EUROPEAN DATA PROTECTION SUPERVISOR

PRESS RELEASE

Brussels, Monday 12 January 2009

EDPS second Opinion on ePrivacy Directive review and security breach: privacy safeguards need to be strengthened

On 9 January, the European Data Protection Supervisor (EDPS) adopted an Opinion on the review of the Directive on Privacy and electronic communications, usually referred to as the ePrivacy Directive. This Opinion follows upon a first EDPS Opinion (pdf), as well as Comments (pdf), in which recommendations were made to help ensure that the proposed changes effectively provide for the best possible protection of personal data.

This Second Opinion comes as a response to the Council's Common Position which, on a number of critical points, fails to endorse some of the data protection safeguards proposed by the European Parliament and the European Commission or previously recommended by the EDPS. The recommendations presented in this Opinion aim at streamlining some of the provisions of the Directive, while at the same time ensuring an adequate level of data protection and privacy.

The Opinion particularly focuses on the provisions relating to the setting up of a mandatory **security breach notification system** for which the Supervisor believes there is still some room for improvement.

Peter Hustinx, EDPS, says*: "The full benefits of security breach notification will be best realized if the legal framework is set right from the outset. To this end, the Parliament and the Council will need to meet the challenge of determining the proper standard setting forth the conditions for notification and ensuring that the appropriate processes are put into effect. Citizens will expect such a system to apply not only to their Internet access providers, but also to their on-line banks and on-line pharmacies."*

The Opinion also includes a number of recommendations covering the following issues:

- **scope of application**: the EDPS supports the Parliament's approach to broaden the scope of application of the Directive to include **publicly accessible private networks** in the Community. He recommends to further clarify the types of services that would be covered by the broadened scope;
- **processing of traffic data for security purposes**: the EDPS considers the new article introduced by the Parliament - and maintained by the Council's Common Position and the Commission's Amended Proposal - legitimising the collection of traffic data for security purpose as being unnecessary. In the EDPS view, such a provision may be subject to risk of abuse, especially if adopted in a form that does not include the necessary data protection safeguards;
- **right of action against infringements to the Directive**: the EDPS calls upon the Commission and the Council to endorse the provision introduced by the Parliament that gives the possibility to legal entities, such as consumer associations, to bring legal action against infringements of any provisions of the Directive.

The EDPS is hopeful that, as the review of the Directive continues to make its way through the legislative process, new amendments will be adopted in accordance with the above recommendations with a view to restoring the necessary data protection safeguards.

Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to 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,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

Background

1. On 13 November 2007, the European Commission adopted a Proposal amending, among others, the Directive on privacy and electronic communications, usually referred to as the ePrivacy Directive[1] (hereinafter "**Proposal**" or "**Commission's Proposal**"). On 10 April 2008, the EDPS adopted an Opinion on the Commission's Proposal where he provided recommendations to improve the Proposal in an attempt to help ensure that the proposed

[1] The review of the ePrivacy Directive is part of a broader review process which aimed at the creation of an EU telecoms authority, the review of Directives 2002/21/EC, 2002/19/EC, 2002/20/EC, 2002/22/EC and 2002/58/EC, as well as the review of Regulation (EC) No 2006/2004 (hereinafter altogether "review of the telecom package").

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

changes resulted in the best possible protection of the privacy and personal data of individuals ("**EDPS First Opinion**")[2].

2. The EDPS welcomed the Commission's proposed creation of a mandatory security breach notification system requiring companies to notify individuals when their personal data have been compromised. Furthermore, he also praised the new provision enabling legal persons (*e.g.* consumer associations and Internet service providers) to take action against spammers to further supplement existing tools to fight spam.

3. During the Parliamentary discussions that preceded the European Parliament's first reading, the EDPS provided further advice by issuing comments on selected issues that arose in the reports drafted by the European Parliament committees competent for reviewing the Universal Service[3] and ePrivacy Directives ("**Comments**")[4]. The Comments primarily addressed issues related to the processing of traffic data and the protection of intellectual property rights.

4. On 24 September 2008, the European Parliament ("**EP**") adopted a legislative resolution on the ePrivacy Directive ("**first reading**")[5]. The EDPS viewed positively several of the EP amendments that were adopted following the EDPS Opinion and Comments mentioned above. Among the important changes was the inclusion of information society service providers *(i.e.* companies operating on the Internet) under the scope of the obligation to notify security breaches. The EDPS also welcomed the amendment enabling legal and natural persons to file actions for infringement of any provision of the ePrivacy Directive (not only for violation of the spam provisions as initially proposed by the Commission's Proposal). The Parliament's first reading was followed by the Commission's adoption of an amended proposal on the ePrivacy Directive (hereinafter "**Amended Proposal**")[6].

5. On 27 November 2008, the Council reached a political agreement on a review of rules on the telecoms package, including the ePrivacy Directive, which will become the Council's Common Position ("**Common Position**")[7]. The Common Position will be notified to the EP under Article 251(2) of the Treaty establishing the European Community, which may entail the proposal of amendments by the EP.

Overall views on the Council Position

6. The Council modified essential elements of the text of the Proposal and did not accept many of the amendments adopted by the EP. Whereas the Common Position certainly

---

[2] Opinion of 10 April 2008 on the Proposal for a Directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ C 181, 18.07.2008, p. 1.

[3] Directive 2002/22/EC on universal service and users' rights related to electronic communications networks, (Universal Service Directive), OJ L 108, p. 51.

[4] EDPS Comments on selected issues that arise from the IMCO report on the review of Directive 2002/22/EC (Universal Service) & Directive 2002/58/EC (ePrivacy), 2 September 2008. Available at: www.edps.europa.eu.

[5] European Parliament legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users´ rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD).

[6] Amended proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation (EC) No 2006/2004 on consumer protection cooperation, Brussels, 6.11.2008 COM(2008)723 final.

[7] Available at the public Website of the Council.

contains positive elements, on the whole, the EDPS is concerned about its content, in particular because the Common Position does not incorporate some of the positive amendments proposed by the EP, the Amended Proposal or the opinions of the EDPS and of European Data Protection Authorities issued through the Article 29 Working Party[8].

7. On the contrary, in quite a few cases, provisions in the Amended Proposal and EP amendments, offering safeguards to the citizens, are deleted or substantially weakened. As a result, the level of protection afforded to individuals in the Common Position is substantially weakened. It is for these reasons that the EDPS now issues a Second Opinion, hoping that as the ePrivacy Directive makes its way through the legislative process, new amendments will be adopted that will restore the data protection safeguards.

