Council of the European Union

Brussels, 12 July 2017
(OR. en)

11107/17

LIMITE

JAI 677
COPEN 232
DAPIX 252
ENFOPOL 350
CYBER 110
EUROJUST 113
TELECOM 186

NOTE

From:	Presidency
To:	Delegations
Subject:	Processing and storage of data in the context of the draft ePrivacy Regulation = Introduction and preliminary exchange of views

1. Introduction

At the informal meeting of Justice and Home Affairs Ministers in Tallinn on 6-7 July 2017, Ministers confirmed that the DAPIX - Friends of Presidency on Data Retention should examine all legislative and non-legislative options to address the data retention issue, including in the context of the proposed e-Privacy Regulation. The group should evaluate the advantages and disadvantages for different stakeholders of any solution.

A number of delegations have referred to the draft e-Privacy Regulation as one of the possible options to be considered in view of the issues arising from the ECJ case law on data retention[1].To structure the work on this particular issue and before starting discussing specific options, the Presidency would like to proceed with an introduction of the main aspects of e-Privacy framework and to invite a general exchange of views in this respect.

[1] Judgment of the Court of Justice of the EU (Grand Chamber) *"Digital Rights Ireland and Seitlinger and others"* of 8 April 2014 in joined Cases C-293/12 and C-594/12 and Judgment of the Court of Justice of the EU (Grand Chamber) *"Tele 2 and Watson"* of 21 December 2016 in joined Cases C-203/15 and C-698/15

2. Link between Tele 2 judgment and e-Privacy

In the Tele 2 judgement, the Court ruled that Art. 15(1) of the e-Privacy Directive[2] read in light of Art. 7, 8, 11 and Art. 52 (1) of the Charter of Fundamental rights precludes national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communications.

The e-Privacy Directive aims to ensure the confidentiality of communications and as a general rule prohibits storage of communication data without the consent of the user concerned, except under certain conditions prescribed by law. The Court confirms that Art. 15(1) allows Member States to introduce exceptions from the obligation of principle of confidentiality, but since this is a restriction of rights, it takes a strict interpretation of the provision. The Court upheld that *"(t)hat provision cannot, therefore, permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58, to become the rule, if the latter provision is not to be rendered largely meaningless"(paragraph 89).*

3. Commission proposal for an e-Privacy Regulation

On 10 January 2017, the Commission presented a proposal for a Regulation on respect for private life and the protection of personal data in electronic communications (e-Privacy Regulation)[3], aiming to replace the current e-Privacy Directive.

---

2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

3 COM(2017) 10 final of 10.1.2017.

Objective

The proposal aims to provide a high level of privacy and personal data protection for users of electronic communications services and a level playing field for all market players in a rapidly changing technological environment. The draft Regulation aims to ensure consistency with the General Data Protection Regulation (GDPR)[4]. It is *lex specialis* to the GDPR and particularises and complements it as regards electronic communications data that qualify as personal data. All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR.

Key provisions of the proposal

As explained in the proposal, end-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail in favour of functionally equivalent online services, such as Voice over IP, messaging services and web-based e-mail services - over-the-top service providers (OTTs) - e.g. Skype, Gmail, WhatsApp, Facebook, Messenger, Viber, Telegram, Facetime. OTTs provide their services in the form of applications running over the internet access service (hence "over-the-top) and are in general not subject to the current EU telecom rules. In order to ensure an effective and equal protection of end-users when using functionally equivalent services, the proposed Regulation extends the scope of the rules to cover not only traditional telecom operators and internet providers, but also OTTs[5]. It also extends to the services where interpersonal communication is only an 'ancillary' feature, thus covering e.g. gaming apps, where messages could be exchanged.

As regards the territorial scope, the proposed Regulation applies to services provided to end-users in the Union, irrespective of whether the provider is established in the Union. Should that not be the case, the provider shall designate a representative in the Union (Article 3 (2)).

Article 5 maintains the general prohibition of any interference with electronic communications data (content and metadata), including storing of data, except when permitted by the Regulation.

---

4 Regulation (EU) 2016/679

5 The draft ePrivacy Regulation refers to the definition of electronic communication services set forth in the proposal for a Directive establishing the European Electronic Communications Code. That definition encompasses internet access services, services consisting wholly or partly in the conveyance of signals, interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services.

Article 6 lists the situations where processing of communication data is allowed, e.g. to meet quality of service requirements, for billing purposes[6], detecting or stopping fraudulent use of communication services, or upon consent of the end-user for specified purposes[7].

Article 7 requires erasing content and metadata or making it anonymous when no longer needed for the purposes of transmission, but allows keeping it for billing purposes under the conditions of paragraph 3.

Article 8 sets out the grounds for collecting of information from end-users terminal equipment (including cookies) or the collection of information emitted by terminal equipment to enable it to connect to another device (Wi Fi tracking).

Article 11 allows the EU or Member States to legislate on restrictions of the scope of rights and obligations under the regulation that are necessary, appropriate and proportionate to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of the GDPR[8].

---

6 Article 6(2) of the e-Privacy Directive authorises the processing of traffic data for the purposes of subscriber billing and interconnection payments up to the end of the period during which the bill may be lawfully challenged or payment pursued. Article 6(2) (b) and 7(3) of the proposal for a new e-Privacy Regulation maintain in essence the processing of traffic and location, renamed metadata (Article 4(3) (c)),if necessary for billing, calculating interconnection payments, detecting or stopping fraudulent or abusive use of, or subscription to, electronic communications services.

7 Under current legislation, the processing of traffic data for the purpose of marketing electronic communications or for the provision of value added services is permitted to the extent and for the duration necessary for such services or marketing, provided that the subscriber or user concerned has given his prior consent or that the data is made anonymous (Article 6(1) and 6(3) of the e-Privacy Directive). The processing of location data is also permitted for the sole provision of value added services to the extent and for the duration necessary for such services, provided that the subscriber or user concerned has given his prior consent or that the data is made anonymous (Article9 of the e-Privacy Directive). Under the proposal for a new e-Privacy Regulation, operators may process metadata if the end-user has given his consent for one or more specified purpose, including for the provision of specific services to such end-user, provided that the purposes concerned could not be fulfilled by processing information that is made anonymous (Article 6(2)(c)).

8 Article 23 (Restrictions), GDPR
1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
(a)national security;

It should be noted that Article 2(2)(d) excludes from the application of the Regulation the activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

4. Questions to delegations

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?
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?

(b)defence;
(c)public security;
(d)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;
(e)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 a matters, public health and social security;
(f)the protection of judicial independence and judicial proceedings;
(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
(h)a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
(i)the protection of the data subject or the rights and freedoms of others;
(j)the enforcement of civil law claims.

3) Given the growing market position of OTTs[9] 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?
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?[10]

The Presidency invites the Member States who see different possibilities to address the issue of data retention in the context of e-Privacy Regulation, to present their ideas in writing by 4 September 2017 (julia.antonova@mfa.ee and milena.petkova@consilium.europa.eu).

Delegations are also invited to provide suggestions in writing on possible solutions for ensuring the availability of data outside the context of the e-Privacy regulatory framework.

The Presidency intends to start in-depth analysis of the proposed options at the DAPIX FoP meeting in September.

---

9 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.

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