Council of the European Union
General Secretariat

Brussels, 15 September 2017

WK 9374/2017 REV 1

LIMITE

JAI
COPEN
DAPIX
ENFOPOL
CYBER

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Contributions by delegations

Delegations will find in Annex contributions by AT, BG, DE, PL, SK, IE, NL, UK, PT, BE, CZ, HU, IT and Europol submitted following the latest DAPIX - FoP meeting of 17 July 2017.

REPUBLIC OF AUSTRIA
FEDERAL MINISTRY OF JUSTICE

BMJ-S884.067/0011-IV 3/2017

Museumstraße 7
1070 Vienna
Austria
phone: +43 1 52152 302753
e-mail: post@bmj.gv.at

Official in Charge:
Mag. Dascha Uljanov, LL.M.(WU)

Re: FoP DAPIX - written contributions by the Austrian delegation on data retention

Dear Presidency!

Following the invitation to provide written contributions, the Austrian delegation would like to make the following comments on the questions in the doc. 11107/17 on the topic of data retention and the draft e-Privacy Regulation.

1) *Delegations are invited to exchange preliminary views on possible solutions for ensuring the availability of data in the context of the e-Privacy regulatory framework. What are the relevant aspects that should be considered to that end?*

We have serious concerns about the incorporation of provisions on data retention in the scope of the e-Privacy Regulation.
In our opinion such a complex issue as data retention demands a broad and wide-ranging discussion; therefore this subject should be dealt with in a separate legal act. From our point of view any exception to the confidentiality of data should only be possible when strictly necessary and should furthermore be interpreted strictly, namely as required by applicable ECJ case law (Tele2Sverige, C- 203/15; C-698/15).
While the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight. Such (national) provisions cannot be justified by the use of the opening clause (Article 11 of the draft e-Privacy Regulation).

2) For the purposes of the prevention and prosecution of crime, to what extent can competent authorities rely on traffic and location data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services? Would these data be sufficient to respond to the operational needs of competent authorities for the purposes of the prevention and prosecution of crime?

From a criminal-investigation-point of view, traffic and location data that are processed for billing purposes can be a valuable source for successful investigations. However, it should be born in mind that retention periods for billing purposes can differ (depending on the individual provider and depending on contractual arrangements – particularly flat rate arrangements). Furthermore, it should be noted, that data that is processed and retained for billing purposes does not thoroughly cover data necessary for various investigation purposes (problem of retention of dynamic IP-addresses and source ports especially when Carrier-grade NAT techniques are being used or flat rate arrangements are in place).

3) Given the growing market position of OTTs could it be concluded that the amount of data that would be processed upon consent of the end-user is exponentially growing? If law enforcement authorities were permitted to access the latter under specific conditions, would it be relevant for the purposes of fighting crime?

The conclusion appears to be logically consistent and could be further explored, especially with regard to the provisions on the designation of a representative in the Union (Article 3 of the draft ePrivacy Regulation).

Finally, we would like to use this opportunity to thank you for the structural analyses and focused approach to the multi-layered topic of data retention.

Vienna, 04. September 2017
On behalf of the Minister:
Mag. Carmen Prior

Signed electronically

Comments of the Bulgarian DPA on
processing and storage of data in the context of the draft ePrivacy Regulation
(FoP DAPIX – Data Retention)

1) Delegations are invited to exchange preliminary views on possible solutions for ensuring the availability of data in the context of the e-Privacy regulatory framework. What are the relevant aspects that should be considered to that end?

The Commission for Personal Data Protection as Bulgarian DPA supports the adoption of an EU legislative act on data retention for national security and law enforcement purposes. Such approach could guarantee a common set of legal safeguards and standards for personal data protection across the Union.

The introduction of legal provisions on data retention in the draft ePrivacy Regulation would have its advantages as well as some challenges:

Advantages:

- Regulation is directly applicable in all Member States and thus there will be no divergent legal regimes at national level;
- The draft ePrivacy Regulation is already under discussions in the preparatory bodies of the Council and there will be no need to wait for a new legislative proposal from the European Commission.

Challenges:

- According to the settled case law of the European Court of Justice, the legislative measures of the Union should in principle be based on a single legal basis. Furthermore, combining the legal basis for adoption of acts on data protection (Article 16 TFEU) with a legal basis on fight against serious crime from Title V "Area of Freedom, Security and Justice" of TFEU could cause confusion and contraction.
- The draft ePrivacy Regulation is part of the wider legislative package with new rules on data protection, consisting also of the GDPR and Directive 2016/681 (Police Directive). The latest discussions at political and expert level on data retention show that reaching an agreement on common EU rules would be a long and difficult process. In this context, there is a risk for significantly delaying the adoption of the ePrivacy Regulation.

2) For the purposes of the prevention and prosecution of crime, to what extent can competent authorities rely on traffic and location data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services? Would these data be sufficient to respond to the operational needs of competent authorities for the purposes of the prevention and prosecution of crime?

Pursuant to Article 6, para. 4 of GDPR, further processing of personal data for a purpose other than that for which the personal data have been originally collected, has to be based on the data subject's consent or on a Union or Member State law. In addition, further processing has to constitute a necessary and proportionate measure in a democratic society and has to be accompanied by a comprehensive set of efficient safeguards protecting the privacy and other fundamental rights of the individual.

3) Given the growing market position of OTTs could it be concluded that the amount of data that would be processed upon consent of the end-user is exponentially growing? If law enforcement authorities were permitted to access the latter under specific conditions, would it be relevant for the purposes of fighting crime?

The possible relevance of OTT data has to be decided by the competent law enforcement and judicial authorities. As a general rule, the same privacy and data protection safeguards should apply with regard to access and processing of OTT services data.

4) Could pseudonymisation of traffic and location data meet the requirements of protection of personal data and confidentiality of communications? Would a system permitting their 'depseudonymisation ' under certain conditions for the purpose of fighting serious crime be compatible with EU Law?

The GDPR encourages the use of pseudonymisation as a tool for enhancing security and protection of personal data. Hence, it would be appropriate in the context of traffic/location data retention as well. However, pseudonymisation alone is not sufficient to ensure protection of personal data and confidentiality of communications and has to be supplemented with other relevant technical and organisational measures.

Data retention in the context of E-Privacy Regulation–statement by Germany

In light of the request of the Presidency to provide for a written contribution regarding the issue of data retention in the context of the e-Privacy Regulation, we would like to discuss the relationship between Article 2 and Article 11 of the e-Privacy Regulation draft:

We would like to question whether the obligations of providers relating to the activities of competent authorities referred to in Article 2 (2) – especially those 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 – should be dealt with within the e-Privacy Regulation itself, i.e. within Article 11.

Reference is made to a written statement submitted be GER to the Presidency in the context of the negotiations regarding the e-Privacy Regulation:

The statement argues that necessary supportive action taken by operators of electronic communication networks and services in relation to activities referred to in Article 2 (2) of the draft should be excluded from the e-Privacy Regulation's scope (rather than being subject to an exemption in Article 11).

GER would be interested to exchange views with other Member States on such an exclusion in relation to retention obligations. In any case, it seems preferable to avoid overloading negotiations regarding the e-Privacy Regulation, which shall apply from Mai 2018, with the complex issue of mandatory data retention and the corresponding requirements defined by the Court in its Tele2 judgment.

Targeted data retention –statement by the German Federal Police Office

As announced in the previous session, please find enclosed a written statement of the German Federal Police Office on the geographical requirement in response to question **III. 2** in document 9558/17 and:

I. On specific practical points in the fight against crime

Imposing geographical limitations on minimum retention periods for traffic data (IP addresses and telephone connection data) in advance does not make sense in practical terms in the fight against crime. This is above all because authorities do not tend to know in advance where crime – especially "serious criminal offences", which were also the focus of the original EU Data Retention Directive – might be committed. Even well-known crime hotspots change and move at irregular intervals.
Although, due to a whole range of primarily sociological factors, higher levels of crime are generally seen in major cities, geographical limitations on the retention of traffic data are not tenable from a practitioner's perspective. Once they are known, such limitations could potentially result in displacement, with professionally run criminal structures (terrorist organisations, organised crime) shifting from urban to rural areas.

Furthermore, in threat prevention and criminal prosecution, the majority of police situations are geographically dynamic, and police work would be severely limited if, for example, a criminal's mobile telephone had registered with a mast "excluded" from the retention requirement and access could not be gained to traffic data related to the offence after the fact.

Furthermore, the dissemination of child pornography and (online) child sex abuse are not only encountered in all groups in society: In geographical terms too, the entire territory of the Federal Republic of Germany is a potential crime scene. In this area of crime, no regional hotspots could be determined in advance.

There are both technological and criminological reasons why cybercrime, above all, can hardly be narrowed down to specific geographical areas. Apart from the various methods of obfuscation that can be used, criminals are not tied to local infrastructure (e.g. with regard to opportunities to commit criminal offences, logistics, procuring the means used to commit the offence). In this connection, a temporary limitation on the storage of traffic data, as detailed in the judgment of the Federal Constitutional Court of 2 March 2010 and in accordance *mutatis mutandis* with the new legal situation applicable in Germany, would appear far better suited to limiting the level of interference with fundamental rights entailed in (blanket yet purpose-specific) data retention.

The assumption that regional criminality hotspots exist for Internet-related offices (investigative approach: IP address of the connection used) or that these could be established through a process of analysis is unrealistic. The single criterion for the commission of criminal offences of this sort is access to the Internet. Since Internet access throughout Germany, including the full-scale roll out of high-speed Internet (particularly in rural areas), is an explicit component of Federal Government and EU policy, this criterion is already in place and the possibilities will continue to grow with greater coverage. Restricted data retention combined with greater opportunities to commit offences will undoubtedly make law enforcement and threat prevention more difficult, if not impossible.

The minimum retention periods in operation as of 1 July 2017 (section 113a et seqq. of the Telecommunications Act – *Telekommunikationsgesetz*, TKG) are specifically designed, in the case of volatile data, to allow a telephone number/IP address to be matched up to a subscriber and/or prove that a communications connection existed at a later date. However, if no data was stored by the provider in a certain geographical area or at a certain time, criminal offences could no longer be solved, or gaps in investigative work would make solving them considerably more difficult. Given the special quality that terrorism has among criminal offences, a conscious reduction in the tools available for prosecution and

threat prevention outside major cities and metropolitan areas would also not be seen as justifiable in social and political terms.

Furthermore, a geographical limitation on data retention makes poor sense from a case-management perspective in the search for fugitives and other persons. That the whereabouts of a person sought is unknown and that those conducting the search mostly cannot even begin to narrow down the person's location is part of the very nature of a search. It is not possible to stipulate a search region in advance as a trigger for data retention.

II. On specific technical points

There are also a number of technical reasons as to why geographical, and even temporal, limitations are not necessarily possible without further arrangements in place:

In the case of IP addresses, regional limitations on data retention are often impossible to implement at the access-provider end: This is because a (dynamic) IP address can be assigned to a customer in Mainz at point "X" in time, and to a customer in Cologne at point "Y" in time. Regional limitations are therefore *de facto* impossible.