8. This Second Opinion focuses on some essential concerns and does not repeat all the points made in the EDPS' First Opinion or the Comments, which all remain valid. In particular, this Opinion discusses the following items:

    - The provisions on security breach notification;
    - The scope of application of the ePrivacy Directive to private and publicly accessible private networks;
    - The processing of traffic data for security purposes;
    - The ability of legal persons to take action for infringements of the ePrivacy Directive.

9. In addressing the above issues, this Opinion analyses the Council's Common Position and compares it with the EP first reading and Commission's Amended Proposal. The Opinion includes recommendations aimed at streamlining the provisions of the ePrivacy Directive and ensuring that the Directive continues to adequately protect the privacy and personal data of individuals.

II. THE PROVISIONS ON SECURITY BREACH NOTIFICATION

10. The EDPS supports the adoption of a security breach notification scheme pursuant to which authorities and individuals will be notified when their personal data have been compromised[9]. Notices of security breaches may help individuals take the necessary steps to mitigate any potential damage that results from the compromise. Furthermore, the obligation to send notices informing of security breaches will encourage companies to improve data security and enhance their accountability regarding the personal data for which they are responsible.

11. The Commission's Amended Proposal, the European Parliament's first reading and the Council's Common Position represent three different approaches to security breach notification currently under consideration. Each of the three approaches has positive aspects. However, the EDPS believes there is room for improvement in each of the approaches and advises to take into account the recommendations described below in considering the final steps towards adoption of a security breach scheme.

12. In analyzing the three security breach notification schemes, there are five critical points to consider: *(i)* the definition of security breach; *(ii)* the entities covered by the obligation to

[8] Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), available at the website of the Article 29 Working Party.

[9] This Opinion uses the word "compromised" to refer to any breach of personal data that occurred as a result of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data, transmitted, stored or otherwise processed.

notify ("covered entities"); *(iii)* the standard that triggers the obligation to notify; (*iv*) the identification of the entity responsible for determining whether a security breach meets or fails to meet the standard, and (*v*) the recipients of the notice.

Overview of the Commission, Council and EP approaches

13. The European Parliament, Commission and Council have all adopted varying approaches for notification of security breaches. The EP's first reading modified the original security breach notification scheme set forth in the Commission's Proposal[10]. Under the EP's approach, the obligation to notify applies not only to providers of publicly available electronic communications services but also to information society service providers ("PPECS" and "ISSPs"). Furthermore, under this approach all breaches of personal data would have to be notified to the national regulatory authority or to the competent authorities (together "authorities"). If authorities were to determine that the breach is *serious*, they would require the PPECs and ISSPs to notify the person affected without delay. In case of breaches that represent imminent and direct danger, PPECS and ISSPs would notify individuals before notifying the authorities and not await a regulatory determination. An exception to the obligation to notify consumers covers entities that can demonstrate to the authorities that "*appropriate technical protection measures have been applied*" rendering the data unintelligible to any person who is not authorized to access it.

14. Under the Council's approach, notification also has to be provided to both subscribers and authorities, but only in cases where the *covered entity* deems the breach to represent a *serious risk* to the subscriber's privacy (*i.e.* identity theft or fraud, physical harm, significant humiliation or damage of reputation).

15. The Commission's Amended Proposal maintains the EP's obligation to notify authorities of all breaches. However, in contrast to the EP's approach, the Amended Proposal includes an exception to the notification requirement with respect to individuals concerned where the PPEC demonstrates to the competent authority that *(i)* no harm (*e.g.*, economic loss, social harm or identity theft) is "*reasonably likely*" to occur as a result of the breach or *(ii)* "*appropriate technological protection measures*" have been applied to the data concerned by the breach. Thus, the Commission's approach includes a harm-based analysis in connection with individual notifications.

16. It is important to note that under the EP[11] and Commission approaches it is *the authorities* who are ultimately charged with determining whether the breach is serious or reasonably likely to cause harm. By contrast, under the Council's approach, the decision is left up to the *concerned entities*.

17. Both the Council and Commission's approaches apply only to PPECS, and not, as does the EP approach, to ISSPs.

The definition of security breach

18. The EDPS is pleased to see that the three legislative proposals contain the same definition of security breach notification, which is described as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data, transmitted, stored or otherwise processed [...]* ".[12]

[10] In particular, EP Amendments 187, 124 to 127 as well as 27, 21 and 32 address this issue.
[11] Except in cases of imminent and direct danger in which case covered entities must notify consumers first.
[12] Article 2 (i) of the Common Position and Amended Proposal and Article 3.3 of the EP first reading.

19. As further described below, **this definition is welcome** insofar as it is broad enough to encompass most of the relevant situations in which notification of security breaches might be warranted.

20. First, the definition includes instances when an *unauthorized access* of personal data by a third party has taken place, such as the hacking of a server containing personal data and retrieving such information.

21. Second, this definition would also include situations where there has been a loss or disclosure of personal data, while unauthorized access has yet to be demonstrated. This would include such situations as where the personal data may have been lost (e.g. CD-ROMs, USB drives, or other portable devices), or made publicly available by regular users (employee data file made inadvertently and temporarily available to a publicly accessible area through the Internet). Because there often will be no evidence demonstrating that such data may or may not, at some point in time, be accessed or used by unauthorized third parties, it seems appropriate to include these instances within the scope of the definition. **Therefore, the EDPS recommends maintaining this definition. The EDPS also recommends including the definition of security breach in Article 2 of the ePrivacy Directive, as this would be more consistent with the overall structure of the Directive and provide more clarity.**

Entities that should be covered by the obligation to notify

22. The obligation to notify under the EP approach applies to both PPECS and ISSPs. However, under the Council and Commission schemes, only PPECS such as telecommunication companies and providers of Internet access will be obliged to notify individuals where they suffer security breaches leading to the compromise of personal data. Other sectors of activity, for example, online banks, online retailers, on-line health providers and others are not bound by this obligation. **For the reasons developed below, the EDPS believes that from a public policy perspective it is critical to ensure that information society services which include online businesses, on-line banks, on-line health providers etc. are also covered by the notification requirement.**

23. First, the EDPS notes that although telecom companies are certainly targets of security breaches that warrant a notification obligation, the same is true for other types of companies/providers. On-line retailers, on-line banks, on-line pharmacies are as likely to suffer security breaches as telecom companies, if not more so. Therefore, risk considerations do not weigh in favor of limiting the scope of a breach notification requirement to PPECS. The need for a broader approach is illustrated by other countries' experience. For example, in the United States almost all of the States (more than 40 at this juncture) have enacted laws on security breach notification which have a wider scope of application, encompassing not only PPECS but any entity holding the required personal data.

