Council of the European Union
General Secretariat

Brussels, 02 February 2018

WK 948/2018 INIT

LIMITE

COPEN
CYBER
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:	General Secretariat of the Council
To:	DAPIX (Friends of the Presidency - Data Retention)
Subject:	Retention of electronic communication data = compilation of MS comments

Following the request to submit by 22 January 2018 written contributions on the specific elements outlined in doc. 14480/1/2017 REV 1 and on specific aspects that need to be considered further in detail, delegations will find in Annex a compilation of the contributions providedby the FR, FI, LV, MT, PT, SE and UK delegations.

FRANCE

Subject: Response to the request for contributions by Member States regarding the working document from the Estonian Presidency 'Data retention = Policy debate' – Note from the French authorities

On the document in general, the French authorities welcome:

- The deletion of the paragraph on limiting personal scope (notably for persons subject to professional secrecy) for data retention (page 7 of the new document). Moreover, the fact that this limitation should be excluded is expressly mentioned on page 9.
- The reference to 'child abuse' to illustrate the serious crimes category, alongside terrorism and organised crime. While this concept does not strictly correspond to criminal offences for certain Member States, the desire to diversify the examples given and to not limit them to terrorism and organised crime alone should be welcomed favourably.

On the notion of targeted data retention, the French authorities wish to comment on the following points:

- On limiting the categories of data retention: they are in favour of drawing up a table with EUROPOL assistance to identify all the different categories of data. It also seems that EUROJUST's expertise can be put to full use. The French authorities do however recall that it is appropriate to continue work on the other issues regarding targeted retention in parallel.

- On renewable retention warrants: the French authorities reiterate their reservations on the consequences of such individual warrants. They seem to be at risk of perpetual circumvention. If they only target certain operators, criminals will turn their attention to those that do not have retention warrants. If they only target certain geographical areas, criminals will artificially establish or fix their connections from uncovered areas. The French authorities also wish to highlight that adding and having overlapping renewable warrants could eventually lead to fragmented, though widespread and indiscriminate data retention that does not meet the requirements of the CJEU.
- On the security of the data stored: the solution of pseudonymisation mentioned in the discussion paper echoes the work already being carried out in France internally.

As part of the ongoing work on data retention arrangements, the French authorities wish to recall their proposed amendments to the 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, the 'e-privacy' Regulation.

Recital 5

Without prejudice to the processing of electronic communications data in the course of an activity which falls outside the scope of Union law, in particular to the processing of such data for the purpose of preserving defense and State security, the provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 and **Directive (EU) 2016/680** as regards electronic communications data that qualify as personal data. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679 and **Directive (EU) 2016/680**. Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation, **without prejudice to the processing of electronic communications data in the course of an activity which falls outside the scope of Union law**.

Recital 26

This Regulation does not apply to the processing of personal data in the course of activities characteristic of States or State authorities and that are unrelated to fields in which individuals are active, such as, in particular, activities aimed at preserving defence and State security. In this respect, unlike Directive 2002/58, this Regulation does not apply to national measures relating to the retention of data and to access to the data retained in the course of activities which fall outside the scope of Union law such as, in particular, activities aimed at preserving defense and State security. Therefore, pursuant to article 2, paragraphe 2, last sentence, TFEU, such processing of electronic communications data are excluded from the scope of this Regulation where they are implemented not in order to ensure the proper functionning of the internal market but on the basis of a legal framework established by the Member States in the course of activities that are characteristic of them. On the other hand, w~~W~~hen the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including ~~**national security, defence, public security and**~~ the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, ~~**including the safeguarding against and the prevention of threats to public security**~~ and other important objectives of general public interest of the Union or of a

Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).

Article 2

Material Scope

1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.
2. This Regulation does not apply to **the processing of personal data:**

(a) **in the course of** activities which fall outside the scope of Union law;

(b) ~~**activities of**~~ **by** the Member States **when carrying out activities** which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;

(c) **in connection with** electronic communications services which are not publicly available;

(d) **in the course of** activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001].