Furthermore, the companies required to retain the data would also very likely perceive a geographical limitation for minimum traffic data retention periods as lacking in feasibility from a systems perspective. After all, geographical limitation criteria, as set out in the ECJ judgment, would pose major technical challenges for the companies (network providers) required to store the data (e.g. due to the use of virtual telephone numbers, VoIP or dynamic IP addresses, etc.). The structures in place at each network would have to be reviewed to establish whether geographical separation is already an option, and, if not, considerable adjustments would be required in order to make this technically possible.

Furthermore, it appears that, at certain times, depending on network use, several (alternating) cells/masts might be used to handle communications in a specific geographical location. This factor would also have to be considered by the companies under obligation to retain data if cells/masts are used as the connecting factor in determining whether individual communications are covered by a geographically restricted retention obligation.

PL contribution following the request of the Presidency at the DAPIX-FoP meeting on data retention of 17 July 2017

1. PL supports the intention of the PRES to analyze the issue of data retention also in light of the draft ePrivacy Regulation which might offer possibilities to address some of the challenges identified so far by the FoP DAPIX – data retention. PL is of the opinion that the provisions of the draft ePrivacy Regulation should guarantee the protection of the security and public order as well as the protection of the consumer rights. These values often take precedence over the right to privacy and therefore the provisions of the proposed Regulation should first of all enable the legal protection of these values.
2. Please find below PL comments on the specific issues connected to the draft ePrivacy Regulation. These comments are included also in doc. WK 8697/2017 of 18.08.2017 circulated within the WP on Telecommunications and Information Society (H.05).
   In order to protect the interests of consumers art.7 para 3 should be obligatory, i.e. it should include an obligation to store the data for this length of time. Although we are aware that different Member States may have different data retention periods, in our opinion data should be stored for at least 12 months. In the preamble to the regulation, however, it should be noted that this period does not harmonize the minimum periods laid down by national law in which the invoice can be challenged but is a practical safeguard for consumer allowing them to make claims when they have experienced a problem.

   Poland proposes that the Regulation (e.g. in the preamble) expressly provides for the admissibility of national regulations governing the storage and use of data in criminal proceedings or for other purposes related to public or national security.

   We have some concerns about the inclusion of the criterion of proportionality in Art. 11. The principle of proportionality itself is unmistakable. However, this provision relates to the relationship of national provisions to the regulation that entrepreneurs will need to comply with. This may provide grounds for private parties to question the provisions of public law.

3. As regards possible approaches to the data retention, we propose also to look at this issue from the perspective of safeguarding the rights of the ends-users (consumers). Generally, they don't have a possibility to retain and secure data that documents ways and scope of their use of electronic communications services. They have to rely on systems designed by service providers for billing and payment purposes. At the same time, there are no common standards as regards the scope and retention periods of this kind of information. This issue is left for the decision of the service providers whose main purpose is to protect their economic interests. As an example, service providers don't have to store data on the location or the exact time of providing of electronic communications service. As a result, it may constitute a significant limitation for the consumers to assert claims connected for example with the lack or limited quality of service or the way payment is calculated. The problem describe above concerns all forms of electronic services, not only electronic communications services (including OTT).
   It has to be underlined that at the time being the period of retention of data by the electronic service providers and sometimes the scope of data (in the absence of regulations concerning this issue) exceed the requirements of data retention for the law enforcement purposes. This data should be subject to the general evidence rules, as information held by the witness.

In many cases, the ability of law enforcement authorities to access this data is sufficient to carry out their duties connected with investigating crimes.

For these reasons regulating the scope of data and theirs retention period by electronic service providers would foster the consumer/end-users rights at the same time safeguarding in the basic terms the legitimate needs of the law enforcement authorities.

4. In relation to the outcomes of the discussions of FoP DAPIX – data retention, PL acknowledges that the issue of data retention (and the applicability of the Tele2 judgement) in the context of national security demands clarification having in mind exclusive competences of the Member States in this area as described in the Treaties (Article 4 par. 2 TEU).
5. As regards the question of the usefulness of location and traffic data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services it has to be pointed out that there are certain operational limitations for example as regards the processing of location data for the payment purposes. In this circumstances locating the device is limited only to situation when the user initiate the connection. In addition, the use of the electronic services (OTT, VoIP, VoLTE, VoWiFi) takes place in the framework of data packages granted to the users.
As a consequence, the data processed for the payment purposes doesn't reflect the actual way the device is used.

Contribution of Slovakia to the discussions on data retention

I. General remarks

1. Distinguish between data retention and data freezing more consistently in the discussion

The data freezing and data retention are much confused in the discussion. We understand data retention as situations when data from the past are continuously retained *ex lege*. Such continuously retained data can subsequently, in duly justified cases and based on an individual decision, be provided to law enforcement authorities and courts. Data freezing should cover situations when based on an individual decision of a judicial authority, data are preserved towards the future.

2. *Improve communication strategy in relation to general public and internet service providers*

Doing a comparison with the 4AML Directive, it is apparent that the legislation concerning obligation to preserve particular types of data for a specific period (5 years) was adopted in the context of preventing banking institutions from being abused for criminal activities, thus protecting both banks and their clients.

It can be said that this goal is not questioned today and accepted by both, the public and the banking sector. Thus, there exists/ a "social contract" on basis of which some privacy interventions as well as increased administrative burden are accepted. Such public perception/understanding would also need to be achieved when data is stored by providers of electronic communications services for criminal law purposes.

The public awareness and knowledge about state interference justified by the protection of national security is often times wrongly confused with the activities of law enforcement agencies. It is essential, within the communication strategy, to clearly distinguish between the activities of entities providing protection to national security (the intelligence agencies) and the law enforcement agencies' tasks which request data only when the interests protected by (criminal) law were violated. At the same time, it should be noted that neither the CJEU judgments nor the GDPR are applicable to the area of information obtained by the intelligence agencies, as this is not an area governed by EU law. Obstacles to the activities of law enforcement agencies do not prevent the collection of data by intelligence services, but prevent the state from prosecuting perpetrators and protecting the rights of citizens / victims of cybercrime.

Due to the fact that our partners are entities of public market, they have market behaviour, it is evident that they are interested to take only those steps, in which their clients (service users) will be interested in or which will be directed to protecting their business / financial interests.

Therefore, we should try to convince the public (clients) that without the cooperation of service providers and without recognizing the need to retain certain types of data, users of electronic services cannot be (effectively) protected against the cybercrime. Alternatively, we should identify areas where the telecommunications sector may be interested in increasing protection.

Fulfilling this part will not be an easy task. There are entities already today which are presenting on the market non-cooperation with law enforcement authorities as their advantage over other market participants. It is therefore in the interest of the competent authorities to set obligations, so that non-cooperating entities do not have a market advantage.

The principle of protection of users´ security is already proposed in the draft e-Privacy Regulation (Article 6 / 1.b, text proposed below).

3. *The problem is not in terms of access to data but in the extent and time of storage*

The previous and ongoing debate has confirmed that the conditions for access to data as required by the jurisprudence of the CJEU are not problematic and those conditions for data freezing and for access to data are now widely respected. It is, however, problematic to take account of the requirements of the jurisprudence (in particular Tele2 Sverige, Digital Rights Ireland) on the scope and conditions for the retention of data, since they do not allow general data retention. Any other alternatives represent either more significant interference with fundamental rights or lead to the situation that data are not available to law enforcement authorities. The requirements of the jurisprudence are based on a lack of distinction between data retention and data freezing and do not take into account the reality of the technical solutions or the needs of the law enforcement authorities. If a certain data is not preserved, it cannot be used in the investigation because it does not exist.

The data that should have originally be retained, as stipulated by annulled Directive 2006/24 / EC on Data Retention (Article 5),[1] supplemented by NAT (Network Address Translation), are considered by the Slovak law enforcement authorities as essential data for conducting an effective investigation / prosecution. These data correspond to the definition of so-called metadata from the draft E-Privacy Regulation (Article 4), though categorisation of dynamic IP address is questionable. It would be useful to know if the overall perception among Member States is identical or not, e.g. a common perception of categories of data to be retained for criminal law purposes should be defined.
Based on preliminary consultations with Slovak service providers and the study of the general terms and conditions of some operators, it appears that the scope of data retained by service providers (i.e. for the purposes of accounting, complaints and marketing purposes) corresponds to traffic data and partially location data under the annulled Data retention directive. The range of data from the so-called “detailed bill” is considerably narrower and limited to some traffic and some location data only.

The biggest issue seems to be the absence of IP address and NAT. The absence of a uniform retention period in practice leads to situations where connection data (and IP address) are sometimes available to some operators for only a few days.

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

It follows from this that the declared scope of data retained by service providers is narrower than the basic range of data identified by Slovak authorities as necessary to conduct an effective investigation. Therefore, there is a question of the need and the possibility of extending the reasons for the mandatory retention of the data also for the additional "security" reason or the reason for the prevention of abuse and the unusual use of services respectively. This is a concept that some service providers are already working with, it only needs to be extended to law enforcement authorities' needs.

To ensure a verifiable identification of the client / service user in the shortest possible time is most important for the Slovak law enforcement authorities. From the type of data stored it is clear that the declared data retained by the service providers could provide this essential requirement, provided that it is confirmed that IP address and NAT will be between these data.

The data retention period is the subject of jurisprudence only for the purpose of assessing proportionality. If we look at the current situation in practice, service providers keep different types of data for different periods. This time is in the range of hours, days to years. For example, for a service complaint on billing purposes, this period, depending on the operator, is in the Slovak Republic ranging from 30 days for the duration of the contractual relationship to at least 4 years after termination of the contractual relationship. Law enforcement authorities cannot therefore be sure that the data needed to identify the person will be available again. Therefore, it is also necessary to set a common minimum length of data storage (e. g. at least 6 months). Most authorizations to process individual types of client data are still linked to the duration of the contractual relationship.

Therefore, it is necessary to provide for the obligation to keep all necessary data for the agreed time period. This obligation should be set out in law.

4. Solutions in relation to new technologies

Current framework which is (as it is stated above) perceived as inadequate in relation to the performance of the role of law enforcement and judicial authorities, does not take into account the increasingly frequent use of encryption and various forms of anonymization, which serve to improve the security of legal services and communications and to protect perpetrators of crime. These issues should therefore also be a matter of interest and legislative adjustment at EU level.

II. Specific suggestions on the draft E-Privacy Regulation

1. Article 3

In line with recitals 8 and 9 of the draft E-Privacy Regulation, it is proposed in the legislative part to amend Article 3 so that every Over-the-top ("OTT") content provider would be obliged to have a representative in the EU. At the same time, it is proposed to modify the possibility of imposing a sanction in accordance with the conditions laid down in the GDPR in the event of non-appointment of such a representative in the EU.

It will be necessary to address in the related discussions the issue of the modalities of cooperation in providing evidence for criminal proceedings and the enforceability of a sanction imposed under the GDPR.