24. Second, while a breach of the types of personal data regularly processed by PPECS clearly may impact an individual's privacy, the same is true, if not more so, for the types of personal information processed by ISSPs. Certainly banks and other financial institutions may be in possession of highly confidential information (*e.g.* bank account details), the disclosure of which may enable use for identity theft purposes. Also, the disclosure of very sensitive health-related information by on-line health services may be particularly harmful to individuals. Therefore, the types of personal data that may be compromised also call for a wider application of the security breach notification that would, at a minimum, include ISSPs.

25. Some legal issues have been raised against widening the scope of application of this article, *i.e.* the entities covered by this requirement. In particular, the fact that the overall scope of the ePrivacy Directive concerns only PPECS has been put forward as an obstacle to applying the obligation to notify also to ISSPs.

26. In this context, the EDPS would like to remind that: ***(i)*** **There is no legal obstacle whatsoever to include other actors than PPECS in the scope of certain provisions of the directive. The Community legislator has a full discretion in this respect.** ***(ii)*** **There are other precedents in the existing ePrivacy Directive of application to entities other than PPECS.**

27. For example, Article 13 applies not only to PPECS but to any company that sends unsolicited communications, requiring prior opt-in consent to do so. Moreover, Article 5(3) of the ePrivacy Directive, which prohibits *inter alia* the storing of information such as cookies in users' terminal equipment, is binding not only upon PPECS, but also upon anyone who attempts to store information or gain access to information stored in the terminal equipment of individuals. Moreover, in the current legislative process, the Commission has even proposed expanding the application of Article 5(3) when similar technologies (cookies/spyware) are not only delivered through electronic communication systems but through any other possible method (distribution through downloads from the Internet or via external data storage media, such as CD-ROMs, USB sticks, flash drives, etc.). All these elements are welcome and should be kept, but also set relevant precedents for the present discussion on scope.

28. Moreover, in the current legislative process the Commission and EP and arguably the Council, have proposed a new Article 6.6 (a), discussed below, that applies to entities other than PPECS.

29. Finally, taken into account the comprehensive positive elements derived from the obligation to notify security breaches, citizens are very likely to expect these benefits not only when their personal data has been compromised by PPECS but also by ISSPs. Citizens' expectations may not be met if, for example, they are not notified when an on-line bank has lost their bank account information.

30. **In sum, the EDPS is convinced that the full benefits of security breach notification will be better accomplished only if the scope of covered entities includes both PPECS and ISSPs.**

The standard triggering notification

31. Regarding the trigger for the notification, as further explained below, the EDPS is of the view that the Amended Proposal's standard "*reasonably likely to harm*" is the most appropriate of the three proposed standards. However, **it is important to ensure that "harm" is sufficiently wide to cover all relevant instances of negative effects on the privacy or other legitimate interests of individuals. Otherwise, it would be preferable to create a new standard pursuant to which notification would be mandatory "*if the breach is reasonably likely to cause adverse effects to individuals*".**

32. As outlined in the previous section, the conditions under which notification to individuals must be provided (referred to as "the trigger" or "standard") vary under the EP, Commission and Council approaches. Obviously, the volume of notices that individuals will receive will depend, in large part, on the trigger or standard set for notification.

33. Under the Council and Commission schemes, notification has to be provided if the breach represents a "*serious breach to the subscriber's privacy*" (Council) and if "*harm to consumer interest is reasonably likely as a result of the breach*" (Commission). Under the EP scheme, the trigger for the notification to individuals is "*seriousness of the breach*" (*i.e.* notification to individuals is required if the breach is deemed "*serious*"). Notification is not necessary below this threshold[13].

34. The EDPS understands that if personal data have been compromised, it may be argued that individuals to whom the data belong are entitled to know, in all circumstances, about this occurrence. However, it is only fair to ponder whether this is an appropriate solution in the light of other interests and considerations.

35. It has been suggested that an obligation to send notices whenever personal data has been compromised, in other words without any limitations, may lead to over-notification and 'notice fatigue', which could result in desensitization. As further described below, the EDPS is sensitive to this argument; yet, at the same time he wants to stress his concern about over-notification being a possible indicator of a widespread failure of information security practices.

36. As mentioned above, the EDPS sees the potential negative consequences of over-notification and would like to help ensure that the legal framework adopted for security breach notification does not produce this result. If individuals were to receive frequent breach notices even in those situations where there are no adverse effects, harm or distress, we may end up undermining one of the key goals of providing notice as individuals may, ironically, ignore notices in those instances where they may actually need to take steps to protect themselves. Striking the right balance in providing meaningful notice is thus important because, if individuals do not react to notices received, the effectiveness of notification schemes is highly reduced.

37. In order to adopt an appropriate standard that will not lead to over-notification, in addition to considering the trigger for notice, other factors, notably, the definition of security breach and the information covered by the obligation to notify, must be considered. In this regard, the EDPS notes that under the three proposed approaches, the volume of notifications may be high in the light of the broad definition of security breach discussed above. This concern for over-notification is further underscored by the fact that the definition of security breach covers all types of personal data. Although the EDPS considers this to be the correct approach (not limiting the types of personal data subject to notification), as opposed to other approaches such as US laws where the requirements are focused on the sensitivity of the information, it is nevertheless a factor to be taken into account.

38. In the light of the above, and taking into account the different variables considered altogether, the EDPS finds it appropriate to include a threshold or standard below which notification is not mandatory.

39. The standards proposed, *i.e.* the breach represents a "serious *risk to privacy*" or is "*reasonably likely to harm*" both seem to include, for example, social or reputational harm and economic loss. For example, these standards would address instances of exposure to identity theft through the release of non-public identifiers such as passport numbers, as well as the exposure of information about an individual's private life. The EDPS welcomes this approach. He is convinced that the benefits of security breach notification would not be fully achieved if the notification system covered only breaches leading to economic harm.

[13] See footnote 11 regarding the exception to this rule.