Article 11

Restrictions

1. **Without prejudice to the competence of Member States to regulate the processing of electronic communications data in the course of activities which fall outside the scope of Union law, such as, in particular, activities aimed at preserving defense and State security,** Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(c) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.

2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

FINLAND

With reference to the discussions of data retention solutions and specific elements, we have found that there are different approaches to the questions at stake. In Finland the Parliament has required that rights of the users of communications services, such as protection of privacy and confidentiality of communications, shall be ensured every which way. On the other hand, the Finnish law enforcement authorities have found that it is challenging to target data retention by restricting geographical scope or persons likely to be involved in crimes since, in practice, it has been considered impossible to predict location or persons involved in crimes in advance. In the current Finnish data retention legislation, the retention obligation is limited to certain operators, services, data categories and retention periods.

We would be particularly interested to hear more about the SE proposal for a "peeling off" approach in the light of a matrix suggested by Europol.

Should other MSs wish to have exchange of views on the question of renewable data retention warrants, it could also be included in the discussions.

LATVIA

I would like to share some of our thoughts in relation to the data retention exercise. The document, which Estonian presidency produced definitely goes into the right direction. It is more and more difficult to implement the judgments of the ECJ, before we can follow-up judgments, which make more precise and provide more clarify to the real life. From one side we think that new regulation is necessary as soon as possible, but from other side we wait for the result of other cases
(C-207/16 _Ministerio Fiscal_ and C-623/17 _Privacy International).

It is correctly concluded in the document 14480/1/2017 that the system of data retention should be effective. It is possible, as in any legal act, some amendments are necessary to the TELE2 judgment, this idea is left for each expert to wonder.

It is clear that geographical criteria will not be possible to implement in practice. It is correctly stated in the document that_ "a strict necessity test implies that there must not be a less intrusive measure that is equally effective to achieve the pursued objective".

_ _

And after these general deliberations we would be very happy to hear what the Presidency is planning to do – next steps with regards to e-privacy, EE PRES document, experts meetings.

In any case, LV planning to continue to deliberate on this question nationally, hopefully helping the Presidency on the way.

MALTA

Malta's Submissions and Contributions to the Data Retention Discussion.

Before getting into the substantial matter of this contribution, Malta would like to thank all those Member States, Europol and the European Counter Terrorism Coordinator (CTC) for their contributions to the discussion endeavouring to find a sensible solution with regards to data retention of electronic communications for the purpose of safeguarding the security of all EU citizens as enshrined in Article 6 of the Charter of Fundamental Rights whilst safeguarding the privacy rights as held in Article 7 and 8 of the same Charter.

Following the meeting of DAPIX Friends of the Presidency (Data Retention) of 18 September 2017, whereby Europol and the CTC expressed their views on the matter, coupled with the various models that may be adopted as presented on the table by the Estonian Presidency, together with other points raised throughout the discussions regarding the relevance of the draft e-Privacy Regulation (ePR) and the requirements set forth by the CJEU, Malta would like to make the following submissions with the scope of putting all factors together, perform an in-depth examination of the legal realities, and explore a possible solution.

1 Lifting the ePrivacy Regulation (ePR) barriers

It has been stated, and correctly argued, that the articulation of Article 11 of the ePR when read in light of Articles 7 and 8 of the Charter, due to its exceptional characteristics, constitute the main barrier to any legal action, whether at Union or Member State level, aimed at providing for the retention of electronic communications data. Malta concurs with this view. In this regard, it must be noted that it appears from the TELE2 ruling that the main issue is where *'the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58*[1] *requires the retention of data to be the exception'* (para. 104).

[1] e-Privacy Directive.

This does not mean that the main solution for data retention is to be included solely within the ePR. Neither does it guarantee that amending the text of the ePR will completely solve the data retention issue. However, any apparent potential barrier for a data retention regime must be eliminated.

With this in mind, Malta believes that the relevant articles of the ePR should be articulated in a way as to offer the European and national legislator the possibility to legislate alternative rules of processing of communications metadata, rather than to derogate from the rules contained in the provisions of the ePR articles. This means that a legislative instrument providing for rules of processing of communications metadata should be put on par with Articles 6 to 11 of the draft ePR, and not provide for an exception to such Articles.