Justification: given that the real providers of the most widespread services are OTTs which have their headquarters outside the EU, they must be subjected to the effective supervision by the European institutions, thereby ensuring the enforcement of rights and obligations.

2. Art. *6, para. 1, letter b in connection to the recital*

It is proposed to amend Article 6, para. 1, letter b) so that the requirement to maintain the security of electronic communications networks and services is extended to the need to maintain the safety of their users. Therefore, we propose to amend the letter b) for example in the following wording: "it is necessary to maintain or restore the security of electronic communications networks and services and its users, or ...". The provision could be complemented by a recital that would interpret / justify the content of the safety requirement, e.g. by the need to prevent the misuse of services and the unusual or unlawful use of services for the purpose of criminal activity. A similar concept is also known to providers of electronic communications services, but is limited to the context of network abuse by clients, e. g. in terms of the benefits of network calling, etc.

Justification: It appears that the data retained by the service providers (i.e., invoicing, complaints and, eventually, marketing) does not cover all the basic needs of the law enforcement authorities and the social contract mentioned above. At the same time, greater emphasis should also be placed on the security aspect of the client (user) in the use of electronic communications services, especially the Internet, before being abused for committing illegal activities, including criminal activity. Particularly sensitive and undesirable are cases of such serious crime as child pornography or grooming which, due to the absence of data retention, remain uninvestigated and their perpetrators unpunished. This is all the more true in cases of greater need to increase the protection of clients / users' privacy against unauthorized data collection and processing by both service operators and the public authorities / bodies in general, in particular by using anonymized communication programs or services

3. *Article 6, para. 2, letter b) in connection to recital*

It is proposed to consider extending the wording of letter b) also to the unusual use of electronic communications services (the wording: "(...) or stopping abusive, abusive, or unusual usage of, ..."). This extension would need to be supplemented by an interpretative recital. Abusive and unusual or unauthorized use of services should be possible to interpret not only in the technical but also in the investigative/criminal sense for instance on the basis of the identified behavioural characteristics of the illegal behaviour in the given area.

Justification: please see above.

4. *Interpretation of Art. 11*

SK understands Article 11 of the Directive as an option (whether nationally or coordinated at EU level) to provide for exceptions / derogations from the generally regulated rules in the E-Privacy Regulation. However, those legislative adjustments will have to respect the general conditions set out in Art. 11 of the Regulation and, of course, to take account the jurisprudence of CJEU.

Article 11 should not be interpreted only as a possibility to modify access to data, since the jurisprudence of the CJEU does not a priori prohibit regulation in the field of data retention, it sets "only" its terms. The problem lies precisely in the nature, partial ambiguity and strictness of these conditions. Strict compliance with these conditions in principle leads to a substantial reduction in the effectiveness and success of the conduct of criminal investigations / criminal prosecutions.

A similar approach has been chosen by the legislator already in the past. The Annulled Data Retention Directive was also adopted with reference to the derogations contained in Article 15 of Directive 2002/58 / EC on privacy and electronic communications (abbreviated) and Article 13 (1) of Directive EP / 46 / EHS on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

III. Political/Legislative Possibilities

1. SK considers it appropriate to use the possibility of improving the current situation following the repeal of the Directive on the retention of data, by amendment(s) and extension of certain obligations in the draft E- Privacy Regulation. However, this does not seem to be a definitive and satisfactory solution.
   At the same time, it is clear that the solution cannot be found in the proposal for this regulation only and it is also necessary to explore the possibilities in discussions related to the Electronic Communications Code (e. g. by adjusting the scope of the data necessary for billing purposes, possibly adding a new reason - the reason for the security of clients to establish the obligation (of ISPs) to store IP addresses and NAT in Internet communication.

   If we were limited to "indirect" solutions in the E-Privacy Regulation or other supplementary legislative instruments in the field of electronic communications services at EU level, it would be necessary to complete these solutions by the national regulation.

2. At the same time, SK supports the continuation of the discussion in order to examine in greater detail the conditions for the retention of data in accordance with the jurisprudence of the CJEU. The jurisprudence of the CJEU allows States to retain data on a targeted approach. An *approach, based on the behavioural characteristics of unlawful or unusual actions that may lead to criminal activity*, is used e.g. by the 4 AML Directive.[2] In the context of data retention, for example, behavioural characteristics of customers could be examined to identify unusual and / or typical suspicious behaviours (clients) in serious crimes (grooming, child pornography, etc.). If we were able to identify such characteristics, this could be in line with the Court's requirement for targeted data retention. Consequently, it could be envisaged to introduce an obligation to report to law enforcement authorities any unusual / risky behaviour of clients in the use of electronic communication services. For example, consideration may be given to evaluating the use of anonymization services, or the creation and subsequent use of tools for such an approach.
3. We support the discussions also in the context of future reflections on the possible adoption of a common European instrument.

[2] 4 AML Directive regulates the targeted retention of data based on behavioural characteristics typical of a certain criminal activity. The result is, for example, a regulation of to the obligation to report and store suspicious bank transaction data above a certain figure.

4. We understand the adoption of common guidelines for data retention as an additional / backup measure. Their added value in any case will be limited. In the case of impossibility or when adoption of a common European legislative solution would be unrealistic, such guidelines should contain the premises for the national solutions in view to ensure that differences between MS are minimized. The guidelines oriented on exchange of experiences would probably not provide much added value taking into account the number of activities at the level of the police authorities, given also the differences in national legislation.

IV. Conclusions

- It seems appropriate to distinguish more consistently between data retention and data freezing (bases and solutions are not identical) in future discussions.
- The communication strategy needs to be changed in relation to the public
- Adopt (complementary) solutions in the E-Privacy Regulation: address the concept of security of the client
- Clearly define applicable law from the perspective of data protection, e.g. that data retention is out of the application of GDPR
- Study/consider the behavioural characteristics of clients in order to identify their unusual or unlawful behaviour
- Establish the obligation to keep data for a set minimum time
  - these data should contain the necessary minimum data necessary for the efficient conduct of the investigation
  - in practice, this should include the extension of previously collected and stored data by the IP address and NAT data
- Define a common perception of categories of data to be retained for criminal law purposes
- Consider the possibility of adopting a separate European instrument

AN ROINN DLÍ AGUS CIRT AGUS COMHIONANNAIS

DEPARTMENT OF JUSTICE AND EQUALITY

DAPIX Friends of Presidency on Data Retention

1107/2017: Processing and storage of data in the context of the draft ePrivacy Regulation = Introduction and preliminary exchange of views

---

Ireland Delegation Comments

1) **Delegations are invited to exchange preliminary views on possible solutions for ensuring the availability of data in the context of the e-Privacy regulatory framework. What are the relevant aspects that should be considered to that end?**

Ideally a solution for ensuring the continued availability of data could be found at EU level and this may be possible through the draft e-Privacy Regulation; this would ensure consistency of approach across Member States. Ireland would also be supportive of the proposed engagement with the Communications Working Group on the draft Regulation in this regard.

2) **For the purposes of the prevention and prosecution of crime, to what extent can competent authorities rely on traffic and location data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services? Would these data be sufficient to respond to the operational needs of competent authorities for the purposes of the prevention and prosecution of crime?**

Traffic and location data processed in this manner could be useful to competent authorities in the context of the prevention and prosecution of crime. However, it is not clear that all providers maintain consistent or comparative datasets in terms of substance and/or duration for these purposes. This means that this base of data would be of limited and inconsistent use to the competent authorities. It may be helpful to seek to ascertain the length of time these data are retained for business purposes by communications services providers in order to establish whether and where there is consistency across providers. This would then allow the Friends of Presidency group establish the context in which to explore the issue further.

3) **Given the growing market position of OTTs[3] could it be concluded that the amount of data that would be processed upon consent of the end-user is exponentially growing? If law enforcement authorities were permitted to access the latter under specific conditions, would it be relevant for the purposes of fighting crime?**

It is clear that day to day communications are migrating towards OTT services. As such, Ireland would be supportive of identifying means for law enforcement authorities to access such data for the purposes of fighting crime and consistent with EU law.

4) **Could pseudonymisation of traffic and location data meet the requirements of protection of personal data and confidentiality of communications? Would a system permitting their 'depseudonymisation ' under certain conditions for the purpose of fighting serious crime be compatible with EU Law?[4]**

This is an area that Ireland considers worthwhile to explore. Of itself, pseudonymisation would be unlikely to satisfy the requirements of the Tele2 judgment, however as one of a range or matrix of measures it could possibly lead towards a solution that would be compatible with the judgment.

---

3 Due to the still increasing popularity of smartphones as well as the growing availability of stable mobile broadband services, a study funded by the European Parliament estimates that the usage of OTT communication services will continue to increase significantly in the coming years and would end up reaching a share of 90% of the total messaging market in 2020.

4 These issues will be further considered in light of the ECJ Opinion on the EU-Canada PNR agreement expected on 26 July 2017.

Document 11107/17 (Processing and storage of data in the context of the draft ePrivacy Regulation), contribution by the Netherlands

In light of the request of the Presidency to provide for a written contribution in response to the questions in document 11107/17, please find enclosed a contribution by the Netherlands.

1) Delegations are invited to exchange preliminary views on possible solutions for ensuring the availability of data in the context of the e-Privacy regulatory framework. What are the relevant aspects that should be considered to that end?

We would like to propose to discuss and scrutinize the suggestions made by the EU Counter Terrorism Coordinator (CTC) as presented during the Informal JHA Council in July. The idea of the CTC, as we have understood it, was to look into the structure of the e-privacy regulation as a whole, to balance data retention and protection of confidentiality in a different way, so as to allow more flexibility for exceptions regarding storage of data.

2) For the purposes of the prevention and prosecution of crime, to what extent can competent authorities rely on traffic and location data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services ? Would these data be sufficient to respond to the operational needs of competent authorities for the purposes of the prevention and prosecution of crime?

At the moment, in the Netherlands we have no data retention legislation in force after a national court declared the legislative act implementing the Data Retention Directive to be invalid following the ruling of the European Court of Justice in the case Digital Rights Ireland. Law enforcement currently has to rely on the traffic and location data which electronic communication services have available for billing purposes. These data are considered not to be sufficient to respond to the operational needs of law enforcement. The same applies for the Intelligence and Security services. The available data are too limited in type of data and retention period. Furthermore, the differences between electronic communication services hamper the effectiveness of investigations. We would also like to point out a development towards a decreasing need for electronic communication services to retain data for some time for billing purposes (f.i. because of the increased use of call and internet bundles).

The observation that the data available for billing purposes is too limited is also made in the report published by the Public Prosecution's Office and the Police on the importance of the retention of communication data for the investigation and prosecution of serious crime, which we submitted to the FoP before.

3) Given the growing market position of OTTs could it be concluded that the amount of data that would be processed upon consent of the end-user is exponentially growing? If law enforcement authorities were permitted to access the latter under specific conditions, would it be relevant for the purposes of fighting crime?

We can answer these questions in the affirmative.