40. Of the two proposed standards, the EDPS prefers the Commission's standard "*reasonably likely to cause harm*", because it would provide a more appropriate level of protection to individuals. Breaches are far more likely to qualify for notification if they are "*reasonably likely to cause harm*" to individuals' privacy than if they are to present a "*serious risk*" of such harm. Thus, covering only breaches presenting a serious risk to individuals' privacy would considerably limit the number of breaches that must be notified. Covering only such breaches would give an inordinate amount of discretion to PPECS and ISSPs as to whether notification is required, insofar as it would be much easier for them to justify a conclusion that no "*serious risk*" of harm exists than that no harm is "*reasonably likely to occur*". While over-notification is surely to be avoided, on balance the benefit of the doubt must be given to protecting individuals' privacy interests, and individuals should be protected at the very least when a breach is reasonably likely to cause them harm. Moreover, the term "*reasonably likely*" will be more effective in practice, both for covered entities and competent authorities, as it requires an objective evaluation of the case and its relevant context.

41. Furthermore, breaches of personal data may cause harm which is difficult to quantify and which may differ. Indeed, the disclosure of the same type of data, depending of the individual circumstances, may cause significant harm to one individual and less to another. A standard that would require the harm to be material, significant or serious would not be appropriate. For example, the Council's approach, which requires that the breach *seriously* affects someone's privacy, would provide inadequate protection to individuals insofar as such standard requires the effect on privacy to be "serious". This also gives scope for a subjective evaluation.

42. While as described above "*reasonably likely to harm*" seems to be a suitable standard for security breach notification, the EDPS nevertheless remains concerned that it may not include all of the situations where notification to individuals is warranted, *i.e.* all situations where negative effects for the privacy or other legitimate rights of individuals are reasonably likely. For this reason a standard could be considered that would require notification "*if the breach is reasonably likely to cause adverse effects to individuals*".

43. This alternative standard has the additional benefit of consistency with EU data protection legislation. Indeed, the Data Protection Directive refers often to adverse affects upon the rights and freedoms of data subjects. For example, Article 18 and Recital 49 which deal with the obligation to register data processing operations with the data protection authorities authorize Member States to exempt this obligation in cases where the processing "*is unlikely adversely to affect the rights and freedoms of data subjects*". A similar wording is used in Article 16.6 of the Common Position in order to enable legal persons to file actions against spammers.

44. Furthermore, taking the above into account, one would also expect covered entities and particularly authorities competent to enforce data protection legislation to be more familiar with the above standard and thus facilitate their assessment as to whether a given breach meets the requisite standard.

Entity to determine whether a security breach meets or fails to meet the standard

45. Under the EP approach (except in cases of imminent danger) and Commission's Amended Proposal it will be up to the Member States' authorities to determine whether a security breach meets or fails to meet the standard that triggers the duty to notify individuals concerned.

46. The EDPS believes that the involvement of an authority plays an important role in the determination of whether the standard is met insofar as it is, to some extent, a guarantee for the correct application of the law. Such a system may prevent companies from inappropriately assessing the breach as not harmful/serious and thus avoiding notification when, in fact, such notification is necessary.

47. On the other hand, the EDPS is concerned that a regime whereby authorities are required to carry out the assessment may be impractical and difficult to apply, or may in practice turn out to be counterproductive. It may thus even diminish the data protection safeguards for individuals.

48. Indeed, under such an approach, data protection authorities are likely to be inundated with notifications of security breaches and may face serious difficulties in making the necessary assessments. It is important to remember that in order to make an assessment of whether a breach meets the standard, authorities will have to be provided with sufficient inside information, often of complex technical nature, which they will have to process very quickly. Taking into account the difficulty of the assessment and the fact that some authorities have limited resources, the EDPS fears that it will be very difficult for authorities to comply with this obligation and might take resources away from other important priorities. Furthermore, such a system may put undue pressure upon authorities; indeed, if they decide that the breach is not serious and nevertheless individuals suffer damage, the authorities could potentially be held responsible.

49. The above difficulty is further underscored if one takes into account that time is a key factor in minimising the risks derived from security breaches. Unless the authorities are able to make the assessment within very short time-limits, the additional time required by authorities to make such assessments may increase the damages suffered by concerned individuals. Therefore, this additional step that is meant to provide more protection for individuals may ironically result in offering less protection than systems based on direct notification.

50. **For the above reasons, the EDPS considers that it would be preferable to set up a system whereby it should be up to concerned entities to make the assessment whether the breach meets or fails to meet the standard, as provided in the Council's approach.**

51. However, to avoid risks of possible abuse, for example of entities declining to notify under circumstances where notification clearly is called for, **it is of utmost importance to include certain data protection safeguards described below.**

52. First, the obligation applying to covered entities to make determinations whether they have to notify must of course be accompanied by another obligation requiring the mandatory notification to authorities of all breaches that meet the required standard. Concerned entities should in those cases be required to inform the authorities of the breach and the reasons of their determination regarding the notification and the content of any notification made.

53. Second, authorities must be given a real oversight role. In exercising this role, authorities must be allowed, but not obliged, to investigate the circumstances of the breach and require any remedial action that may be appropriate[14]. This should include not only the notification

[14] Article 15a.3 recognizes this oversight powers by establishing that "*Member States shall ensure that competent national authorities and, where relevant, other national bodies have all investigative powers and resources necessary, including the possibility to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.*"

of individuals (when this has not yet taken place) but also the ability to impose an obligation to undertake a course of action to prevent further breaches. Authorities should be granted effective powers and resources in this regard, and authorities must have the necessary leeway to decide when to react to a notification of security breach. In other words, this would enable authorities to be selective and engage in investigations of, for example, large, truly harmful security breaches, verifying and enforcing compliance with the requirements of the law.

54. In order to achieve the above, in addition to the powers recognised under the ePrivacy Directive such as Article 15.a.3 and Data Protection Directive, the EDPS recommends inserting the following language: "*If the subscriber or individual concerned has not already been notified, the competent national authority, having considered the nature of the breach, may require the PPECS or ISSP to do so*".

55. Furthermore, the EDPS recommends the EP and the Council to confirm the obligation proposed by the EP (Amendment 122, article 4.1.a) for entities to conduct a risk assessment and identification on their systems and the personal data that they intend to process. Based on this obligation, entities shall draw a tailored and accurate definition of the security measures which will be applied in their cases and which should be at the disposal of the authorities. If a security breach occurs, this obligation will help covered entities - and eventually also the authorities in their oversight role - to determine whether the compromise of such information may cause adverse effects or harm to individuals.

