ARTICLE 29 DATA PROTECTION WORKING PARTY

00350/09/EN
WP 159

Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)

Adopted on 10 February 2009

Table of Contents

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29, 30(1)(a) and 30(3) of that Directive, and Article 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to Article 255 of the EC Treaty and to Regulation (EC) no. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents,

having regard to its Rules of Procedure

HAS ADOPTED THE PRESENT DOCUMENT:

1. BACKGROUND

On 13 November 2007, the Commission adopted a Proposal for a Directive ("the Proposal") amending the Directive 2002/58/EC (ePrivacy Directive) concerning the processing of personal data and the protection of privacy in the electronic communications sector and the f Directive 2002/21/EC (Framework Directive).

In its first reading, on 24 September 2008, the European Parliament adopted amendments to the Proposal ("the Parliament's Amendments"), that were commented on 6 November 2008 by the European Commission in COM(2008)723 final ("the Commission's Comments").

Then, on 27 November 2008, the Council of the European Union reached a political agreement ("the Council's Agreement").

The Article 29 Working Party wishes to comment on the Parliament's Amendments, on the Commission's Comments and on the Council's Agreement.

The Working Party recalls that it has already adopted two Opinions on the proposals amending the EU's regulatory framework for electronic communications networks and services (Opinion 8/2006 adopted on 26 September 2006[2] and Opinion 2/2008 adopted on 15 May 2008[3]).

Though the Working Party is pleased that some of its previous recommendations were taken into account, it wishes to underline some essential concerns related to the issues raised after the first reading at the Parliament and at the Council; the Working Party does not repeat all the points made in its previous opinions, which still remain valid.

---

1 Official Journal L281 of 23/11/1995, p. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

3 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf

2. NOTIFICATION OF PERSONAL DATA BREACHES

2.1. Observations

The Working Party fully supports the proposed strengthening of Article 4 of the ePrivacy Directive by requiring providers of publicly available communication services to notify security breaches. Breach notifications may become an important tool for Data Protection Authorities to increase focus and effectiveness when enforcing the obligation of service providers to take appropriate security measures.

In general, the Working Party recommends the following approach to the issue of personal data breach notifications:

- the competent national regulatory authority is informed whenever there is a risk of adverse effects[4] to individuals' privacy and data protection;

- it is essential that affected users are informed immediately by the service providers in those cases where the security breach is likely to lead to adverse effects[5] to individuals' privacy and data protection, notwithstanding the possibility for the competent national regulatory authority to disclose publicly information about the breach and to force the service provider to disclose information about the breach;

- each service provider should maintain records[6] of all personal data breaches.

The Working Party also observes that the three proposals (by the Parliament, the Commission and the Council) adopt substantially different approaches to the issue of security and personal data breaches, especially when considering:

- the scope of the obligation (which extends to information society services in the Parliament's Amendments and is limited to publicly available electronic communications services for the Council and the Commission); the Working Party strongly supports an extension of the scope of the obligation to Information Society Services;

- the entity on which rests the decision to notify individuals (it is the competent authority for the Parliament and the Commission and it is the service provider for the Council);

- the types of breaches to be notified (all breaches in the Parliament's Proposal and in the Commission's Comments and only serious breaches in the Council's Agreement);

- and the persons who may be notified (subscribers or individuals for the Parliament and the Commission but only subscribers for the Council).

---

4 The risk of adverse effects should be assessed taking into consideration elements such as the amount of data affected by the breach, their nature, the impact of the breach on an individual, for instance, identity theft, financial loss, loss of business or employment opportunities, or a combination of these or other similar circumstances. The qualitative and quantitative criteria for assessing the impact of adverse effects will need to be defined precisely during the commitology procedure, taking into account that it is important not to flood authorities with minor cases and not to alarm individuals unnecessarily.

5 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

6 the format of those records should be standardised to ensure that the records are auditable by the competent national regulatory authority

Scope of the notification: Information Society Services

The Working Party strongly supports Amendments 187/rev and 184 of the Parliament's Amendments. **An extension of personal data breach notifications to Information Society Services is necessary given the ever increasing role these services play in the daily lives of European citizens,** and the increasing amounts of personal data processed by these services. Online transactions including access to e-banking services, private sector medical records and online shopping are few examples of services that may be subject to personal data breaches causing significant risks to a large number of European citizens. Limiting the scope of these obligations to publicly available electronic communications services would only affect a very limited number of stakeholders and thus would significantly reduce the impact of personal data breach notifications as a means to protect individuals against risks such as identity theft, financial loss, loss of business or employment opportunities and physical harm.