We would like to use this opportunity to state that we subscribe to the fact that the increasing use of so-called Over-The-Top services brings new challenges for law enforcement agencies, which in our view should, separately, also be discussed at EU level.

4) Could pseudonymisation of traffic and location data meet the requirements of protection of personal data and confidentiality of communications? Would a system permitting their 'depseudonymisation ' under certain conditions for the purpose of fighting serious crime be compatible with EU Law?

We consider the suggestions of some Member States to look at the possibilities for pseudonymization to be an interesting avenue to explore and are open to further discuss this, but we have no experiences to share in the context of dataretention.

UK proposals for possible solutions to ensuring the availability of communications data in context of the e-Privacy regulatory framework

This document responds to the Presidency's invitation to Member States who see different possibilities to address the issue of data retention in the context of the draft e-Privacy Regulation to present their ideas in writing to the Friends of the Presidency Group on Data Retention for in-depth analysis at our September meeting. It represents proposals for discussion and should not be considered to reflect the UKs finalised position.

1. The UK welcomes the opportunity to exchange views on possible solutions for ensuring the availability of communications data in the context of the e-Privacy regulatory framework.

2. As we noted at the Friends of the Presidency meeting on Data Retention on 17 July the UK intelligence community is currently subject to a legal challenge on the lawfulness of certain data acquisition powers for national security purposes. A significant part of this challenge relates to the extent to which, if any, the safeguards detailed in the Tele2 judgment apply to such powers in the light of Article 4(2) of the Treaty of the European Union, and it therefore has the potential to impact upon the use of such powers by Member States for national security purposes.

3. The UK Investigatory Powers Tribunal (IPT) has indicated that it will make a preliminary reference to the Court of Justice of the European Union (CJEU) in this case. We await further court hearings in September and possibly October which should confirm the terms and timing of the reference.[5]

4. We understand that our Member States partners have already expended significant effort to produce vital proposals which can assist the group in its aim to mitigate the impact of the Tele2 judgment on the retention of communications data for the purpose of prevention or detection of serious crime. We look forward to considering those proposals.

5. While that should be the primary purpose of any amendments to the draft e-Privacy Regulation, we also consider it to be critical to try and limit any possibility that the CJEU may seek to limit retention of or access to communications data (as well as other crucial investigatory powers), where the purpose those powers are used for is not in scope of EU law. In the interests of burden sharing we have therefore focussed our efforts on this analysis, based on the understanding we have generated from observations in our ongoing litigation.

National security and e-Privacy

6. The current e-Privacy Directive and the draft e-Privacy Regulation lack clarity regarding the extent to which they seek to regulate activity undertaken for national security purposes and we consider that this should be addressed through amendments to the draft e-Privacy Regulation. This would also make the proposal consistent with the approach set out in the General Data Protection Regulation (Regulation 2016/679).

[5] We would be happy to discuss in further detail the proposed application of the Tele2 judgment to this case with Member States where required.

7. The main confusion concerns:
    a. ***The interaction between Articles 1(3) and 15(1) of the existing e-Privacy Directive, replicated in the current draft of the e-Privacy Regulation at Articles 2 and 11***. This is because it is not sufficiently clear whether the drafting of Article 1(3) aims to place activity undertaken for purposes of national security outside the scope of the directive, in accordance with Article 4(2) of the Treaty of the European Union, **or** whether it is intended that it remains in scope but that Member States can derogate from some of the requirements of the directive where activity is undertaken for the purpose of national security, as provided for by Article 15(1). The Tele2 judgment tries to reconcile why some matters are referred to in Article 1(3) and 15(1) but, significantly, states the structure does 'not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose.' This could be interpreted as meaning that national security, despite being referenced by 1(3), is still in scope of the directive. **However, we consider that the original drafting intention was that such activity was out of scope of the directive. This intention also reflects the approach in Article 2(2)(a), read with recital (16), of the General Data Protection Regulation. This repeats the position set out previously in the Data Protection Directive (95/46/EC).** Our proposed amendments to Article 2, Article 11 and Recital 26 of the draft Regulation addressing this issue are in paragraph 9 below.

    b. ***The scope of the national security exemption. We consider any processing which communications service providers are required to do for national security purposes falls within the exemption. Consequently, such processing is outside the scope of the proposed Regulation.*** We consider that where a communications service provider processes data for national security purposes (as required by a Member State) then that processing is outside the scope of EU law. . The amendments suggested below are intended to cover this as well.

8. In light of the above we believe it is necessary to clarify these elements in the draft e-Privacy Regulation and make the following proposals for the Group's consideration[6].

<u>Clarifying the relationship between Articles 2 and 11 in the draft e-Privacy Regulation</u>

9. In order to clarify the relationship between articles 2 and 11 in the draft e-Privacy Regulation to ensure that activity undertaken for the purpose of national security is outside its scope, we propose the following amendments:

    a. Add a new recital using the text from recital 16 of the General Data Protection Regulation:

This Regulation does not apply to issues of protection of fundamental rights and freedoms related to activities which fall outside the scope of Union law, such as activities concerning national security.

[6] Texts relied upon in these proposals which are not fully reproduced in the body of analysis can be found at Annex A

b. Amend article 2(2)(a) of the draft e-Privacy Regulation, to specify that national security is an activity which falls outside the scope of Union law.

Article 2 (2)

This Regulation does not apply to:

(a) activities outside the scope of Union law, **such as activities concerning national security**;
(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;
(c) electronic communication services which are not publically available;
(d) activities of competent authorities for the purpose 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.

c. Amend Article 11(1) by removing the reference to the interests listed in Art 23(1)(a)-(e) of the General Data Protection Regulation (GDPR), directly inserting the specified grounds for derogation but excluding the reference to national security. This means that the only reference to national security is in Art 2(2)(a) and a new recital to make it clear that it is out of scope.

Article 11 (1) 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 **following** general public interests ~~**referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679**~~:

defence;

public security;

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;

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, including monetary, budgetary and taxation matters, public health and social security; or

a monitoring, inspection or regulatory function connected to the exercise of official authority for ~~such~~ **these** interests.

d. Amend recital 26 of the draft e-Privacy Regulation to reflect the change to Article 11(1) proposed above.

Recital 26 – UK proposal

When 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).

10. We welcome thoughts from Member States on these proposals or other means to reconcile articles 1(3) and 15(1) of the directive.

ANNEX A

General Data Protection Regulation (Regulation 2016/479)

Article 2 This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law

Recital 16: This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union

E-Privacy Directive (Directive 2002/58/EC)

Article 1(3): This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Recital (11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Article 15: Application of certain provisions of Directive 95/46/EC

Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1)

Relevant paragraphs of CJEU judgment in C-698/15 Tele2 (our underlining)

71. Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, 'legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 [of that directive]'. The second sentence of Article 15(1) of that directive identifies, as an example of measures that may thus be adopted by Member States, measures 'providing for the retention of data'.

72. Admittedly, the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 51). Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive.

73. However, having regard to the general structure of Directive 2002/58, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.

74. Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services. Accordingly, Article 15(1), read together with Article 3 of that directive, must be interpreted as meaning that such legislative measures fall within the scope of that directive.

75. The scope of that directive extends, in particular, to a legislative measure, such as that at issue in the main proceedings, that requires such providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data.

76. The scope of that directive also extends to a legislative measure relating, as in the main proceedings, to the access of the national authorities to the data retained by the providers of electronic communications services.

77. The protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including 'any data related to such communications', in order to protect the confidentiality of electronic communications.

78. In those circumstances, a legislative measure whereby a Member State, on the basis of Article 15(1) of Directive 2002/58, requires providers of electronic communications services, for the purposes set out in that provision, to grant national authorities, on the conditions laid down in such a measure, access to the data retained by those providers, concerns the processing of personal data by those providers, and that processing falls within the scope of that directive.

79. Further, since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services.

80. That interpretation is confirmed by Article 15(1b) of Directive 2002/58, which provides that providers are to establish internal procedures for responding to requests for access to users' personal data, based on provisions of national law adopted pursuant to Article 15(1) of that directive.

81. It follows from the foregoing that national legislation, such as that at issue in the main proceedings in Cases C-203/15 and C-698/15, falls within the scope of Directive 2002/58.

PORTUGAL

1) Delegations are invited to exchange preliminary views on possible solutions for ensuring the availability of data in the context of the e-Privacy regulatory framework. What are the relevant aspects that should be considered to that end?

Portugal is of the opinion, following the invalidation of Directive 2006/24/EC, that the Commission should propose a new instrument on the retention of data by telecommunications operators, not agreeing with the addition, in the e-privacy proposal for a regulation, of rules on data retention, especially as such regulation will apply to telecommunications companies while the subject of retention concerns the authorities with criminal jurisdiction. In addition, the e-privacy proposal for a regulation, as drafted, already allows for exceptional regimes such as data retention (see Article 11 of the proposal).

However, if it is considered essential to add to the e-privacy proposal for a regulation rules on data retention, it is important to establish, on this regard, what requirements are to be laid down by national legislation, not only with regard to access and use by competent authorities, but mainly as regards the conservation criteria that should govern the obligation imposed on the telecommunication operators.

It should be noted that in order to comply with the case-law of the CJEU, conservation must be selective, i.e. only for the purpose of combating serious crime, limited to what is strictly necessary for the categories of data retained, the media, persons targeted and the duration of conservation, with sufficient guarantees, concerning suspects and objective circumstances, with prior control of a court or other independent entity, by providing information to the persons concerned and destroying the data after the necessary period, which only shall be kept within the territory of the Union.

2) For the purposes of the prevention and prosecution of crime, to what extent can competent authorities rely on traffic and location data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services? Would these data be sufficient to respond to the operational needs of competent authorities for the purposes of the prevention and prosecution of crime?

Relevant data for criminal purposes relate to the communication (source, destination, date, time, duration and type), the equipment and location of the equipment.

3) Given the growing market position of OTTs could it be concluded that the amount of data that would be processed upon consent of the end-user is exponentially growing? If law enforcement authorities were permitted to access the latter under specific conditions, would it be relevant for the purposes of fighting crime?

Yes, OTT data are also relevant for criminal purposes.

4) Could pseudonymisation of traffic and location data meet the requirements of protection of personal data and confidentiality of communications? Would a system permitting their 'depseudonymisation ' under certain conditions for the purpose of fighting serious crime be compatible with EU Law?

Pseudonymisation is a measure of data protection under the General Data Protection Regulation. The re-identification of data subject to pseudonymisation may be authorized for criminal purposes.

Releasable to Council Working Party on Information Exchange and Data Protection (DAPIX) Friends of Presidency

The Hague, 30 August 2017

EDOC# 909633v11

Releasable to Council Working Party on Information Exchange and Data Protection (DAPIX) Friends of Presidency

Data retention in the context of the ePrivacy Regulation

Contribution from Europol

The purpose of this document is to point out the importance of European legislation taking data retention for law enforcement purposes into account. Furthermore, this contribution seeks to inspire further discussion by providing an additional solution approach to the pending questions in the Council's Working Party on Information Exchange and Data Protection (DAPIX). In that regard, it will be shown that not only targeted data retention is permitted based on the *Tele2 ruling*[7].