56. Third, the obligation applying to covered entities to make determinations regarding whether they have to notify individuals must be accompanied by an obligation to maintain a detailed and comprehensive internal audit trail describing any breaches that have occurred and any notifications thereof as well as any measures undertaken to avoid future breaches. This internal audit trail must be at the authorities' disposal for their review and possible investigation. This will enable authorities to carry out their oversight role. This could be achieved by adopting language along the following lines: "*The PPECS and ISSPs shall keep and maintain comprehensive records detailing all security breaches occurred, relevant technical information related thereto and remedial action taken. Records shall also contain a reference to all notifications issued to subscribers or individuals concerned and to the competent national authorities, including their date and content. The records shall be produced to the competent national authority at its request.*"

57. Of course, in order to ensure consistency in the implementation of this standard as well as other relevant aspects of the security breach framework, such as the format and procedures for the notification, it would be appropriate for the Commission to adopt technical implementing measures, after consultation with the EDPS, the Article 29 Working Party and relevant stakeholders.

Recipients of the notification

58. As to recipients of the notices, **the EDPS prefers the EP's and Commission's terminology over the Council's.** Indeed, the EP has replaced the word "subscribers" with the words "users". The Commission uses "subscribers" and "individual concerned". Both the EP and the Commission language would include as recipients of the notices not only current subscribers but also former subscribers and third parties, such as users who interact with some covered entities without subscribing to them. The EDPS welcomes this approach and calls upon the EP and the Council to maintain it.

59. However, the EDPS notes a number of inconsistencies with respect to terminology in the EP first reading which should be fixed. For example, the word "subscribers" has been

replaced in most cases, but not all, with the words "users", in other cases with the word "consumers." This should be harmonised.

III. SCOPE OF APPLICATION OF THE ePRIVACY DIRECTIVE: PUBLIC AND PRIVATE NETWORKS

60. Article 3.1 of the current ePrivacy Directive establishes the entities primarily concerned by the Directive, *i.e.* those which process data "*in connection with*" provision of public electronic communication services in public networks (referred above as "PPECS")[15]. Examples of PPECS include providing access to the Internet, transmission of information through electronic networks, mobile and telephone connections, etc.

61. The EP passed an Amendment 121 modifying Article 3 of the initial Commission's Proposal, pursuant to which the scope of application of the ePrivacy Directive was broadened to include "*the processing of personal data in connection with the provision of publicly available electronic communications services in public* ***and private*** *communications networks* ***and publicly accessible private networks*** *in the Community****, [...]***" (Art. 3.1 ePrivacy). Unfortunately, the Council and Commission have found it difficult to accept this amendment and therefore have not incorporated this approach into the Common Position and the Amended Proposal.

Application of the ePrivacy Directive to publicly accessible private networks

62. **For the reasons explained below and to help foster consensus, the EDPS encourages keeping the essence of Amendment 121. In addition, the EDPS suggests including an amendment to help further clarify the types of services that would be covered by the broadened scope.**

63. Private networks often are used to provide electronic communications services such as Internet access to an undefined number of people, which could potentially be large. This is the case, for example with Internet access in Internet cafes as well as at Wi-Fi spots available in hotels, restaurants, airports, trains and in other establishments open to the public where such services are often provided as a complement to other services (beverages, accommodation, etc).

64. In all of the above examples, a communications service, *e.g.* Internet access, is made available to the public not through a public network, but rather through what may be considered a private one*, i.e.* a privately operated network. Furthermore, although in the above cases, the communications service is provided to the public, because the type of network used is private rather than public, the provision of these services *arguably* is not covered by the entire ePrivacy Directive or at least by some of its articles[16]. As a result, the fundamental rights of individuals guaranteed by the ePrivacy Directive are not protected in these instances and an uneven legal situation is created for users accessing the same Internet access services through public telecommunications means *vis-a-vis* those who access them via private ones. This despite the fact that the risk to individuals' privacy and personal data in all of these cases exists to the same degree as it does when public networks

---

[15] "*This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks*".

[16] A *contrario*, it could be argued that because the communications service is provided to the public, even if the network is private, the provision of such services is covered by the existing legal framework, despite the fact that the network is private. In fact, for example, in France employers providing Internet access to their employees have been deemed to be equivalent to providers of Internet access that offer Internet access on a commercial basis. This interpretation is not widely accepted.

are used to convey the service. In sum, there does not appear to be a *rationale* justifying the differential treatment under the Directive of communications services provided over a private network versus those provided over a public network.

65. Therefore, the EDPS would support an amendment, such as Amendment 121 of the EP, pursuant to which the ePrivacy Directive would also apply to the processing of personal data in connection with the provision of publicly available electronic communications services in *private* communications networks.

66. The EDPS recognizes, however, that this language could lead to unforeseeable and possibly unintended consequences. Indeed, the mere reference to private networks could be interpreted to cover situations that clearly are not intended to be covered by the Directive. For example, it could be asserted that a literal or strict interpretation of this language could bring owners of WiFi-equipped homes[17], which enable anyone in their range (usually the home) to connect, under the scope the Directive; even though this is not the intention of Amendment 121. In order to avoid this outcome, the EDPS suggests rephrasing Amendment 121 including under the scope of application of the ePrivacy Directive *"the processing of personal data in connection with the provision of publicly available electronic communications services in public* ***or publicly accessible private communications networks*** *in the Community,..."*

67. This would help to clarify that only private networks that are publicly accessible would be covered under the ePrivacy Directive. By applying the provisions of the ePrivacy Directive *only* to ***publicly accessible private networks*** **(and not to all private networks)** a limit is set so that the Directive will cover only communication services provided in private networks that are intentionally made *accessible* to the public. This formulation will help further underscore that *availability* of the private network *to members of the public at large* is the key factor in determining whether the Directive would cover (in addition to the provision of a publicly available communications service). In other words, independently of whether the network is public or private, if the network is intentionally made available to the public in order to provide a public communications service, such as Internet access, even if such service is complementary to another one (*e.g.* hotel accommodation), this type of service/network would be covered by the ePrivacy Directive.

68. The EDPS notes that the approach supported above pursuant to which the provisions of the ePrivacy Directive are applied to ***publicly accessible private networks*** is consistent with the approaches adopted in several Member States, where the authorities have already deemed such types of services as well as services provided in purely private networks under the scope of application of the national provisions implementing the ePrivacy Directive[18].