Furthermore, it should be noted that the ePR is an instrument that seeks to protect the privacy rights of individuals with regards to their personal data generated and processed in a particular sector. On the other hand, a data retention instrument would seek to protect other overriding interests of public nature - public security – most notably with regards to the prevention, investigation, detection, and prosecution of terrorist offences and serious crime. Any action in this regard inherently arises from, or results in, the protection of the right of European citizens to security as enshrined in Article 6 of the Charter.

This necessarily entails that a legislative instrument providing for a data retention regime should invoke a distinct legal basis from the one underlying the ePR.

Furthermore, as already indicated, there are various models that may be possibly adopted for a data retention regime. In this regard, it is important that the articulation of the ePR articles, that are essentially the responsibility of another working party, be open enough so as not to hinder any possible solution and model that may be proposed and resorted to in the future.

For these reasons, Malta proposes the following changes to the draft ePR[2]:

[2] Changes marked in **Red**

Article 6

Permitted processing of electronic communications data

1. **Without prejudice to Article 11**, providers of electronic communications networks and services shall be permitted to process electronic communications data only if:

(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or

(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors and/or attacks in the transmission of electronic communications, for the duration necessary for that purpose.

2. Without prejudice to paragraph 1, providers of electronic communications networks and services shall be permitted to process electronic communications metadata only if:

(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 for the duration necessary for that purpose; or

(a) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(b) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

3. Without prejudice to paragraph 1, providers of the electronic communications networks and services shall be permitted to process electronic communications content only:

(a) for the sole purpose of the provision of a service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or

(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.

(e)

Article 7

Storage and erasure of electronic communications data

1. **Unless otherwise provided for by Union or Member State law in accordance with Article 11**, without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

2. **Unless otherwise provided for by Union or Member State law in accordance with Article 11**, Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

3. **Without prejudice to paragraph 2,** where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.

Article 8

Protection of information stored in terminal equipment of end-users and [related to or processed by or emitted by] such equipment

1. **Without prejudice to Article 11,** the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(f)

(b) the end-user has given his or her consent; or

(c) it is necessary for providing an information society service requested by the end-user; or

(d) it is necessary for audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user or by a third party on behalf of the provider of the information society service provided that conditions laid down in Article 28 of Regulation (EU) 2016/679 are met;

(g)

(e) it is necessary for a security update provided that the privacy settings chosen by the end-user are not changed in any way, the end-user is informed in advance and is given the possibility to postpone or turn off the automatic installation of these updates.

(h)

2. **Without prejudice to Article 11,** the collection of information emitted by terminal equipment of the end-user to enable it to connect to another device and, or to network equipment shall be prohibited, except ~~if~~ on the following grounds:

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or

(b) the end-user has given his or her consent; or

(c) it is necessary for the purpose of statistical counting that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose.

2a. For the purpose of paragraph 2 points (b) and (c), a clear and prominent notice shall be displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.

2b. For the purpose of paragraph 2 points (b) and (c), the collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

3. The information to be provided pursuant to paragraph 2a may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

4. [The Commission shall be empowered to adopt delegated acts in accordance with Article 25 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.]

Article 11

Processing of electronic communications data for other purposes

1. **Union or Member State law may provide by way of a legislative measure for the processing of electronic communications data in order to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests, provided that such measure respects the essence of the fundamental rights and freedoms and is a strictly necessary, appropriate and proportionate measure in a democratic society.**

2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

2 The Retention of Data

As was explained by Europol during the meeting of 18 September 2017 , there is a distinction between the legal effects and consequences of the *Digital Rights* and the *Tele2* ruling. In *Digital Rights*, the question brought forward to the Court concerned the lawfulness of EU secondary law. On the other hand, the *Tele2* ruling concerned the lawfulness of Member States' legislation in light of EU secondary law (e-Privacy Directive).

The former relies and is bound to adhere to EU primary law – the Treaties and the Charter. The latter is bound and confined to the EU secondary law read and interpreted in light of the Treaties and the Charter.