Therefore, the Working Party deeply regrets that this proposal was not backed by the Commission and by the Council and it recalls that some provisions of the ePrivacy Directive already apply beyond the strict scope of electronic communication services[7].

Responsibility and criteria for notification

The relevant service providers should be responsible for assessing the risks created by personal data breaches; they are in the best position to determine without delay whether affected persons should be notified, based on the assessment rules set by the authorities. **Notwithstanding their obligation to notify the competent national regulatory authorities of all breaches whenever there is a risk of adverse effects, service providers should determine if notification to subscribers or individuals is required. To ensure that accurate and relevant information is provided to the public, the competent national regulatory authorities may decide to disclose the breach publicly, whenever it is deemed necessary, and may force the service provider to disclose information about the breach.**

Since notification will be carried out by the service provider, **it is essential that the Directive provides safeguards to ensure that breaches were not concealed**, that the assessment of the breach was correctly carried out, and that individuals were notified whenever it was required.

The authorities will be notified in a larger number of cases so they can be in a position to exercise supervision over the process of notification to individuals by service providers. The format of the notification should be harmonised on a European level and should include objective and clear criteria that assist in assessing the impact of the adverse effects caused by the breach. In addition, the competent national regulatory authority should check if the assessment of the breach was correctly carried out by the service provider, and if appropriate measures were taken following the personal data breach. Finally, **to prevent the concealing of breaches it is essential that the Directive provides the competent national regulatory authority with the power to impose punitive financial sanctions (penalties)**[8] **in cases**

---

[7] Certain provisions of the ePrivacy Directive such as Article 5(3)(cookies and spyware) and Article 13 (unsolicited communications) are already general provisions which are applicable not only to the electronic communication services.
This possible extension beyond the strict scope of publicly available electronic communications services is also envisaged in other situations, because the Commission proposed to extend the scope of application of Article 5(3) to cover cases when cookies and spyware are delivered through media such as CD-ROMs or USB keys, which are not publicly available electronic communications services.

[8] The Working Party takes note that such provisions were proposed by the Parliament, the Commission and the Council in a new article 15a (1)

where a service provider fails to report or incorrectly reports the personal data breaches to the individuals and or the NRA.

The types of breaches to be notified to individuals: the notion of adverse effects

The Working Party welcomes the introduction of a new definition of "personal data breach" in Article 2[9], as proposed in the Commission's Comments[10] .

However, the Working Party observes that the three proposals use a different wording to qualify when breaches should be notified to data subjects. Therefore, **the Working Party recommends that security breaches should be notified to data subjects when they may lead to adverse effects to individuals' privacy and data protection.** In this respect, the Council's Agreement provides useful examples in Recital 29.

The persons who may be notified

The Working Party welcomes the references to "subscribers or individuals", to "affected users" and to the "competent national authority" included in Recital 29 of the Parliament's Amendments[11]. The Council's Agreement restricts notifications to "subscribers" and therefore, some personal data breaches which had been described in Opinion 2/2008 will not be notified to affected persons.

2.2. Notification exemptions

The Working Party acknowledges that breach notifications should include information about the circumstances of the breach, including whether personal data had been protected by encryption; this information is essential for the competent national regulatory authority in the event of a breach to determine the appropriate action, if any, to be taken with the service provider.

However, **the Working Party objects to the creation of notification exemptions[12] when service providers have implemented "appropriate technological protection measures, and those measures were applied to the data concerned by the security breach". This provision would significantly reduce the quality and usefulness of the information delivered to affected persons.** Affected users may only be in the position to take appropriate measures to mitigate the risks they are facing if they have been adequately informed. Therefore, **the Working Party emphasises the importance of the notification format and risk assessment in determining whether individuals should be notified, regardless of the technical measures that were actually taken to protect their data.**

---

9 see Commission's Comments on Amendments 187/rev and 184 of the Parliament's Amendments

10 Nevertheless, this notion of "personal data breach" is general and should not be restricted to data processed in connection with the provision of publicly available electronic communication services; it should also cover at least information society services.

11 see Amendment 183

12 see recital 29 in the Parliament's Amendments (Amendment 122) and recitals 29 and 32 in the Council's Agreement

3. TRAFFIC DATA

3.1. Processing of traffic data for security purposes

In a new Article 6.6 (a), the Parliament, the Council and the Commission propose to create a new exemption in the ePrivacy Directive allowing for the processing of traffic data for security purposes.