The document makes reference to Europol's contribution to the DAPIX Friends of Presidency discussion of 15 May 2017 "Data categories to be retained for law enforcement purposes"[8] and the Working Party's latest discussion of 17 July 2017.

Contents

[7] Judgement of the Court of Justice of the EU *Tele2 and Watson* of 21.12.2016 in joined Cases C-203/15 and C-698/15 (following: *Tele2*).
[8] EDOC# 895573v9.

1. Relationship between ePrivacy Regulation and data retention

The Presidency requested preliminary views on possible solutions for ensuring the availability of data for law enforcement purposes in the context of the ePrivacy Regulation (question (1) of Presidency's note of 12 July 2017).[9]

There is an essential need to incorporate explicit data retention rules for law enforcement purposes into the upcoming ePrivacy Regulation or another suitable European legislative act. Not only the protection of personal data but also the protection of public security interests through the fight against terrorism and serious crime must be determined as a specific purpose.

The lack of such legislation at EU level firstly leads to an unnecessarily fragmented data retention framework in Europe.[10] Secondly, and even more importantly, the current – as well as the envisaged – EU ePrivacy framework prevent Member States from adopting broader data retention measures.

Whereas *Digital Rights* seemed to allow some room for manoeuvre for (general) data retention legislation, *Tele2* was multiply interpreted as "unequivocally stat[ing] blanket data retention measures incompatible with EU law, read in light of the Charter."[11] It will be shown that this statement is based on a misunderstanding of the Court's jurisdiction and misses an important difference between *Digital Rights* and *Tele2*.

1.1. Stricter criteria in Tele2

Indeed, the criteria established by the Court in its *Digital Rights ruling*[12] restrict the scope of data retention not as far as the criteria set in *Tele2*.

For instance, the Court stresses in the latter for the first time that storage of data must not become the rule[13]. Moreover, the Court did not take the right to security (Article 6 of the Charter) into consideration and thus deviated from *Digital Rights,*[14] but also from the recent *PNR Canada Opinion.*[15]

Finally, only in *Tele2* the Court ruled general and indiscriminate retention of data *per se* unlawful, irrespective of how high the safeguards considering storage safety and access might be. In contrast, in *Digital Rights* the Court did not clarify whether every detected deficit (regarding retention, storage and access) by itself or only their cumulative effect made the underlying data retention framework not proportional.[16]

1.2. *Tele2* criteria do not necessarily derive from the Charter

To frame the legal significance of the various criteria set out by the Court in *Digital Rights* and *Tele2* correctly, it is important to determine their legal source. Some of them may derive directly from EU primary law (in particular the Charter); others may only derive from the system put in place by EU secondary law (Directions and Regulations). This legal distinction is essential, because the former criteria are constitutional and therefore not easily modifiable by

[9] Council DOC 11107/17.

[10] Cf. *Xavier Tracol*, The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: The need for a harmonised legal framework on the retention of data at EU level, Computer Law & Security Review 33 (2017), 541, 551.

[11] *Orla Lynskey*, Tele2 Sverige AB and Watson et al: Continuity and Radical Change, http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/.

[12] Judgement of the Court of Justice of the EU *Digital Rights Ireland* of 8.4.2014 in joint Cases C-293/12 and C-594/12 (following: *Digital Rights*).

[13] *Tele2*, para. 89.

[14] Cf. Digital Rights, para. 42.

[15] Opinion of the Court of Justice of the EU *PNR agreement between Canada and the EU* of 26.7.2017 in Opinion 1/15 (following: *PNR Canada*), para. 149.

[16] Even the Court's Advocate General interpreted *Digital Rights* in his *Tele2 Opinion* as not precluding general and indiscriminative data retention as such, as long as additional safeguards to protect the stored data against misuse were implemented and the access by public authorities was restricted in accordance with the Court's postulations (Vid. Opinion of Advocate General *Saugmandsgaard Øe* in Tele2 and Watson of 19.7.2016 in joined Cases C-203/15 and C-698/15, para. 199, 262).

the ordinary legislator ("hard criteria"), whereas the latter can be altered by the European legislator ("soft criteria").

To figure out whether the *Digital Rights* and *Tele2* criteria are to be categorised as hard or soft, the different background of these cases has to be taken into account.

In *Digital Rights* the question brought in front of the Court concerned the lawfulness of EU secondary legislation, namely the Data Retention Directive. To answer this question, the Court had to examine the compatibility of the Data Retention Directive (only) with EU primary law, and ultimately declared it to be invalid because of exceeding the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter. Thus, the criteria for lawful data retention set by the Court in this judgement all have to be seen as enshrined in the Charter itself. They all are therefore "hard criteria", binding and not at the disposal of the European or Member States legislators unless the Charter itself would be altered - which is not the intention.

The situation is different as regards the criteria established in *Tele2.* In contrast to *Digital Rights*, this ruling concerned the lawfulness of Member States' legislation in light of EU law. The Court had to examine the compliance of national retention regimes with the Charter, but moreover its compliance with EU secondary law, in particular with the (changeable) data protection framework provided by the ePrivacy Directive.

In this regard, the Court's wording is clear only in the fact that "Article 15(1) of Directive 2002/58, read in light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted" in a certain way.[17] This shows, that the stricter criteria set by the Court in *Tele2* are not necessarily enshrined in the Charter itself, but may only arise from the structure of the ePrivacy Directive, i.e. the single-sided targeting on data protection without taking law enforcement purposes into account.

Data retention was only designated as an exception in Article 15 of the Directive 2002/58. A similar provision is envisaged as regards Article 11 of the ePrivacy Regulation. Arguably, the European legislator restricts data retention more than required by the Charter. Member States' legislators are then bound respectively.[18]

1.3. Data retention can be "the rule"

The criterion that storage of data must not become the rule[19] does not derive from the Charter itself but is a logical consequence of Article 15 ePrivacy Directive that has been phrased as an exceptional rule. The fundamental rights to privacy and protection of personal data as such do not prevent the regular but proportionate storage of metadata. Neither in its *Digital Rights ruling* nor in its recent *PNR Canada Opinion* the Court stated such a requirement, although both cases concerned the general retention of personal data. Moreover, the Court's wording in *Tele2* is unambiguous in this regards. Merely "the system put in place by [the ePrivacy Directive] requires the retention of data to be the exception."[20]

That leads to the conclusion that the European legislator is free to adopt legislative measures which provide for data retention being the rule rather than the exception to the extent that this is implemented in a way which is necessary and proportionate in order to prevent and combat serious crime and terrorism. The missing consideration of law enforcement purposes in the current – as well as the envisaged – European ePrivacy framework makes broader data retention legislation on Member States' level impossible.

[17] Vid. *Tele2*, para. 112.
[18] Member State's data retention legislations must be in line with EU secondary law (esp. the ePrivacy Directive, but also other data protection legislation) and the Charter. The Court clarified that national data retention legislations fall within the scope of the ePrivacy Directive, cf. *Tele2*, para. 65-81.
[19] *Tele2*, para. 89.
[20] *Tele2*, para. 104.

2. "Restricted data retention" and "targeted data access"

Moreover, the Presidency asked for suggestions for further development of the mind map provided in the Annex to the Presidency's note of 12 July 2017.[21]

In this regard, Europol suggests replacing the term "targeted data retention" by the term "level 1: restricted data retention"; and the term "access conditions" by the term "level 2: targeted data access". This is to provide for a better structured, but also more flexible approach to a possible concept of data retention. The aim is to be compliant with the requirements of the ECJ on the one hand and to meet the practical needs of law enforcement on the other.

2.1. Interference levels

The Court determined in *Digital Rights* and *Tele2*, that general and indiscriminate metadata retention measures interfere in a particularly serious manner with the rights to respect for private life and to the protection of personal data.

Self-evidently, this interference is caused by the access to and the subsequent use of data by national authorities. Besides, and in line with its settled case-law, the Court stresses that also the sole retention of data by private providers causes this interference.[22] The overall "wide-ranging"[23] interference, leading to particularly high justification requirements as regards proportionality, results from the aggregate impact of both, the retention of and the access to the data. Nevertheless, the distinction of the Court criteria between those relating to the *first level* interference (caused by the retention as such) and *second level* interference (caused by access and use) facilitates a constructive discussion.

2.2. Level 1: restricted data retention

As regards the initial retention of metadata, *Tele2* arguably does not only permit targeted data retention, but also restricted data retention. Solely general and indiscriminate data retention is incompatible with current European law.[24] The differentiation between "general", "targeted" and "restricted" data retention and the compatibility of the latter with the ECJ's criteria will be set forth in the following.

2.2.1. Definition of restricted data retention

General data retention pursuant to the ECJ's rulings in *Digital Rights* and *Tele2* is the "general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of communication."[25] On account of its very nature, this retention method does not presuppose any link between the data retained and the objective pursued. Following the Court's judgements, this link is necessary to justify any data retention measure. Although the retention of all communication data would fulfil the needs of law enforcement, the Court stresses its incompatibility with EU law and thus ultimately declares this tool unavailable for criminal investigations.

In contrast, the term *targeted data retention* has been introduced referring to the collection of specific data only if there is relevance for already pending investigations, based on objective evidence. Following this approach, data are stored only if law enforcement authorities can demonstrate their importance in a particular case. The Court states that targeted data

[21] Council DOC 11110/17.
[22] Cf. *Digital Rights*, para 34 f.
[23] Cf. *Digital Rights*, para 37.
[24] As regards EU secondary law, this limitation only pertains invariably if *Tele2* (resp. *Digital Rights*) is read in ways that the Charter itself prevents general data retention on level 1, irrespectively of how high the safeguards on level 2 might be (cf. above 1.1. and 1.2.). This "clarification" is a novelty in *Tele2* and therefore could also be interpreted as coming from the system put in place by the ePrivacy Directive. In fact, *Digital Rights* was prominently interpreted as allowing the compensation of a far-reaching first level interference through provisions reducing the impact of the second level interference by Advocate General *Saugmandsgaard Øe* (vid. above fn. 10).
[25] *Tele2*, para 112.

retention is compatible with EU law.[26] This is undisputable, since even more coercive measures (e.g. access to content of communication, online search, etc.) are legally provided under these circumstances.

In between these two retention schemes the Charter arguably allows for a mediating third approach. It could be described as *restricted data retention*, i.e. the limitation of general data retention to what is strictly necessary by excluding all data that are not even potentially relevant for the purpose of fighting serious crime and terrorism.

Unlike targeted data retention, restricted data retention does not demand predefining data categories as important for criminal investigations and solely collecting these specific data. Operational experience has shown that such classification is impractical in advance, as set forth by Europol in previous contributions. The principle of proportionality and strict necessity cannot require retaining data only on the basis of indeterminate predictions. Restricted data retention merely requires the limitation of retention as far as is possible without losing its crucial value for law enforcement purposes.