With regard to data retention, Malta favours an action at European level rather than at national level in order to have a harmonised system adopted across all Member States. The electronic communications activity, for various reasons – sociological, economic, technical, amongst others - has certainly no territorial confines. This facilitates crossborder criminal activity and provides a platform for criminal and terrorist networks without limitation.

A criminal offence resulting in one Member State may have been prepared or partly committed, to say the least, in other Member States or in any other corner of the globe. Thus, a common approach across the European Union territory creates certainty both for law enforcement authorities with regard to the availability of communications data required for an investigation on the one hand, and for individuals as to knowledge and awareness of the retention and possible use of their communications data throughout the EU.

Legislative action at EU level namely directives and regulations constitute secondary law. This would require such a legislative instrument to be compatible and in line with EU primary law, namely the Charter.

It follows from this that, in assessing the compliance of such legislative action with the Charter, focus should mainly be made on the *Digital Rights* ruling rather than the *Tele2* ruling, without completely disregarding the latter, since the *Digital Rights* ruling involved the examination and assessment of a secondary law (namely the Data Retention Directive – Directive 2006/24/EC) against EU primary law.

3 The *Digital Rights* ruling

The CJEU in the Digital Rights ruling leaves no doubt as to whether the interference with the rights guaranteed in Articles 7 and 8 of the Charter for the purpose of fighting serious crime and international terrorism, is justified and satisfies the objective of general public interest (see *inter alia* paras. 41 - 45).

However, the same ruling is not that clear when it comes to the proportionality aspect i.e. the interference with fundamental rights by the retention of electronic communications metadata of all users and subscribers of electronic communications services, which in the words of the court itself *'entails an interference with the fundamental rights of practically the entire European population'*(para. 56).

Nonetheless, throughout the critical assessment of the Data Retention Directive, the Court referred, on various accasions, to the fact that the Directive required the retention of communications metadata of every user using the communications services. It seems that such criticism is more directed towards the lack of *'clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data'* (para. 54) rather than towards the data retention of all users and subscribers itself. In no instance did the court rule out, completely or blatantly, the retention of communications metadata.

Notwithstanding this line of argumentation, it must be admitted thatthe ambiguity as to whether the retention of communications metadata, due to its serious interference, can ever be in line with the Charter still remains.

In this respect, although the PNR ruling sheds some light on the situation by accepting the systematic retention of passengers departing from Canada, it cannot be overlooked that the Court, in light of Article 7 of the Charter said that '*even if PNR data may, in some circumstances, reveal very specific information concerning the private life of a person, the nature of that information is limited to certain aspects of that private life, in particular, relating to air travel between Canada and the European Union'* (para. 155). This means that the far-reaching effects of the interference with regards to the transfer and retention of PNR data are very limited when compared to that of communications metadata.

On the other hand, with regard to Article 8 of the Charter, the Court went on to consider only the existence of the purposes of the processing (the fight agains terrorism and serious crime) and '*the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing*' (para. 155).

Notwithstanding the above, however in light thereof, Malta still opines that the DAPIX-FoP (Data Retention) should strive to provide a solution at EU level. In fact, these arguments are only being raised to ensure that any discussion and possible solutions will be possibly proposed/put forward and take into account such realities, which although blur the way forward for data retention, do not necessarily hamper it.

PORTUGAL

Data retention for the purposes of prevention and prosecution of crime

Contributions regarding doc. 14480/1/2017 REV 1

I. General comments

We welcome the Presidency's proposal of specific elements aiming at the adoption of a new regime on data retention for the purposes of prevention and prosecution of crime.

The specific elements presented propose the concept of "*restricted data retention and targeted access*" as a basis for outlining the new regime, structured on a differential two-level approach. This could serve as a possible solution to overcome the tension between ensuring the effectiveness of the prevention and prosecution of crime and, ultimately, public security, and minimizing the interference in the fundamental rights of individuals, as required by the ECJ.

As, in order for the access and use of data not to be rendered ineffective, the data retained has to be generally broad, the way forward must focus on establishing and setting up comprehensive safeguards and protection measures. The Presidency's elements show a significant effort towards erecting a regime which ensures this delicate balance and, at the same time, significantly reduces the scope and range of the interference in the rights of the individuals.

