# EDPS COMMENTS ON POSSIBLE PLENARY TEXT ("PPT") ON PROCESSING OF DATA FOR SECURITY PURPOSES: ARTICLE 6(6a)

## I. PPT in a nutshell:

1. Article 6(6a) authorizes legal and physical entities ("entities") to process traffic data for security purposes. The PPT reads as follows: " ***Without prejudice to compliance with the provisions other than Article 7 of Directive 95/46/EC and Article 5 of this Directive,*** traffic data may be processed by ***any natural or legal person with a legitimate interest except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject*** for the purpose of implementing technical measures to ensure the ***network and information*** security, ***as defined by Article 4 (c) of Regulation (EC) 460/2004,*** of a public electronic communication service, a public or private electronic communications network, an information society service or related terminal and electronic communication equipment. Such processing must be restricted to that which is strictly necessary for the purposes of such security activity" (hereinafter "Art 6(6a)").

2. As explained below, the EDPS believes that this provision is unnecessary. However, if adopted, the EDPS suggests that it apply only to data controllers. The current legal framework enables data controllers authorized to process personal data, here traffic data, to outsource the data processing to data processors, in this case security companies. Accordingly, he favours inclusion of a reference to data controllers in Art 6(6a) so as not to preclude the possibility of outsourcing the data processing activities to data processors. He also believes that the Amendment's current wording ***"legitimate interest except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject"*** should be maintained. He proposes a slight modification to the language to address the above points.

## II. How does Article 6(6a) fit within the existing data protection legal framework?

3. The ePrivacy Directive is regarded as a *lex specialis*, complementing the Data Protection Directive ("DP Directive"). Therefore, the provisions of the ePrivacy Directive must fit together (like pieces of a puzzle) with those of the DP Directive.

4. Article 7 of the DP Directive establishes that data controllers may process personal data if they comply with at least one of a list of enumerated legal bases, also referred to as legal grounds.[1] An example of one such legal basis could be a contract between the individual and the data controller[2]. Another such example is Article 7(f), which establishes that data controllers can process personal data if doing so is "*necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data are disclosed, except when such rights are overridden by the interest for fundamental rights and freedoms of the data subject . . . .*" The DP Directive does not specify instances in which processing of personal data would

[1] See also the general provision in Article 6 (2): "*It shall be for the controller to ensure .....*"

[2] For example, if on-line company X sells a product, it will be entitled, because of the contract, to collect some information from the customer, including, name, address and payment related information.

meet this requirement. Instead, determinations are made by data controllers, on a case-by-case basis, often with the agreement of national data protection authorities.

5. The interplay between Article 7(f) of the DP Directive and Art. 6.6(a) of the ePrivacy Directive should be considered. Art. 6.6(a) is an illustration, i.e. an instance, of a set of circumstances under which the requirements of Article 7(f) described above are met. Indeed, by authorising the processing of traffic data to help ensure network and information security, Art. 6.6(a) enables such processing for the purposes of the legitimate interest pursued by the data controller. In other words, processing of traffic data for security purposes is a specification of a data processing operation that complies with Article 7(f) of the DP Directive.

6. ***Is the specification made in* Article 6.6(a) *necessary?*** From a legal point of view, in principle, it is not necessary to establish by law whether a particular type of processing activity, in this case the processing of traffic data for security purposes, meets (or fails to meet) the requirements of 7(f) of the DP Directive. As pointed out above, this assessment is usually made by companies, at implementation level, in consultation with data protection authorities, and where necessary, eventually by the courts. Generally speaking, the EDPS believes that in most cases the processing of traffic data for security purposes will meet the requirements of 7(f) of the DP Directive. **Therefore a legal provision confirming this assessment is in principle unnecessary.** The EDPS understands, however, that security companies desiring legal certainty have requested this Amendment.

## III. Why does Article 6(6a) apply to data controllers?

7. The DP Directive divides the actors who process personal data into "data controllers", i.e. those who determine the purposes and means of the processing and "data processors", i.e. those who carry out processing activities *on behalf of* data controllers, following the *instructions* of the data controller[3].