The Working Party is aware that "providers of security services" deploy security solutions[13] (such as anti-virus and anti-spam software, firewalls, or intrusion detection systems) that may require the processing of traffic data for the purpose of securing personal data of the users and protecting the service itself. Nevertheless, it is concerned that the current wording might lend legitimacy to large scale deployment of deep packet inspection[14], both in the network and in user equipment such as ADSL boxes, while the current legal framework already details the cases in which traffic data may be processed for security purposes.

Indeed, the legal grounds allowing for the processing of traffic data by publicly available electronic communication services and for the processing of personal data by data controllers are laid down in Article 6 of the ePrivacy Directive as well as Article 7 and 17 of the Data Protection Directive. The extent to which personal data may be processed for the legitimate interests pursued by the controller is detailed in Article 7 (f) of the Data Protection Directive; it must not override the interests for fundamental rights and freedoms of the data subject. Article 17 of the Data Protection Directive also places an obligation on the data controller *"to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access… and against all other unlawful forms of processing"*. The measures adopted must also be proportionate to the risks represented by the processing and the nature of the data to be protected.

The Working Party also underlines that the scope of Amendment 180 of the Parliament's Amendments has been clarified in the Commission's Comments. **The Working Party takes note that the wording proposed by the Commission establishes beyond all doubt that the processing of traffic data falls within the scope of the Data Protection Directive.** Therefore, providers of security services shall notify the national Data Protection Authorities whenever it is required, and ensure that the rights of the persons can be exercised.

Finally, the Working Party recalls that the processing of traffic data for security purposes is already carried out in Member States where specific measures were adopted pursuant to Article 15 (1) of the ePrivacy Directive which allows Member States to adopt legislative measures waiving the principle of anonymisation or deletion of traffic data[15] when they are no longer needed for the purpose of the transmission of the communication to prevent unauthorised use of the electronic communication system.

For the reasons invoked above, **the proposal for a new Article 6(6a) is unnecessary.**

---

[13] either in terminal equipment of the user or in the network

[14] deep packet inspection allows for very invasive tracking and tracing of user behaviour

[15] laid down in Article 6 (1)

4. IP ADDRESSES

The Parliament and the Commission propose to introduce a new Recital (27a) on IP addresses[16].

The Working Party welcomes the wording proposed in the Commission's Comments when it makes specific reference to its work. However, the Working Party does not support the proposal to make an explicit reference to this issue in a directive.

In this respect, **it re-emphasises its earlier Opinion[17] that unless the service provider "***is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side"*.

IP addresses relate to identifiable persons in most cases. Identifiability means identifiable by the access provider or by other means, with the help of additional identifiers such as cookies or in interactions with internet services with which the data subject is identified explicitly or implicitly.

Recital 26 of the Data Protection Directive clearly specifies that to determine if a person is identifiable, "*account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person"*.

The definition of personal data in the Data Protection Directive refers to data 'relating' to a person, and IP addresses are commonly used to distinguish between users to whom should be applied a different treatment for example in the context of targeted advertisement serving or profile creation.

While the Working Party is prepared to assist the Commission in undertaking the work on IP addresses suggested by the Parliament[18], it agrees with the Commission that a substantive provision of a directive is not the most suitable way of addressing this issue, and that a reporting obligation referring to 'purposes not covered by this Directive' is not appropriate.

5. INFORMATION OF DATA PROTECTION AUTHORITIES

In its first reading, the Parliament adopted amendment 136 on Article 15 of the ePrivacy Directive, which was then amended in the Commission's Comments. This proposal would create an obligation for all providers of telecommunication services and networks and all providers of information society services to report to the competent data protection authority any request "received pursuant to paragraph 1"[19] and an obligation for this authority to investigate each request and report back to the appropriate judicial authorities if it deems that the relevant provisions of national law have not been complied with."

The proposed reporting is a useful addition in the interest of greater transparency and control by regulatory authorities. But while this provision would strongly enhance the supervision and enforcement capabilities of the data protection authorities thus contributing to an improved application of lawful access to the information, it would also create an administrative burden, both for the companies involved and for the data protection authorities. With this respect, the Working Party is concerned by the need to monitor the growing number of requests by

---

16 amendment 185 of the Parliament

17 Opinion 4/2007 on the concept of personal data and the Opinion on data protection issues related to search engines

18 in Amendments 139 and 186/rev

19 which describes data retention obligations formalized in the Data Retention Directive (2006/24/EC)

judiciary authorities[20] and by the new responsibility for data protection authorities to control every single judiciary investigation, which requires a substantial increase of the financial and personnel resources of these authorities.

