIX
ENFOPOL
CYBER

WORKING DOCUMENT

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	Contribution to the discussion on data retention

FoP Data retention 18 September 2017

Data retention: Contribution by the EU Counter-Terrorism Coordinator

As the contributions of Member States have shown, data that is currently retained by telecommunications operators and over-the-top service providers (OTTs) for business purposes is not enough to ensure that law enforcement and other competent authorities have access to the necessary information (variety of length of retention, not all necessary information is being kept). Therefore, additional data retention obligations are necessary.

The EU Counter-Terrorism Coordinator suggests to explore adopting an EU instrument on data retention, to have a level playing field across the EU and find a common solution, while allowing for sufficient flexibility for Member States to tailor national solutions to their specific needs, based on the common European framework. Data retention legislation at EU level would avoid a piecemeal situation across 27 MS, which is also difficult and costly for companies. An EU legislation that addresses the points of the European Court of Justice (ECJ) might also carry additional weight in the Court.

Art. 11 of the draft e-privacy regulation would be the legal basis for an EU instrument on data retention, subject to the proportionality principle as interpreted by the ECJ.

1. EU data retention legal instrument

An EU data retention instrument has to fulfil the needs of law enforcement and other competent authorities as well as the requirements of the ECJ and could have three parts:
(1) obligation to retain restricted traffic and location data for 6 months maximum, where access of competent authorities is limited for the purposes of counter-terrorism, organized and serious crime, including cyber attacks[1],
(2) with storage of the data in the EU in an encrypted fashion,
(3) with all the strict conditions for access suggested by the ECJ.

(1) Restricted data retention necessary to fight terrorism and serious crime

Data retention cannot be "general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication"[2].

[1] Data retention is key for attribution and investigation of cyber attacks
[2] Para 134 of the Tele 2 ruling, the Court ruling.

Hence, the measure has to be limited to the strictly necessary, be based on objective evidence and needs to set out clear and precise rules. The ECJ states that retention needs to be restricted in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) *persons who could, for other reasons, contribute, through their data being retained, to fighting crime.*

It is suggested to use the concept of restricted data retention (the minimum required to fight serious crime and terrorism effectively) instead of the more limited targeted retention.

- The EU instrument could assess the current very serious terrorist threat to the EU as well as the increased use of cyber space and communications technology for serious crime, hence the serious threat to public security. The instrument could include a review clause after several years and require each Member State to assess on a regular basis the threat/risk to public security on its territory which requires data retention and renew the measure following these risk assessments.

- As a first step, to address one of the concerns of the ECJ, there could be an opt-out possibility for persons whose communications are subject, according to the rules of national law, to the obligation of professional secrecy[3]. This means that such users could request that their data not be retained and hence consent to the processing of their personal data relevant for operating this exception. Rules for such an opt-out would need to be specified.

- Beyond these exceptions, it is suggested to restrict the retention to the minimum by focusing the necessity test on data categories and providers and only retain data categories that are absolutely and objectively necessary to safeguard public security. It would be important to establish and demonstrate this link. The necessity test would not focus on groups of persons or specific geographical areas within the territory of a Member State. This would allow to restrict retention while corresponding fully to the law enforcement needs. There would be a general EU wide approach, the strict parameters and criteria of which would be set out in the instrument, based on strict necessity tests as to which type of data absolutely needs to be retained. Objective evidence with regard to the necessity of the data types could potentially be included in the legal instrument or implementing measures. It could be explored whether on the basis of such a EU instrument, the

[3] para 105 of the Tele 2 ruling: "Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 57 and 58).

Member States would have the possibility to issue retention warrants to the relevant companies that offer services on their territory, taking into account the particular situation in each Member State, or they can adopt implementing legislation, while relying on general common rules. These measures would have to be regularly renewed after new necessity assessments.

A strict necessity test could and should be carried out for the data categories that are indispensable for retention. Approaches in some Member States show that a number of data categories are indeed not necessary. This is similar to the approach suggested by Europol for restricted retention (excluding data categories that are not even potentially relevant). Common work in the EU on baseline data categories necessary to be retained could take place. It would be important to make any legal text future proof (there might be new additional data categories in the future with technological developments).

A strict test should also be carried out with regard to the various types of providers offering services based on their size and the type of service they offer. It may not be necessary to include all providers, as some have very specialized services, such as for example a small provider just offering WIFI in pizza restaurants, the data of which may potentially not be indispensable for retention.

Carrying out these necessity assessments, based on the needs of law enforcement and other competent authorities, requires effort and analysis, but allows to narrow down the scope of the data retained to the minimum necessary for the law enforcement purpose, in line with the ECJ requirements.

If there are strict necessity filters, data retention would not be generalized (only a part of the communications data categories will be retained, even though it might cover a large percentage of the population). On the other hand, retention would not be targeted to specific time periods, locations or groups of persons which would not satisfy the needs of law enforcement. The additional exemptions for persons linked to professional secrecy also mean that not the whole population is affected. The population covered by the measures would fall under the category that they "could, for other reasons, contribute, through their data being retained, to fighting crime". It needs to be recalled that the general proportionality test which is applied to restrictions of fundamental rights, which includes the strict necessity test, means that there must not be a less intrusive measure that is equally effective.

Hence, the EU data retention instrument would need to show why retention of certain types of data is absolutely necessary, while also showing that there is a thorough methodology to determine data retention obligations.

To satisfy the ECJ requirements, the possibility of competent authorities to access data stored could be limited to the purposes of counter-terrorism, organized and serious crime, including cyber attacks only.