2.2.2. Compatibility of restricted data retention with *Tele2*

In the Court's wording, restricted data retention implies the retention of data "in relation to […] a particular time period and/or geographical area and/or a group of persons likely involved […] in a serious crime or persons who could, for other reasons, contribute, through their data retained, to fighting crime".[27] This remarkable diction shows that even if retention measures are limited only in reference to one of these categories, they cannot be considered "general and indiscriminate" anymore.[28] Therefore, they are not prohibited *a priori*, but have to be proven proportionate on a case-by-case basis.

The *Tele2* judgement must not be misinterpreted in providing for targeted retention only. The Court does not determine such a requirement. The relevant passage solely makes clear that targeted data retention is permitted in any case, without exhaustively designating all legally possible ways of non-general data retention.[29]

Restricted data retention preserves the balance between the fundamental rights to data protection and privacy and the right to security through effective law enforcement. It provides the required link to the fight of serious crime based on "objective evidence which makes it possible to identify a public whose data is likely to reveal [at least an indirect] link" with such offences.[30] Depending on the circumstances, data retention could become the rule with this approach, without exceeding the limits of what is strictly necessary.

Also the recent *PNR Canada Opinion* of the Court shows that retention of data without restriction to a particular circle of persons is proportionate, if these restrictions are not possible without rendering the whole measure useless for the pursued purpose. In that case, the Court generally approved the storage of all air passengers' PNR data available (except sensitive personal data) for the purpose of fighting serious crime and terrorism for a limited time period (the time of the air passenger being in Canada). The judgement accepted the lack of differentiations as regards specific data subjects and data categories. It emphasised the existence of "the necessary connection between that data [being retained] and the objective pursued" solely through the limited retention period.[31] Only after the air passengers' departure from abroad this connection discontinues, engendering the need of another "merely indirect connection" to justify further retention.[32]

---

[26] Cf. *Tele2*, para. 108.
[27] *Tele2*, para. 106.
[28] Cf. *Tele2* para. 105 f.: The Court finds in para. 105 that the legislation in question covers general data retention without providing for any exception. In the subsequent paragraph, the Court states several options to avert data retention to be general and indiscriminate. While doing so, it connects the different options grammatically by the conjunctions "and/or". This noticeable diction indicates that not only the accumulation of these restrictions prevent general data retention, but also the alternative restriction in regard to only one of the categories.
29 Cf. Tele2, para. 108: Article 15 of Directive 2002/58 in the light of the Charter "does not prevent" targeted retention, but not solely permits targeted retention.
[30] Cf. *Tele2*, para. 111.
[31] Cf. *PNR Canada*, para. 197.
[32] Cf. *PNR Canada*, para. 205.

2.2.3. Realisation of restricted data retention

Still, the initial retention of metadata must be restricted in some way in order to meet the Court's criteria as regards the first level interference. As mentioned above, such restriction is difficult to achieve without losing the additional value of the whole measure.

However, even a marginal – but reasonable – exclusion of data will arguably provide the required link between the measure and its purpose. As a result, the data retention measure does not already fail the Court's requirements on first level, but has to be proven proportionate on level two.

Consequently, Europol recommends following the "peeling-off" approach, proposed by the Swedish representative at the latest DAPIX meeting, but in ways of singling out data categories not even potentially relevant in order to exclude those from being retained.

In order to facilitate this assessment, as a first step a matrix with different categories of retainable metadata should be developed. The matrix should contain main-categories (e.g. content data, traffic data, location data, subscribers' data) and multi-level sub-categories. Especially the latter differentiation should not only take legal and operational requirements into account, but should mainly focus on the technical capability to spare the initial retention of specific data. In other words, one sub-category should only contain data which can, from technical perspective, be retained in their entirety solely.

As a second step, this matrix should be consulted with relevant Member States' and European authorities concerned with law enforcement operations.

2.3. Level 2: targeted data access

In contrast to the initial retention, the access to the data by the competent law enforcement authorities has indeed to be targeted. According to the Court's rulings, the 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. […] In that regard, access can, as a general rule, be granted […] only to the data of individuals suspected of planning, committing or having committed a serious crime or being implicated in one way or another in such crime."[33]

This ensures the compensation of the far-reaching first level interference, and thereby satisfies the requirement of strict necessity. Strong safeguards and limitation as regards storage, access and use reduce the overall impact of the measure, also by alleviating the "feeling [of the persons concerned] that their private lives are subject of constant surveillance."[34] The latter was one main reason for the Court to assume a "particularly serious" interference of data retention with fundamental rights of the Charter.[35]

Moreover, strict limitations on second level are more feasible from a practical point of view. It can be ensured, that only the specific data actually needed for a definite investigation are revealed. This reduces the impact on individuals to a minimum. On the other hand, law enforcement authorities keep an important tool to prevent serious crime and terrorism.

The Court's criteria as regards storage, access and use are emphasised clearly in *Digital Rights* and *Tele2*. Besides, they are comprehensively illustrated by the mind map provided in the Annex to the Presidency's note of 12 July 2017. With reference to this document, Europol encourages a discussion about possible solutions to limit access to what is strictly necessary and to provide "clear and precise rules […] imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their private data against the risk of misuse."[36]

[33] *Tele 2*, para. 119.
[34] *Digital Rights*, para. 37; cf. *Tele2*, para. 100.
[35] Cf. *Digital Rights*, para. 37; *Tele2*, para. 100.
[36] *Tele2*, para. 109.

3. Conclusion

Only the criteria established by the Court in *Digital Rights* are binding for the European legislator *a priori*. The stricter criteria in *Tele2* only partially derive from the Charter itself; they also partly derive from the wording of Article 15 ePrivacy Directive. If data retention to ensure public security was defined as specific purpose in the upcoming ePrivacy Regulation or another suitable European legislative act and correlating measures were adapted, data retention as a crucial law enforcement tool could be implemented in a proportionate manner living up to the jurisprudence of the ECJ. Hereby, data retention legislation compliant with both the right to privacy and the right to security would be provided.

Secondly, Europol argues that *Digital Rights* and *Tele2* do not only permit targeted data retention at EU level, but also restricted data retention. The latter has to be restricted just as far as it is practically possible without rendering the whole data retention measure useless for the purpose of fighting serious crime and terrorism. By assessing concluded criminal investigations, data categories not even potentially relevant for law enforcement can be detected and subsequently excluded from retention.

Even if this approach provides just a slight reduction of the quantity of data being retained, compliance with the Court's criteria can be ensured by higher safeguards with regard to storage, access and use of the data.

BELGIUM

1. possible solutions for <u>ensuring the availability of data</u> in the context of the e-Privacy regulatory framework - what are the relevant aspects that should be considered to that end?

The proposed e-privacy regulation entails a legal base for providers of electronic communications networks and services to store and process electronic communications data for operational, billing, commercial and security purposes. Although this information is often of value for the prevention and prosecution of crime, it is not deemed sufficient. Furthermore, one of the guiding principles of the proposal for an e-privacy regulation implies that providers should erase or anonymise all metadata when it is no longer needed for the purpose of the transmission of communication. The time frames for commercial or operational purposes do often not correspond with the required time frames to obtain this type of information within a criminal investigation.

We don't think it's feasible to significantly enlarge the number of data to be stored for billing or commercial purposes. In order to ensure the availability of data in for the prevention and prosecution of crime, it is essential to maintain a legal base which allows national and European (!) legislation on obligatory data retention. This restriction remains in line with the settled case-law of the Court of Justice that allows derogations from and limitations on the protection of personal data in so far as is strictly necessary to obtain the objective and in line with the principle of proportionality.

Possible elements that could be further discussed in the context of the e-privacy regulation are the following:

- **Public interest** justifying an exception under article 11 of the e-privacy regulation: In the cases *Digital Rights* and *Tele2,* the Court made an assessment of general data retention schemes in the framework of prevention and prosecution of serious and organised crime. Article 11 of the proposal for an e-privacy regulation lists other public interests, which could maybe justify a broader data retention scheme. We would like to insist on the fact that **consumer protection** should be considered as one of the "general public interests" at stake, allowing competent consumer's protection authorities to fulfil their mission. Therefore, this could be done either by **clarifying** in the recitals that the reference to Article 23.1, a) to e) of the GDPR encompasses consumer protection; or by adding a reference to art. 23.1, h), of the GDPR on monitoring, inspection or regulatory departments. This would ensure a higher availability of data, which could only be acquired within criminal investigations by means of a judicial decision in and individual case. In any case, we deem necessary to extend the reference to article 23, paragraph 1 in its entirety.
- Article 15 of the current e-privacy directive contains an **explicit mention of data retention**, which is no longer in the proposed regulation. The following text is mentioned in the explanatory memorandum of the proposal for an e-privacy directive: '*Member States are free to keep or create national data retention frameworks that provide, inter alia, for targeted retention measures, in so far as such frameworks comply with Union law, taking into account the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and theCharter of Fundamental Rights*'. This idea is nonetheless not incorporated in article 11, nor in recital 26 of the proposal, that gives further information on the restrictions in article 11: '*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'*. This silence in the text could in the future lead to an even stricter interpretation of this article.
- **Types of data** covered: The Courts ruling is limited to traffic and communication data, therefore excluding the least sensitive measure, being subscriber data. The progress report presented to the JHA-ministers in June 2017 (ST 9802/17) stipulates that there seems to be a common understanding that basic subscriber information, e.g. IP address attributed to an user, would not fall within the scope of the Tele 2 Judgment. Should this element be taken into account while looking at the wording of article 11 and/or recital 26 of the proposed regulation?
- **Internal procedures providers**: article 11.2 of the proposal stipulates that providers should establish internal procedures in order to respond to requests for access. It is important to emphasise that the conditions for law enforcement to access this information cannot be dealt with within this instrument without amending the legal base of this instrument. This amendment and the following discussion would have a significant impact on the timeline for the adoption of the e-privacy regulation.

- **Lawfulness of processing**: The question arises whether article 6 on the lawfulness of processing should be complemented by the following ground: 'compliance with a legal obligation'.

2. for the purposes of the prevention and prosecution of crime, to what extent can competent authorities rely on traffic and location data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services ? Would these data be sufficient to respond to the operational needs of competent authorities for the purposes of the prevention and prosecution of crime?

Subscriber, traffic and location data are of particular value for law enforcement authorities, emergency services and security services. Although data processed for billing are often part of the essential information for the prevention and prosecution of crime, it is not deemed sufficient. Our practitioners emphasise that data collected for billing purposes are often incomplete, for example incoming calls are not registered, IP connection data is discarded or location data is not retained (at least for what concern the classical telecommunication providers). Furthermore, the retention period and types of data collected may vary from one ISP to another according to their commercial policy, their business model or billing model (f.e. flat rate that are not anymore linked to the actual use of the telecommunication means by the users).

More transparency on the data held by ISPs could be an interesting option, since this will lead to more legal certainty for citizens and practitioners. This should nonetheless be completed with broader data retention scheme.

3. Given the growing market position of OTTs could it be concluded that the amount of data that would be processed upon consent of the end-user is exponentially growing? If law enforcement authorities were permitted to access the latter under specific conditions, would it be relevant for the purposes of fighting crime?