In this regard, we have identified some aspects which should be further developed and improved.

II. Detailed comments

(i) Scope and delimitation

As a general remark, we would point out that the lack of precise definition on what constitutes a "*serious crime*" or a "*competent national authority*" can lead to different implementations of the directive, thus defeating the overall purpose of harmonisation. Therefore, although it is clear that the harmonisation of these concepts faces significant challenges, in our view, efforts should be put into finding a common ground in order to clearly define the scope and extent of the regime across the Union.

(ii) "*Restricted data retention*"

For this effect, the Presidency proposes a set of specific proportionality/necessity filters for consideration:

a) Limiting data categories

We agree with the "peeling off" approach proposed by the Presidency.

Collecting and analysing qualitative and quantitative information to establish and demonstrate the role that each set of data retained may represent for the purposes of preventing and prosecuting serious crime will, in principle, be extremely beneficial to delimit the data which should actually be retained and can lead to the reduction the level of interference in individual rights. In this regard, we suggest to also collect information regarding the means of electronic communication relevant for this effect.

However, we note that this limitation of data, *per se*, does not allow for a restriction of the universe of subjects potentially affected by such a measure, at the first level of interference. This may prove problematic having in consideration ECJ's case law.

b) Renewable retention warrants

These retention warrants seem to be based on the method of *data preservation*, which allows only the specifically relevant data to be retained. Although, in principle, recourse to these warrants represent a lesser interference in the fundamental rights of citizens, we fear that the effectiveness of the prevention and prosecution of crimes may be compromised and have doubts as to how and to which extent this can be articulated with the differentiated approach proposed.

c) Limited storage period

We suggest the collecting of information, as mentioned above, also for this effect. For the sake of better harmonisation, the maximum period of retention foreseen in Directive 2006/24 (2 years), which seems overall excessive, should be reduced.

We agree with making a differentiation of the retention period considering the special nature of the data. Differentiation should also be established according to the data's actual relevance for the purposes of the investigation, to be evaluated having into consideration the analysis of the information collected as mentioned above.

d) Ensuring the security of data stored

Further to the measures proposed by the Presidency, we suggest to add, for consideration, the blocking of data since the beginning of its retention, as a security measure. The data shall only be "unblocked" subject to a judicial order and for the purposes of transmission to the competent authorities.

(iii) "Targeted access to data"

In our view, the access to data retained should be subject to a reasoned request by the competent authorities. This request should be specifically directed, that is, target certain data of specific people and state the underlying reasons for that request, in particular, the evidential value expected.

Regarding the categories of people that the request can target, in our opinion, the last category mentioned – "*being implicated in one way or another in such crime*" – should be better densified and, in particular, a reference to the role of intermediaries should be included. On the other hand, the inclusion of the category of victims for this effect, whenever the access is in their interest and the relevant consent is provided, could also be considered.

As for the second part of this proposed provision, in order to avoid possible abusive recourse to this provision, the specific elements thereof should be exhaustively densified (type and level of threat, categories of people possibly included, objective elements to be considered, what is meant by "effective contribution", etc.).

In our view, access to data should be subject to prior *judicial* review. In fact, a judicial intervention is the best way to ensure the fundamental rights at risk. The judge's decision shall be well-founded and access shall only be granted when it is proved relevant to the truth-finding process or if it is not possible or it is very difficult to prove it otherwise. Further to this, the judge shall take into account the need to protect professional secrecy.

Finally, in our view, specific rules should be provided regarding the conditions for the transmission of the data to the competent authorities and imposing the mandatory destruction of data in their possession once that data stops being necessary for the purposes of prevention and persecution of crime.