69. To further legal certainty regarding the entities covered by the new scope, it may be useful to include an amendment in the ePrivacy Directive defining "publicly accessible private networks" which could read as follows: "*'publicly accessible private network means a privately operated network to which members of the public at large ordinarily have access on an unrestricted basis, whether or not by payment or in conjunction with other services or offerings, subject to acceptance of the applicable terms and conditions* ."

70. In practice, the above approach would mean that private networks in hotels and other establishments that provide access to the Internet to the public at large via a private network would be covered. Conversely, the provision of communications services in purely private networks where the service is restricted to a limited group of identifiable individuals

[17] Typically wireless Local Area Networks (LANs).
[18] See footnote 16.

would not be covered. Therefore, for example, virtual private networks and consumer homes equipped with Wi-Fi, would not be covered by the Directive. Services provided through purely corporate networks would not be covered either.

Private networks under the scope of application of the ePrivacy Directive

71. The exclusion of private networks *per se* as suggested above should be considered as an *interim* measure which should be subject of further debate. Indeed, given on the one side the privacy implications of excluding purely private networks as such and, on the other side, that it affects a large number of people who usually access the Internet through corporate networks, in the future, this may need to be reconsidered. For this reason, and in order to foster debate on this topic, **the EDPS recommends including a recital in the ePrivacy Directive pursuant to which the Commission would carry out a public consultation on the application of the ePrivacy Directive to all private networks, with the input of the EDPS, data protection authorities and other relevant stakeholders.** In addition, the recital could specify that as a result of the public consultation, the Commission should make any appropriate proposal to expand or limit the types of entities that should be covered by the ePrivacy Directive.

72. In addition to the above, the different articles of the ePrivacy Directive should be amended accordingly so that all the operational provisions explicitly refer to publicly available private networks in addition to public networks.

IV. PROCESSING OF TRAFFIC DATA FOR SECURITY PURPOSES

73. During the legislative process related to the review of the ePrivacy Directive, companies providing security services asserted that it was necessary to introduce into the ePrivacy Directive a provision legitimising the collection of traffic data to guarantee effective online security.

74. As a result, the EP inserted Amendment 181, which created a new Article 6.6(a) that would explicitly authorize the processing of traffic data for security purposes: "*Without prejudice to compliance with the provisions other than Article 7 of the 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 the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, 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*".

75. The Commission Amended Proposal accepted this amendment in principle, but removed a key clause designed to ensure that the other provisions of the Directive had to be respected in removing the clause that reads "*'Without prejudice* […]*...of this Directive'*). The Council adopted a redrafted version, which went yet another step further in watering down the important protections and balancing of interests that were built into Amendment 181, in adopting language that reads as follows: "*Traffic data may be processed to the extent strictly necessary to ensure […] the network and information security, as defined by Article 4(c) of Regulation (EC) 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency."*

76. **As further explained below, Article 6.6(a) is unnecessary and subject to risk of abuse, particularly if adopted in a form that does not include the important safeguards, clauses respecting other provisions of the Directive, and balancing of interests. Therefore, the EDPS recommends to reject this Article, or at a minimum, ensure that any such article on this issue includes the types of safeguards that were included in Amendment 181 as adopted by the EP.**

Legal grounds to process traffic data applicable to electronic communications services and other data controllers under current data protection legislation

77. The extent to which providers of publicly available electronic communications services may legally process traffic data is regulated under Article 6 of the ePrivacy Directive, which restricts the processing of traffic data to a limited number of purposes such as billing, interconnection, and marketing. This processing can only take place subject to specified conditions, such as consent of individuals in the case of marketing. In addition, other data controllers such as information society service providers may process traffic data under Article 7 of the Data Protection Directive which 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.

78. An example of one such legal basis is Article 7(a) of the Data Protection Directive, which requires consent of the data subject. For example, if an on-line retailer wishes to process traffic data for the purposes of sending advertisement or marketing materials, he must obtain the consent of the individual. Another legal basis set forth in Article 7 may allow, in certain instances, the processing of traffic data for security purposes by, for example, security companies offering security services. This is based on Article 7(f) which establishes that data controllers may 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 Data Protection Directive does not specify instances in which processing of personal data would 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 and other authorities.

79. The interplay between Article 7 of the Data Protection Directive and the proposed Article 6.6(a) of the ePrivacy Directive should be considered. The proposed Article 6.6(a) is a specification of the circumstances under which the requirements of Article 7(f) described above would be met. Indeed, by authorising the processing of traffic data to help ensure network and information security, Article 6.6(a) enables such processing for the purposes of the legitimate interest pursued by the data controller.

80. As further explained below, the EDPS believes that the proposed Article 6.6(a) is neither necessary nor useful. Indeed, from a legal point of view, in principle, it is unnecessary to establish whether a particular type of data processing activity, in this case the processing of traffic data for security purposes, meets or fails to meet the requirements of Article 7(f) of the Data Protection Directive, in which case, consent of the individual may be necessary *ex* Article 7(a). As noted above, this assessment is usually made by data controllers, *i.e.* companies, at implementation level, in consultation with data protection authorities, and where necessary, by the courts. Generally speaking, the EDPS believes that, in specific cases, the legitimate processing of traffic data for security purposes, carried out without jeopardising fundamental rights and freedoms of individuals, is likely to meet the requirements of Article 7(f) of the Data Protection Directive and can therefore be carried out. Moreover, there is no other precedent in the DP and ePrivacy Directives for singling

out or providing special treatment for certain types of data processing activities that would satisfy the requirements of Article 7(f), and there has been no demonstrated need for such an exception. By contrast, as noted above, it appears that under many circumstances, this type of activity would fit comfortably within the current text. **Therefore, a legal provision confirming this assessment is in principle unnecessary.**

The EP, Council, and Commission versions of Art 6.6(a)

81. As explained above, although unnecessary, it is important to highlight that Amendment 181 as adopted by the EP was nevertheless drafted, to some extent, taking into account privacy and data protection principles embodied in data protection legislation. The EP Amendment 181 could further address the data protection and privacy interest, for example, by inserting the words "in specific cases" in order to ensure the selective application of this article or by including an specific conservation period.