OTTs log an exponential high number of data purely for commercial reasons. Access to those data would certainly be relevant for criminal purposes and efforts should be made to alleviate existing obstacles. Although a lot of these companies are located outside the European Union, they are offering services worldwide and, more important, they are often active within the Member States of the EU. Since they are not European companies, an important number of them does not feel obliged to execute warrants issued by a local judicial authority. Some OTTs are nonetheless willing to execute these warrants on a voluntary base, other companies require a MLA request. The negative effects (time-consuming, lack of legal certainty, important differences between OTTs) and the possible ways to address these issues are being discussed within the e-evidence group.

The direct cooperation between local authorities and OTTs is an important link in the chain to obtain crucial information for investigations. This should be accompanied by other measures ensuring the availability of information.

4. Could pseudonymisation of traffic and location data meet the requirements of protection of personal data and confidentiality of communications? Would a system permitting their 'depseudonymisation ' under certain conditions for the purpose of fighting serious crime be compatible with EU Law?

Pseudonymisation is indeed a valuable security measure, but we are not convinced it meets all the principle requirements set by the Court of Justice in its Tele2 ruling. In particular, it does not address the issue of targeted retention, pseudonymisation is indeed a valuable additional security feature, as it would prevent any illegal use of the retained data. It could be envisaged that the key (allowing the depseudonymisation) is kept by a third party. The data would then be depseudonymised only in case the access is granted by a judicial authority. Such a system could alleviate some of the critics of the Court but might not address all of them.

5. Other options: limits of the Tele2 ruling

The Court of Justice listed in point 111 of its ruling a number of conditions to be respected by the national legislator. Immediately after the ruling, most Member States discarded these options out of fear of discrimination or being impractical or arbitrary. Given the need of data retention schemes and the lack of proportionate alternatives, we are ready to take a second look at these criteria. We understand certain Member States believe their national legislation to be in conformity with these criteria and we are eager to learn more about their approach. Others states are just reflecting on different options. We find it interesting to explore these options within the working party and analyse possible criteria (f.e. distance from cities or relevant public places), how can these criteria be established (criminological data, etc.), should we look for static or dynamic criteria, etc.

CZECH REPUBLIC

1) Delegations are invited to exchange preliminary views on possible solutions for ensuring the availability of data in the context of the e-Privacy regulatory framework. What are the relevant aspects that should be considered to that end?

In particular, after the ECJ judgment *Tele2*, the topic of data retention has been discussed quite thoroughly at various EU fora. We would like to contribute to the development of practicable solutions that take into account the requirements of law enforcement practice on the one hand and the protection of confidentiality of communications and privacy of users on the other hand.

ePrivacy

The ECJ judgment is based mostly on Articles 5, 6 and 15 of the ePrivacy Directive. These provisions establish confidentiality of communications, limit storage of metadata and provide for exceptions for their different processing in order to combat crime and certain other purposes. The ECJ judgment first observes that while data retention was intended to be an exception, it became a rule (para 104) and then (para 105) elaborates on the lack of differentiation among persons or situations covered by rules adopted pursuant to Article 15(1).

At present, the draft ePrivacy Regulation, intended to replace the ePrivacy Directive, is being considered by the Council bodies. The basic structure of rules applicable to communications and metadata is kept, however. If anything, the draft Regulation contains stronger protections and applies to a wider scope of data. Thus no change of the legal reasoning should be expected in future.

However, given the tendency to extend regulation of ePrivacy to other fields than electronic communications, it may be argued that the list of grounds available for exceptions should be broadened rather than restricted. In particular, the prevention of unauthorized use of electronic telecommunication system, which features in Art. 15(1) of the ePrivacy Directive, should be reintroduced and broadened to cover the abusive use of IT systems.

Cyber security

Directive 2016/1148 could be used as an inspiration. Several groups of regulated entities are recognized, including providers of digital services (search engines, on-line marketplaces, and cloud services, while the latter include e.g email services). The providers of electronic communication services may also be identified as regulated essential services. This Directive already provides for a harmonized Union reference framework for the identification of particularly important IT systems and services in all Member States for the purposes of cyber security.

Cyber crime

While the focus of this Directive is on prevention and on addressing of ongoing security incidents and their immediate impacts, it is our responsibility to provide conditions for combating cybercrime. The last of the prerequisites of a secure environment (prevention, handling of an incident, punishment) is missing; therefore, the general preventive effect of punishment is also missing, weakening, in turn, the preventive efforts.

Digital threats without digital enforcement

The reliance of modern European societies on digital and electronic services, products and platforms will increase even more in the near future. Today, a DNA sequencer may be attacked by modified DNA samples. Tomorrow, brakes in a moving car may be disabled until money is paid. Moreover, the attack may misuse several devices or networks in order to compromise its real target in the long term.

To ensure the cyber security and to prevent cybercrime in the long term requires the European Union to ensure that attacks on important devices and networks are not only made harder and their impacts minimized, but also prosecuted, and their perpetrators punished. As indicated above, the 2016/1148 Directive contains a framework to determine important systems and services which should be protected in particular for the purposes of cyber security.

Therefore, the efforts to address data retention should consider imposing, as a positive obligation, relevant retention requirements on certain persons to ensure security and reliability of these most important systems, and to prevent their abuse as a part of their responsibilities to avoid harm and provide proper service. We believe that the approach taken by the 2016/1148 Directive identifying relevant providers and operators should be taken into account. Due to the possibility of long-term attacks, various attack vectors and global nature of many electronic communications and networks, targeted approach to retention requirements would not be enough to achieve the necessary level of reliability.

The data retained would be accessible to cyber security authorities for the purpose of detection and handling of incidents and, subject to appropriate safeguards and limitations, to other authorities for protection of general public interests referred to in Article 23(1) (a) to (e) of Regulation 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Of course, Article 23(2) of GDPR also calls for appropriate safeguards; we are open to practical suggestions in this regard.

2) For the purposes of the prevention and prosecution of crime, to what extent can competent authorities rely on traffic and location data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services? Would these data be sufficient to respond to the operational needs of competent authorities for the purposes of the prevention and prosecution of crime?

From our experience, it is clear that mere billing data will not be sufficient for the operational needs of the law enforcement. The companies store narrower range of the traffic and location data than that is necessary for operational needs of competent authorities (see the example below). In addition, the data are not retained for six months but mostly for few weeks (sometimes even hours).

Subscriber vs. traffic data – Case of child pornography

During the investigation of a criminal offence of child pornography, the police found out that the perpetrator had distributed child pornography via e-mails.

First step – a request to freemail providers

According to the Czech law, freemail providers are not obligated to retain data. However, the law enforcement may request the data and freemail providers have to provide all the data retained for their own business purposes. Based on this request, all the subscriber data (registration data) and also IP address at signup are being provided. Subscriber data include personal data as stipulated in the contract and also partly traffic data (but only the information referring to the identification of the user and IP address or telephone number).

This first step does not depend on the data retention regulations as freemail providers have to process some data for their own business purpose. Law enforcement can gain important intelligence; on the other hand, it is not sufficient for the identification of the perpetrator.

Second step – user detection, request to Internet service providers

After the detection of IP logs as described in step 1, the police in cooperation with Internet service providers (for home use or for businesses) will find out which user was connected to an e-mail box containing child pornography. Internet service providers have the obligation to retain telecommunication data for six months and provide them to entitled state authorities according to the criminal law. These data are retained only for law enforcement purposes as there is no need to retain them for business purposes. However without these data police cannot effectively investigate the case.

3) Given the growing market position of OTTs could it be concluded that the amount of data that would be processed upon consent of the end-user is exponentially growing? If law enforcement authorities were permitted to access the latter under specific conditions, would it be relevant for the purposes of fighting crime?

Access to these data would be relevant for the purposes of fighting crime. However, it is necessary to solve data retention mechanism itself in the first place.

4) Could pseudonymisation of traffic and location data meet the requirements of protection of personal data and confidentiality of communications? Would a system permitting their "depseudonymisation" under certain conditions for the purpose of fighting serious crime be compatible with EU law?

With regard to this area, we cannot expect that pseudonymisation of traffic and location data could mitigate the actual needs and the impact of data retention on a broader scope. According to the ECJ, it isn´t compatible with the EU legislation providing for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users as regards all means of electronic communication. Pseudonymisation cannot solve the problem of general and indiscriminate retention.

In addition, we have serious doubts whether it is feasible from the technical point of view. A telecommunication company has to retain the data; only these companies can do the *pseudonymisation*.

Another thing is that in the CZ it is the state that has to bear the costs for the retention. We suppose that the expenses for pseudonymisation would also have to be paid to the companies by the state. It would be quite costly and we are not sure if it would help to solve the issue with targeted retention.

Written contribution

by Hungary

on questions of the EE PRES on data retention

Reflections on document ST 11107/2017

1) Delegations are invited to exchange preliminary views on possible solutions for ensuring the availability of data in the context of the e-Privacy regulatory framework. What are the relevant aspects that should be considered to that end?

We do not have any objection against regulating general issues of data retention within the framework of the e-Privacy regulation, the proposal on which was presented by the Commission on 10 January 2017. Advance of this solution is that the draft regulation intends to extend its scope to new communications services including internet-based services enabling inter-personal communications (Over-The-Top communications services, hereinafter referred to as: OTTs), thus it could serve as a uniform framework of regulation for each communication sector. There is clearly a point in providing within this instrument that the set of data processed by service providers – including the ones necessary for the prosecution of crimes – would be available.

The set of data subject to retention obligation should by all means include data, which are generated during the provision of services, enabling criminal investigation authorities to identify the specific user (e.g. user's IP address, registration e-mail, phone number, bank account number or other billing and payment data, location data, list of calls/traffic). As service providers in most cases are resident outside the EU, in order to reach an efficient regulation model, the introduction of a system of sanctions may be considered, which would offer technical means the prevent the provision of services by providers that are unwilling to restore and submit such data to the criminal investigation authorities.

Disadvantage of the concept of the e-Privacy regulation as data retention framework is that the form of regulation – instead of the form of directive – is generally not flexible enough to address requirements elaborated by the case law of the CJEU, and its capability of bridging differences among member states' criminal law systems is questionable. Defining the concept "serious crime" – as the precondition of data retention and access – at an EU level would e.g. restrict member states' interpretation in this respect and different structure of regulation could result in different possibilities of access by authorities in the different member states.

The purpose of prevention and prosecution of serious crime should by all means be laid down in the e-Privacy regulation as a purpose that justifies retention of and access to data processed by the concerned service providers. For the sake of expediency, specific conditions and detailed regulations of data retention and access are to be preserved as a subject to national legislation of member states at the same time. That is why it is hard to imagine that a concept of arranging all relevant aspects of data retention in the e-Privacy regulation would be feasible. We consider the concept, which is followed as well by the current e-Privacy directive, entitling the Union or the member states to restrict the scope of the obligations and rights provided for by the e-Privacy regulation – and thus to regulate the retention of and access to data – through legislative measures and containing a set of general rules defining requirements for such legislative measures, more realistic.