In practice, the retention obligation would also cover data categories that are already kept for business purposes, often with the consent of the subscriber, hence minimizing the impact further. This is in particular relevant for OTTs, which have a much more data driven business model than traditional telecoms providers. In the future, the share of communications via OTTs is projected to further increase, compared to traditional providers. Hence the trend of consumers is to consent to business relevant data being kept. Today, however, experience with data retention focuses mainly on traditional telecoms providers.

The six months retention period would be the lower limit of previous EU data retention legislation. To comply with para 122 of the Tele 2 ruling, it seems that the EU instrument would have to mandate irreversible destruction of the data at the end of the data retention period. However, it would need to be clarified how this relates to data that is retained for business purposes anyhow (where the same data is covered by the retention obligation). Probably it would mean destruction only of the data that otherwise would not have been retained.

(2) Storage in Europe and in encrypted fashion/pseudonymisation

The ECJ requires " 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". Therefore, mandating requirements for data security, storing the data in the EU (as the ECJ requires in para 122 of the Tele 2 ruling) and in encrypted fashion would protect against unauthorized access. It would need to be clarified whether encrypted storage is possible with regard to business models and what other privacy by design could be incorporated, such as for example homomorphic encryption, which allows encrypted searches, with decryption possibility only on the basis of a warrant. Another option to explore would be pseudonymisation, a method where names are replaced by an alias and hence data is no longer connected to a name. In contrast to anonymisation, it is possible to re-identify the data with the name of the person

(3) Strict access conditions set out by the ECJ in the Tele 2 ruling

The EU instrument would include all the strict access conditions set out by the ECJ in the Tele 2 ruling. This includes:

- restricting access solely to the objective of fighting terrorism and serious crime[4]
- prescribing clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data
- access, subject to prior review by a court or an independent administrative authority (exception cases of urgency)
- information to the subscriber, provided the interests of the investigations can no longer be jeopardized
- legally binding instruments at EU level (and as appropriate implementing rules at national level)

(4) Conditions for access of data retained for business purposes

It could be further considered combining data retention for the purposes of prevention, investigation and prosecution of serious crime with a parallel system of ensuring access to data kept for business purposes by providers (not subject to storage obligations or kept for business purposes although there are also storage obligations), resulting in a hybrid model. Such a hybrid model could be instrumental in ensuring the availability of data in emergency or life threatening situations not necessarily related to criminal activity, e. g. missing persons. Hence, the EU data retention instrument could also include a passage regulating conditions for access for law enforcement and other competent authorities to data that is retained by companies for business purposes.

2. Draft e-privacy regulation

One of the arguments of the ECJ against generalized data retention in the Tele 2 case was also the structure of the e-privacy directive (the general rule - prohibition of storage - cannot be circumvented by a general obligation of retention[5]). As Europol points out in its contribution, the

[4] para 119 of the ECJ ruling: 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 (see, by analogy, ECtHR, 4 December 2015, Zakharov v. Russia, CE:ECHR:2015:1204JUD004714306, § 260). 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.

[5] para 89 of the Tele 2 ruling: "Nonetheless, in so far as Article 15(1) of Directive 2002/58 enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data,

secondary EU law on which the Member States had based their national data retention legislation was at issue in the ruling in addition to its interpretation in light of the EU Charter of Fundamental rights. Hence the stricter criteria set by the ECJ in Tele 2 (compared to Digital Rights) are not necessarily enshrined in the Charter itself, but may arise from the structure of the e-privacy directive. Therefore, some relevant adjustments to draft the e-privacy regulation could also be considered to avoid having the new EU data retention instrument assessed against fundamentally the same logic of secondary law, as in Tele2 (the key elements of the structure of the e-privacy directive and the proposed e-privacy regulation remain the same). This would address the argument of the Court that data retention legislation cannot turn the exception of retention in the e-privacy legislation, its legal basis, into the rule.

Some adjustments in the draft e-privacy regulation could be considered in this respect:

- The importance of data retention to fight terrorism and serious crime could be highlighted in the draft regulation.
- In Art. 5 of the draft e-privacy regulation, "storing" could be removed from the list of prohibited "interference" or to delete the examples altogether (as "storing" is a form of "processing", which is also mentioned in the examples)A step further would be to delete or change sentence 2 of Art. 5, removing the general prohibition but clarifying that any interference with electronic communications data would need to be authorized in law and meet the proportionality test.
- In Art. 7 of the draft e-privacy regulation, storage of data could be allowed if legally required to assist governments to fight serious crime and terrorism. It could also be explored to no longer require erasing or making anonymous the data after the transmission for the time of the retention period, but require instead encryption or pseudonymisation.

In order to achieve increased transparency about data retention for business purposes, it may be useful to distinguish between the traditional telecommunications providers (less data retained) and the OTTs (business model often data driven, hence probably much more data retained). Overall, it would be important to have more clarity about which data is retained for business purposes. While there are some transparency obligations in the GDPR which telecoms and OTT will have to apply,

---

that provision must, in accordance with the Court's settled case-law, be interpreted strictly (see, by analogy, judgment of 22 November 2012, *Probst*, C-119/12, EU:C:2012:748, paragraph 23). *That provision cannot, therefore, permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58, to become the rule, if the latter provision is not to be rendered largely meaningless*."
para 104 of the Tele 2 ruling: "In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, *is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.*"

the transparency obligations for telecoms and OTTs to disclose what type of data is being retained for how long (including based on consent) as well as the manner in which the information is provided could be clarified in the e-privacy directive.

It could also be considered to further clarify the elements legislation based on Art. 11 of the e-privacy regulation needs to contain (as has been done in Art. 23 GDPR). However, the quickly evolving nature of the technology (and hence data categories) in the area of electronic communications needs to be taken into account.