82. Amendment 181 contains some positive elements. It confirms that the processing should comply with any other data protection principle applicable to the processing of personal data ("*Without prejudice..... to compliance with the provisions [..] of the Directive 95/46/EC and [..] of this Directive*). Furthermore, although AM 181 permits the processing of traffic data for security purposes, it strikes a balance between the interests of the entity that processes traffic data and those of the individuals whose data is processed so that such data processing can take place only if the interests for the fundamental rights and freedoms of individuals are not overridden by those of the entity processing the data ("*except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject").* This requirement is essential insofar as it may permit the processing of traffic data for specific cases; however, it would not enable an entity to process traffic data in bulk.

83. The Council's redrafted version of the amendment contains elements to be praised, such as retaining the term "*strictly necessary*" which underscores the limited scope of application of this Article. However, the Council version eliminates the data protection and privacy safeguards referred to above. While in principle general data protection provisions apply, irrespective if specific reference is made in every case, Council's version of Article 6.6(a) may nevertheless be interpreted as giving full discretionary powers to process traffic data without being subject to any data protection and privacy safeguards that apply whenever traffic data is processed. Therefore, it might be argued that traffic data may be collected, stored, and further used without having to comply with data protection principles and specific obligations that otherwise apply to responsible parties, such as the quality principle or the obligation of fair and lawful processing and to keep the data confidential and secure. Furthermore, because no reference is made to applicable data protection principles that impose time limits for storage of the information or to specific time limits within the article, the Council version may be interpreted as enabling the collection and processing of traffic data for security purposes for an unspecified period of time.

84. In addition, the Council has weakened the privacy protections in certain parts of the text by potentially broadening the language. For example, the reference to the "*legitimate interest of the data controller"* has been removed, raising doubts regarding the types of entities that would be able to avail themselves of this exception. It is of utmost importance to avoid opening the door to any user or legal entity to benefit from this amendment.

85. The recent experiences in the EP and Council demonstrate that it is difficult to define by law the extent and conditions under which the processing of data for security purposes can be lawfully executed. Any existing or future article is unlikely to remove the obvious risks of an overly broad application of the exception for reasons other than purely security

related or by entities that should not be able to benefit from the exception. This is not to say that such processing may not take place in any event. However, whether and to what extent it could be carried out, may be better assessed at implementation level. Entities wishing to engage in such processing should discuss the scope and conditions with the data protection authorities and, possibly, with the Article 29 Working Party. Alternatively, the ePrivacy Directive could include an article allowing the processing of traffic data for security purposes, subject to explicit authorization by data protection authorities.

86. Taking into account on the one hand the risks that Article 6.6(a) poses to the fundamental right to data protection and privacy of individuals, and on the other hand the fact that, as explained in this Opinion, from a legal point of view, this Article is unnecessary, **the EDPS has come to the conclusion that the best outcome would be for the proposed Article 6.6(a) to be deleted altogether.**

87. **If any text along the lines of any current version of Article 6.6(a) is adopted, against the recommendation of the EDPS, it should in any event incorporate the data protection safeguards discussed above. It should also be properly integrated into the existing structure of Article 6, preferably as a new paragraph 2a.**

V. THE ABILITY OF LEGAL PERSONS TO TAKE ACTION FOR INFRINGEMENTS OF THE ePRIVACY DIRECTIVE

88. The EP passed Amendment 133 giving the possibility for Internet access providers and other legal entities such as consumer associations to bring legal action against infringements of any of the provisions of the ePrivacy Directive[19]. Unfortunately, neither the Commission nor the Council has accepted it. The EDPS considers this amendment as very positive and recommends maintaining it.

89. To understand the importance of this amendment one needs to realize that in the area of privacy and data protection the damage inflicted upon a person individually considered, is usually not sufficient in itself for him/her to initiate legal action before a court. Individuals normally do not go to court on their own because they were spammed or because their name was wrongly included in a directory. This amendment would permit consumer associations and trade unions representing the interest of consumers at a collective level to take legal action on their behalf before courts. A greater diversity of enforcement mechanisms is also likely to encourage a better level of compliance and therefore in the interest of an effective application of the provisions of the ePrivacy Directive.

90. There are legal precedents in some Member States' legal frameworks which already foresee the possibility of collective redress in order to allow consumers or interests groups to claim for compensation from the party who caused damage.

91. Moreover, some Member States' Competition laws[20] entitle consumers, interest groups (in addition to the *affected competitor)* to file a lawsuit against the breaching entity. The *ratio* behind this approach is that companies acting in breach of competition laws are likely to profit since consumers suffering only marginal damages are as a general rule reluctant to file a lawsuit. This rationale can be applied *mutantis mutandi* in the field of data protection and privacy.

92. More important, as mentioned above, entitling legal entities such as consumer associations and PPECS to file lawsuits fosters the position of consumers and it promotes overall

[19] Article 13.6 of the EP first reading.
[20] See, for example, § 8 UWG - German law on Unfair Competition.

compliance with data protection legislation. If breaching companies are facing a higher risk to be sued, they are likely to invest more in complying with data protection legislation, which in the long run increases the level of privacy and consumer protection**. For all of these reasons, the EDPS calls upon the EP and the Council to** adopt a provision enabling legal entities to bring legal action against infringements of any of the provisions of the ePrivacy Directive.

VI. CONCLUSION

93. The Council's Common Position, EP first reading and Commission's Amended Proposal contain, to varying degrees, positive elements that would serve to strengthen the protection of individuals' privacy and personal data.

94. However, the EDPS believes that there is room for improvement, particularly with respect to the Council's Common Position which, unfortunately, has not maintained some of the EP amendments intended to help ensure the adequate protection of individuals' privacy and personal data. The EDPS urges the EP and the Council to restore the privacy safeguards embedded in the EP first reading.

95. In addition, the EDPS believes that it would be appropriate to streamline some of the provisions of the Directive. This is particularly true in the case of the security breach provisions, as the EDPS believes that the full benefits of breach notification will be best realized if the legal framework is set right from the outset. Finally, the EDPS considers that it would be appropriate to improve and clarify the formulation of some of the provisions of the Directive.

96. In the light of the above, the EDPS urges the EP and the Council to increase efforts to improve and clarify some of the provisions of the ePrivacy Directive, while at the same time, reinstating the amendments adopted by the EP first reading aimed at providing an appropriate level of privacy and data protection. To this end, the points 97, 98, 99 and 100 below summarise the issues at stake and put forward some recommendations and drafting proposals. The EDPS calls upon all parties involved to take them into account as the ePrivacy Directive makes its way towards final adoption.