2) For the purposes of the prevention and prosecution of crime, to what extent can competent authorities rely on traffic and location data processed for billing and interconnection payments or for detecting or stopping fraudulent or abusive use of, or for the subscription to, electronic communication services? Would these data be sufficient to respond to the operational needs of competent authorities for the purposes of the prevention and prosecution of crime?

The requirement of necessary and proportionate data retention may concern different data categories by data retention for billing and payment purposes than by that for criminal investigation purposes, even though the data retained often overlap in the two cases. Based on this requirement, the Hungarian regulation provides different authorisation for each different purpose: while data listed in article 157 of Act C of 2003 on electronic communications (hereinafter referred to as Eht.) are retainable for billing and collecting connected fees, for the purpose of criminal investigation, data listed in Article 159/A of Eht. are retainable. Difference between the two set of data may be seen in cases of subscriptions involving tariffs independent of traffic or provide pre-paid service. By these subscriptions, communication data could not be retainable for billing purpose. Data retained – and available – for billing and payment purposes could of course, depending on the information demand, be efficiently used for criminal investigation purposes. However, it is hardly questionable that the criminal investigation purpose differs from data retention by service providers for billing purposes: request for data for criminal investigation purpose presents a wider set of data even when it concerns traffic data stored for billing purposes and extends to traffic data that are irrelevant from billing aspect. We conclude that data available for billing purposes can be useful in specific cases for the purpose of criminal investigation, however, the data retention regime facilitating billing and payments is not capable of satisfying need for information for criminal investigation purposes. (The set and the retention period of and the means of storing data for billing purposes is not in line with criminal prosecution purposes: the databases operated for billing purposes does not include itemised call list containing caller and called numbers, data recording by the service provider is focused on handling complaints of costumers related to communication.)

According to practical experience, the set of data retained by service providers obliged by the current Hungarian legislation as well as the retention period is adequately helping criminal investigation authorities' work, as those enable them to identify the user of the specific service. Some (e.g. Facebook, PayPal) of those OTT service providers, which are not obliged by the national law to retain data, are generally cooperative in providing data, however most of them are unable to provide timely and useful data, thus there is clearly a point in extending data retention obligation to these service providers as well.

3) Given the growing market position of OTTs could it be concluded that the amount of data that would be processed upon consent of the end-user is exponentially growing? If law enforcement authorities were permitted to access the latter under specific conditions, would it be relevant for the purposes of fighting crime?

The market position of OTTs is clearly growing, this statement is correct even without a deeper knowledge necessary to forecast tendencies related to the amount of communication data in social context. Access by authorities to data processed in the framework of OTTs could be of high importance for the interest of criminal investigations. According to general experience, OTTs are in focus of a growing number of criminal procedures. The reason for that is the growing popularity of such services among law abiding members of society on one hand, but on the other hand, the

intentional use of such services by offenders in order to prevent authorities to detect communication related to the crimes committed and thus to avoid prosecution. Introducing data retention obligation for OTTs would certainly contribute to the success of prosecution of crimes and has long time been a challenge to be addressed.

As by OTT services, service providers do not have an insight to the content of communication, obliging them to data retention would force them to transform technical solutions applied by the provision of such services. This obligation would, however, be justified in the interest of protecting society and related rights of citizens as well as of providing fair competition in the market of communications services, with special regard to the fact that the use of OTTs is growing, while the use of traditional communications services that are subject to data retention obligation is decreasing.

Regarding this question by the PRES we note that, it is not quite clear what the term „be processed upon consent of the end-user" means, and what this aspect (consent of the end user) would add to the discussion of this issue. This would need further clarification.

4) Could pseudonymisation of traffic and location data meet the requirements of protection of personal data and confidentiality of communications? Would a system permitting their 'depseudonymisation' under certain conditions for the purpose of fighting serious crime be compatible with EU Law?

We uphold our view[1] explained in the written contributions submitted following the DAPIX FoP meeting held on 29 May 2017. A solution similar to the one foreseen by the PNR Directive, which stipulates that after 6 months within the 5 years' data retention period PNR data should be depersonalised, and after that a re-personalisation is only possible for a restricted set of purposes, may be feasible in the field of data retention as well. When depersonalisation/encryption of data is provided in a similar framework and dissolving that is allowed in a more restricted set of purposes within the original purposes of the data processing, a limiting of access could reduce implications of general data retention, thus in such cases, encryption could mean a real guarantee. If, on this basis, dissolving of encryption of data of a person not concerned by a crime is not allowed, data of this

[1] Not any technical means that disrupt connection between the data and the person concerned, do change the personal nature of data, as long as this connection could be restored. That is the interpretation, on which Section (3) of Paragraph 4 of Act No. CXII of 2011 on information self-determination and freedom of information is based, which stipulates that personal data reserves its very character until its connection with the data subject is restorable.
Temporary encryption of personal data is a question of information security and is not suited to serve as a basis for restriction of the range of data to be retained. When the legislation foresees general retention of data while providing encryption of those, which is later to be dissolved, the data retained concerns the rights of a person the same way as do data stored without the use of encryption.
Attention should be drawn to the fact that there is an EU legislation using a framework of anonym storing of data after a general data retention period, when a more restricted processing of data is allowed until their final deletion. [See Article 12 of the Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, which stipulates that after 6 months within the 5 years' data retention period PNR data should be depersonalised, and after that a re-personalisation is only possible for a restricted set of purposes.]
When depersonalisation/encryption of data is provided in a similar framework and dissolving that is allowed in a more restricted set of purposes within the original purposes of the data processing, a limiting of access could reduce implications of general data retention, thus in such cases, encryption could mean a real guarantee. If, on this basis, dissolving of encryption of data of a person not concerned by a crime is not allowed, data of this person remain anonym in the data retention system, which contributes to a higher level of safeguards.

person remain anonym in the data retention system, which contributes to a higher level of safeguards.

By using pseudonyms, both regulation and the applied technical solution must be perfect, otherwise confidentiality of communication cannot be provided. (Constant use of the same pseudonym for the same data subject may lead to the identification of the person via indirect syllogism following the comparison of communications.) Referring to the analogy of the abovementioned solution applied by the PNR Directive, “pseudonymisation” can only present a higher level of guarantee, if “depseudonymisation” is only possible in a more restricted set of cases within the original data processing purpose.

ITALY'S CONTRIBUTION ON DATA RETENTION IN THE CONTEXT OF E-PRIVACY REGULATORY FRAMEWORK

Italy, in response to the invitation made by the Estonian Presidency during the 17.7.2017 meeting, submits the following contribution on the issue of data retention for criminal investigation purposes in the context of the e-Privacy regulatory framework.

Preliminarily, Italy confirms to attach great importance to data retention regarded as a precious tool in the fight against crime. As pointed out by others Member States and Europol, retained data helps to direct the investigations, link suspects to victims, identify contact and possible co-conspirators, check alibis. There are cases where retained data represents the only possible starting point for investigation. Retained data is in any case a very useful tool, since it allows to discern and corroborate other form of evidence.

In the Italian practice access to retained data for investigative purposes is quite common, especially for crimes such as murders, stalking, cyber-crimes, corruption, terrorism, organized crime, etc.

Accordingly, we strongly support the efforts made by the Estonian Presidency to address deeply and thoroughly the issue of data retention with the goal of finding possible solutions for ensuring the availability of retained data for criminal investigation purposes.

As clarified in the explanatory memorandum annexed to the proposal for the Regulation on Privacy and Electronic Communications, that proposal does not include any specific provision in the field of data retention and leave the Member States free to lay down data retention frameworks in so far as such frameworks comply with the Union law, taking into account the relevant case-law of the Court of Justice. In that regard it seems undoubtedly sensible to explore possible solutions to the data retention issue in the context of the e-Privacy Regulation.

In Tele2 judgment the ECJ stated that: *§108. However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.*

§ 109. 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. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 54 and the case-law cited).

In our opinion the key concepts in the Court statements are the followings: that *the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse* and that the national legislation ensures that a data retention measure *is limited to what is strictly necessary.*

As already pointed out by other Member States during the WG discussions, the need to access specific data related to electronic communications normally arises only after a crime was perpetrated, whereas decision on the retention should be made as soon as the data is generated. Moreover, the type of data to be accessed may differ from case to case depending on the specific circumstances.

So, when decision on retention of data is taken, it is not actually possible to foresee and predict exactly what data, regarding which persons and in relation to which geographical area or period of time law enforcement and prosecutors may need. Thus, a targeted data retention may actually result in a limitation of the potentially crucial contribution that access to electronic data might bring to investigations.

In addition to that, as far as Italy is concerned (but the point is also common to other Member States), a targeted data retention based on a mere geographical criterion would be in contrast with our Constitution (precisely with the principle of non-discrimination).

Since a targeted data retention would actually impair the benefits of retained data for law enforcement, it is possible to argue that data retention as a general measure meets the requirement of strict necessity. In fact, only a data retention as a general measure permits to achieve fully the purposes of prevention, investigation, detection and prosecution of criminal offences.

The problem then is how to reconcile the data retention as a general measure, considered strictly necessary for criminal investigation purposes, with the respect for rights to privacy and data protection.

The interference entailed in the fundamental rights enshrined in article 7 and 8 of the Charter by general retention of traffic and location data could be made less dangerous and serious by applying strong security measures, e.g. by pseudonymisation or other similar techniques, and by providing proper safeguards as regards the access to the retained data.

Pseudonymisation of data to be retained would reduce in fact the interference in privacy and data protection rights, since any identifying characteristics of data will be replaced by a pseudonym, which does not allow the data subject to be directly identified. Thus the risks of a data breach for data subjects will be minimized as well as the possibility to draw up from retained data precise conclusions on the lives of identified persons.

The de-pseudonymisation should take place only in case of access to retained data, necessary to carry out investigations on crimes already perpetrated or about to be perpetrated. The reference to specific events will imply, as a result, a delimitation of the data to be accessed.

Accordingly, the serious interference with privacy and data protection rights that takes place when accessing the retained data will affect specific persons and specific data.

Compliance with the requirements of the Court of Justice about substantive and procedural conditions governing the access of the competent national authorities to the retained data can be provided without the usefulness of data retention being impaired. In that regard access to retained data should be granted under judicial control and in relation to specific investigations.

In conclusion, it is our opinion that a fair balance between privacy and data protection rights on the one hand and fight against crime on the other hand might be secured by distinguishing between the stage of retention of data and the stage of access to retained data and by reinforcing security measures and safeguards as regards both stage taking into account their respective specificity and purposes.

Thus, as far as retention stage is concerned, a preventive selection of data to be retained according to possible criteria such as time periods, groups of people, geographical area, means of electronic communication, etc., would not be practicable without impairing the benefits for criminal investigations. Protection against the risks of misuse of retained data would, instead, be guaranteed by pseudonymisation or other similar techniques and by providing precise substantive and procedural conditions for the access to retained data, such as judicial control and connection with specific investigations.