SWEDEN

As a follow-up to my presentation in FoP Data Retention in November, I attach to this e-mail a list with categories and types of data that have been assessed by the Swedish Inquiry with a view to conclude if each type of data is proportionate and strictly necessary. The conclusion is that a series of types of data can be retained while others cannot. Necessity of retaining certain types of data has also been an important basis for the assessment. I hope this can be a first contribution to the development of a matrix that we can work on.
Let me also say that there are obviously a number of other categories and types of data that have been and are discussed in the context of data retention. As you know, the baseline for the Tele2/Watson-judgement is 2006 and since a technical development for communications have taken place. In other words, I take it that also other categories and types of data will emerge in the discussions we have before us.

Types and categories of data to be retained and not to be retained according to the Swedish Inquiry on Data Retention; follow-up of presentation of the Inquiry and its proposals in FoP Data Retention November 2017

I. Traffic and localisation data considered to be strictly necessary and proportionate and therefore proposed to be retained by the SE Inquiry on data retention

Telephone services and **messaging**

Only communications connected via a mobile access point:

1. calling and called numbers or equivalent address;
2. for telephony: callers and called subscriber- and equipment identity;
3. data on subscriber and registered user connected to 1 and 2;
4. date and time when the communication was initiated and was terminated or a message was sent and received;
5. for telephony: data on localisation at the beginning and end of the communication;
6. date, time and localisation of first activation of pre-paid, anonymous services;
7. **missed calls** are to be included in the retention.

Internet access

1. subscribers ip-addresses and other data necessary to identify a subscriber and registered users;
2. data on subscribers and registered users;
3. date and time regarding logging on and off the service that provides internet access;
4. **data that identify the equipment that finally secluded** the communication from the service provider to the subscriber.

II. Traffic and localisation data considered not to be strictly necessary and proportionate and therefore proposed not to be retained by the SE Inquiry on data retention

Telephone services and messaging

i) Communications that are not connected via a mobile access point

Fixed telephony (not ip-telephony)

1. calling number;
2. called number and number to which the call is directed;
3. data on calling and called subscribers and, where applicable, registred user;
4. date and time at the beginning and end of the communication;
5. data on used service or services.

Fixed ip-telephony

1. calling number;
2. called number and number to which the call is directed;
3. data on calling and called subscribers and, where applicable, registered user;
4. date and time at the beginning and end of the communication;
5. data on used service or services.
6. caller and calleds ip-addresses;

7. date and time for log on and log off of the service or services used;
8. data that identify the equipment that finally secluded the communication from the service provider to the subscriber;
9. data that identify the equipment from which the communication is secluded by the CSP (retention obligation) to the one who finally (no retention obligation) secludes the communication to the individual subscriber.

Messaging
1. senders and recipients number, ip-address or other address for a message;
2. data on sending and receiving subscriber and, where applicable, registered user;
3. date and time for log on and log off of the service or services used;
4. date and time for sending and receiving message;
5. data on used service or services.

ii) Communications that are connected via a mobile access point

Mobile telephony (not ip-telephony)
1. number to which the call has been directed from the calling number;
2. data on used service or services**.**

Mobile ip-telephony
1. number to which the call has been directed from the calling number;
2. data on used service or services;
3. caller and calleds ip-addresses;
4. date and time for log on and log off of the service or services used;
5. data that identify the equipment that finally secluded the communication from the service provider to the subscriber;
6. data that identify the equipment from which the communication is secluded by the CSP (retention obligation) to the one who finally (no retention obligation) secludes the communication to the individual subscriber.

Mobile messaging

1. date and time for log on and log off of the service or services used;
2. data on used service or services.

Internet access

Type of capacity for transmission

UK

Thank you for the opportunity to submit comments prior to the FOP DAPIX working group meetings.

Our primary suggestion for the agenda is exploring the mechanism by which formal recommendations are made to the Telecoms group about amendments to the e-Privacy Regulation.

- It would also be useful to talk about the appropriate level of security that should attach the retained data, as a one-size-fits-all approach will unlikely be the solution.
- We would furthermore be interested in looking at the risks of data retention being too limited in its scope (i.e. limiting to geographic location or a certain type of people).
- We would also be interested in discussing the merits of a data preservation power to enhance data retention. This power could be done in various ways but would see law enforcement require CSPs to preserve data on criminal targets at the earliest opportunity. We would be interested to exchange views on the point at which this became data retention.