Therefore, **the Working Party suggests that such reporting could be done only once a year. It could include details about internal procedures used to answer the requests for access to users' personal data, the number of requests received, the legal justification invoked, and the problems encountered, if any.** It is also essential that such reporting obligation would be harmonised and detailed on a EU level.

6. UNSOLICITED COMMUNICATIONS

Amendment 131 of the Parliament provides clarification that MMS and similar technologies are covered by the definition of 'electronic mail' given in Article 2(h).

Firstly, the Working Party observes that Recital 40 of the ePrivacy Directive already clarifies that SMS fall within the definition of e- mail[21].

Secondly, it is necessary to adapt Article 13 (1) to emerging technologies, following the principle laid down in Recital 4[22]. The current wording of Article 13.1 makes the assumption that the person is already connected to the network on which the communication (for instance a call or an email) is conveyed. It does not cover cases where a solicitation would ask a user to connect to a network that serves advertisements exclusively. This may typically be the case in Bluetooth marketing applications.

Therefore, the Working Party welcomes the clarifications provided in the Commission's Comments to the scope of Article 13 concern mainly the use of the word "communication" and the new Recital referring to "similar technologies'. This ensures that prior consent is required in Bluetooth marketing applications, thus taking into account the observations made by the Working Party in its Opinion 2/2008 on the "need to protect users of short range wireless media against unsolicited communication as defined in Article 13". An explicit reference to Bluetooth could also be included in Recital 40.

Thirdly, the Working Party recalls its observation of Opinion 2/2008 about the use of the term "subscriber" in Article 13, and takes note with satisfaction of the wording proposed in the Council's Agreement.

Lastly, the proposal by the Council to amend Article 13 (2) by adding the phrase "at the time of the collection of the contact details" is also very useful since it gives unequivocal information about the moment when users shall be able to object to the use of their electronic contact details for direct marketing purposes.

---

[20] many telecommunication operators receive several hundreds of requests per day

[21] which is defined in Article 2(h) of the e-Privacy Directive

[22] which states that the e-Privacy Directive has "to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used"

7. BROWSER SETTINGS

The Working Party strongly objects to the amendment 128 adopted by the Parliament, stating that default browser settings would be a means to provide prior consent. Even though this amendment was included in the Commission's Comments and the Council's Agreement, the Working Party wishes to comment on this amendment.

Aside from the formal problem of creating such technology-specific language in the Directive, the Working Party is concerned about the erosion of the definition of consent and a subsequent lack of transparency.

Most browsers use default settings that do not allow the users to be informed about any tentative storage or access to their terminal equipment. Therefore, default browser settings should be "privacy friendly" but cannot be a means to collect free, specific and informed consent of the users, as required in Article 2 (h) of the Data Protection Directive.

With regard to cookies, the Working Party is of the opinion that the controller of the cookies should inform its users in its privacy statement and may not rely on (default) browser settings. Also, the chosen wording is not limited to the current issue of cookies, but implies any other new technology that could be used to track the users' behaviour using their browser.

8. LEGAL ACTION BY INDIVIDUALS AND LEGAL PERSONS

The Working Party supports the Parliament's proposal[23] to introduce in Article 13 (6) the possibility for "any individual or legal person to take legal action in case he was affected by infringements of national provisions adopted pursuant to the ePrivacy Directive".

This provision will undoubtedly strengthen user rights and contribute to the development of better security practices among industry players.

9. OTHER ISSUES

Finally, the Working Party takes note with satisfaction:

- that the legislator intends to punish phising practices[24];
- that the Commission and the Council have taken into account[25] the Working Party's request to be consulted during the comitology procedure set forth in Article 4 (4);
- that it has been included in the consultation process provided for in Article 15a (4);
- that it will be consulted in preparation of the report on the application of the revised ePrivacy Directive[26];
- that the Commission, the Council and the Parliament wish to clarify that the ePrivacy Directive applies to emerging technologies, such as RFID[27] or NFC, which rely on contactless identification devices using radio frequencies.

---

23 in amendment 133
24 see amendment 132 of the Parliament
25 in its comment to amendment 127 of the Parliament
26 see Amendment 139 and 186/rev of the Parliament
27 in Article 3 and recital 28

10. CONCLUSION

The Article 29 Working Party calls on the European legislators to consider foremost, amongst the other issues highlighted in this Opinion, the extension of the scope of personal data breach notification obligations to information society services, given its essential impact on the protection of the personal data of all European citizens.

Done at Brussels, on 10/02/2009

For the Working Party
The Chairman
Alex TÜRK