8. This distinction is very important because *(i)* most of the obligations under the DP Directive must be met by controllers; *(ii)* controllers, rather than processors, are liable for data protection violations and, *(iii)* processors have a more limited role, and in effect, are only supposed to process personal data as directed by controllers. For the reasons described below, Art 6.6(a) should apply only to controllers:

   a) If Art 6.6(a) were to apply to processors or to any other third party, the effect would be that such entities (legal or physical) would be entitled to process personal data, without being subject to many of the other obligations that arise from the data protection legal framework, which primarily apply to data controllers. These processors or third parties would thus be in a situation whereby they would, on the one hand, benefit from having legal grounds authorising the processing of data, but on the other hand, not be subject to the

[3] Typical scenario where this distinction applies is the following: Company X (data controller) entrusts company Z (data processor) to process the pay slips of company X's employees. To this end, company X provides certain data of its employees to company Z, specifying the means and purposes of the processing.

obligations, e.g. data protection safeguards, that apply to any entity that legally processes data as data controller.

b) Because, as described above, Article 6.6(a) is an illustration/instance of Article 7(f)'s application to data controllers, logically, Art 6.6(a) should apply to them.

c) Where a data processor would be acting *on his own* - i.e. not *on behalf of* a data controller - he should himself be considered as a data controller, and if necessary be held responsible for his activities.

9. It may be argued that Art 6.6(a) implicitly applies to controllers (and not to processors) and therefore it is unnecessary to explicitly reference controllers in Art 6.6(a). However, the EDPS believes that the inclusion of this express reference will help avoid any potential misunderstanding. .

**IV. Why doesn't the application of Article 6.6(a) to data controllers prevent the processing of such data by data processors, entrusted by data controllers (case of firewalls)?**

10. It has been suggested that if Art 6.6(a) were to apply only to controllers, such an approach would jeopardise the ability of companies that provide security services (such as firewalls) to hospitals, retailers, IT companies and governments to prevent malicious attacks and secure data. The legal argument put forth under this argument is that the security company would not be a data controller but a data processor and would not benefit from the authorisation to process such data. **This is legally inaccurate.**

11. In the above cases, hospitals, retailers, IT companies and governments would be deemed to be data controllers for the traffic data that needs to be processed for security purposes. Art 6.6(a) effectively authorises them (and not others) to process such data. However, Art 17 of the DP Directive foresees the possibility of data controllers outsourcing the processing of personal data to processors. If data controllers have authorisation to process data for a given purpose, in this case for security purposes, data processors (e.g. security companies) would not need independent authorisation as their authorization derives from that of the data controller on whose behalf they are processing data. In other words, the existing legal framework allows data controllers benefiting from Art 6.6(a) to outsource to data processors (security companies) the activity consisting in processing of traffic data on their behalf. Obviously the contractual arrangements between hospitals, retailers, IT companies and service providers would need to reflect the respective roles played by each party (controller v. processor), as well as their respective rights and obligations.

12. The EDPS believes that Art 6.6(a) should not be read as preventing data processors from processing traffic data on behalf of data controllers. As outlined above, the current legal framework, particularly Art 17 of the DP Directive, provides for this possibility. To avoid any misunderstanding on this point, perhaps Art 6.6(a) could be changed as follows:

> "***Without prejudice to compliance with the provisions other than Article 7 of Directive 95/46/EC and Article 5 of this Directive,*** traffic

data may be processed ***for the legitimate interest of the data controller*** for the purpose of implementing technical measures to ensure the ***network and information*** security, ***as defined by Article 4 (c) of Regulation (EC) 460/2004,*** of a public electronic communication service, a public or private electronic communications network, an information society service or related terminal and electronic communication equipment, ***except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.*** Such processing must be restricted to that which is strictly necessary for the purposes of such security activity"

13. The effects of the above changes are two fold: *(i)* if "*processed by any natural and legal person*" is replaced by "*for the legitimate purpose, pursued by the controller*", it does not call into question the possibility of subcontracting with a data processor and also, *(ii)* by inserting the words "controller", the reference to "any natural or legal person" is redundant.

## V. Why, if adopted, should Article 6.6(a) refer to "*with a legitimate interest except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject*"?

14. The wording "*with a legitimate interest except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject*" sets up a limit to the authorisation of processing of traffic data. This limitation is appropriate because:

a) The processing of traffic data should not be justified if the underlying interests pursued are illegitimate or unlawful.

b) A balance should be struck between the interests of the controller and the rights of individuals. The legitimate interests of the data controller should not prevail over fundamental rights and freedoms of the data subject.

c) Art 7(f) of the DP Directive contains this wording. Because Art 6.6(a) of the ePrivacy Directive is an instance of compliance with Art. 7(f) of the DP Directive, it is appropriate that the same requirements appear in the Amendment.