Security Breach

97. The European Parliament, Commission and Council have all adopted varying approaches for notification of security breaches. Differences between the three models exist regarding, *inter alia*, the entities covered by the obligation, standard or trigger for the notification, data subjects entitled to be notified, etc. There is a need for the EP and Council to do its utmost to come up with a solid legal framework for security breach. To this end, the EP and Council should**:**

- ***Maintain*** the **definition of security breach in the EP, Council and Commission texts** as it is broad enough to encompass most of the relevant situations in which notification of security breaches might be warranted

- With respect to the scope of the entities to be covered by the proposed notification requirement*,* ***include*** **providers of information society services.** On-line retailers, on-line banks, on-line pharmacies are as likely to suffer security breaches as telecom companies, if not more so. **Citizens will expect to be notified not only when**

Internet access providers suffer security breaches but particularly when this happens to their on-line banks and on-line pharmacies.

- Regarding the trigger for the notification, the Amended Proposal's standard "*reasonably likely to harm*" is an appropriate standard which provides for the functionality of the scheme. However, **it is important to ensure that "harm" is sufficiently wide to cover all relevant instances of negative effects on the privacy or other legitimate interests of individuals. Otherwise, it would be preferable to create a new standard pursuant to which notification would be mandatory "*if the breach is reasonably likely to cause adverse effects to individuals*". T**he Council's approach, which requires that the breach *seriously* affects someone's privacy, would provide inadequate protection to individuals insofar as such standard requires the effect on privacy to be "serious". This also gives scope for a subjective evaluation.

- While the involvement of an authority to determine whether a concerned entity must notify individuals certainly has positive effects, it may be impractical and difficult to apply, and might also take resources away from other important priorities. If authorities cannot react extremely quickly, the EDPS fears that such a system may even diminish the protection for individuals and put undue pressure upon authorities. Thus, **on the whole, the EDPS advises to *setting up a* system where it is up to concerned entities to make the assessment as to whether they must notify**.

- In order to enable authorities to exercise oversight over the assessments made by covered entities regarding whether to notify, ***implement*** the following safeguards:

  - ***Ensure*** that such entities are obliged to notify authorities of all breaches that meet the requisite standard.

  - ***Provide*** authorities with an oversight role that enables them to be selective in order to be effective. To achieve the above, insert the following language: "*If the subscriber or individual concerned has not already been notified, the competent national authority, having considered the nature of the breach, may require the PPECS or ISSP to do so*".

  - ***Adopt*** a new provision requiring entities to maintain a detailed and comprehensive internal audit trail. This could be achieved by adopting the following language: "*The PPECS and ISSPs shall keep and maintain comprehensive records detailing all security breaches that occurred, relevant technical information related thereto, and remedial action taken. Records shall also contain a reference to all notifications issued to subscribers or individuals concerned and to the competent national authorities, including their date and content. The records shall be produced to the competent national authority at its request.*"

- In order to ensure consistency in the implementation of the security breach framework, ***provide*** the Commission with the ability to adopt technical implementing measures, following prior consultation with the EDPS, the Article 29 Working Party and other relevant stakeholders.

- Concerning the individuals to be notified, ***use*** **the Commission or EP's terminology "individuals concerned" or "affected users"** as it includes all the individuals whose personal data has been compromised.

Publicly Accessible Private Networks

98. Communications services are often made available to the public not through public networks, but through privately operated networks (*e.g.* Wi-Fi spots available in hotels, airports), which are arguably not covered by the Directive. The EP adopted Amendment 121 (Article 3) broadening the scope of application of the Directive to include public and **private** communications networks, as well as **publicly accessible private networks**. In this regard, the EP and Council should**:**

- ***Keep* the essence of Amendment 121, but *rephrase*** it to include under the scope of the ePrivacy Directive only "*the processing of personal data in connection with the provision of publicly available electronic communications services in public* ***or publicly accessible private communications networks*** *in the Community*". Purely privately operated networks (as opposed to publicly accessible private networks) would not be explicitly covered.

- ***Amend*** accordingly all the operational provisions to explicitly refer to publicly accessible private networks in addition to public networks.

- ***Include*** an amendment defining "'*publicly accessible private network means a privately operated network to which members of the public at large ordinarily have access on an unrestricted basis, whether or not by payment or in conjunction with other services or offerings, subject to acceptance of the applicable terms and conditions*". This will provide more legal certainty regarding the entities covered by the new scope.

- ***Adopt*** a new recital per which the Commission would carry out a public consultation on the application of the ePrivacy Directive to all private networks, with the input of the EDPS, Article 29 Working Party and other relevant stakeholders**.** Specify that as a result of the public consultation, the Commission should make any appropriate proposal to expand or limit the types of entities that should be covered by the ePrivacy Directive.

Processing of Traffic Data for Security Purposes

99. The EP first reading adopted Amendment 181 (Article 6.6(a)), authorizing the processing of traffic data for security purposes. The Council's Common Position adopted a new version watering down some of the privacy safeguards. In this regard, the EDPS recommends that the EP and the Council:

- ***Reject*** this Article entirely because it is unnecessary and, if abused, could unduly threaten the data protection and privacy of individuals.
- Alternatively, if some variation of the current version of Article 6.6(a) is to be adopted, ***incorporate*** the data protection safeguards discussed in this Opinion (similar to those of the EP Amendment).

Actions for Infringements of the ePrivacy Directive

100. The Parliament adopted Amendment 133 (Article 13.6) giving legal entities the ability to bring legal action against infringements of any provisions of the Directive. Unfortunately the Council did not maintain it. The Council and EP should:

- ***Endorse*** the provision affording the possibility to legal entities, such as consumer and trade associations, the right to bring legal action against infringements of any provisions of the Directive (not only for infringement of the spam provisions as is the current approach in the Common Position and Amended Proposal). A greater diversity of enforcement mechanisms will encourage a higher level of compliance and effective application of the provisions of the ePrivacy Directive as a whole.

Meeting the Challenge

101. In all the above matters, the EP and Council must meet the challenge of devising proper rules and provisions that are both workable, functional and respect the rights to privacy and data protection of individuals. The EDPS is hopeful that the parties involved will do their utmost to meet this challenge and hopes that this Opinion will contribute in this endeavor.

Done in Brussels, 9 January 2009

(signed)

Peter HUSTINX
European Data Protection Supervisor