Commentary on Directive 2002/58/EC, article 6

Rosier, Karen

Published in:
Concise European IT law

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

recognises that cookies are personal data, a point that has on occasion been contested in the past. The processing of data generated through these devices is subject to the other principles of the Data Protection Directive. For example, the duration of the placement of a cookie might be limited to the period justified by the legitimate purpose. This consideration is important insofar as, in many cases, cookies are placed for very long periods of time (20-30 years). *'pt-in system.* The most noticeable modification of the art. 5(3) brought by ıe Amending Directive is the option taken of the European legislator of ıe opt-in system as claimed by privacy advocates. The activation of this pt-in system ideally presupposes that the internet users' browsers would be onfigured in such a way to permit the expression of the consent according o the parameters chosen by the users. As EDPS asserts: 'I note in particular he emphasis on more effective enforcement of the rules on spyware and cookies. This has special relevance where privacy rights must be protected in relation to so called targeted advertising.' *Doubts about the scope of this new requirement.* As regards the scope of this modification, certain doubts have been raised. The reference to the conditions regarding the consent introduced by the Amending Directive to para. 3 creates ambiguity because it seems to limit the consent requirement to personal data, as opposed to other types of information. Even if under the opinion of the Working Party about the notion of personal data (Working Paper 4/2007 on the concept of personal data, Working Paper 136 (20 June 2007) as well as of many European national data protection authorities, persistent cookies containing a unique user ID are to be considered as processing personal data and therefore are subject to applicable data protection rules, this position is still contested by certain EU jurisdictions. Anyway, it might still be considered that some cookies (or similar technologies) may not meet the criteria to be qualified as personal data and therefore fall outside the scope of this provision. Second point, as far as the consent requirement is concerned, the provision does not explain how and when obtaining the consent. The provision does not explicitly refer to 'prior' consent. The use of the past tense ('has given') might mean that the European legislator intended to make sure that users are offered a simple opportunity to refuse cookies prior to their installation on users' computers. How will consent have to be obtained in this specific context? The recitals of the Amending Directive include the following remark: 'where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application'. In its opinion about the Amending Directive, the Working Party strongly objected the idea of using default browser settings as a mean to provide consent. Concerned about the possible erosion of the definition of consent and of a subsequent lack of transparency, the Working Party opined that: 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'.

6. Exceptions to the opt-in system. Two exceptions to the opt-in system are provided by the Directive. The first one mentions the necessity of 'storage and access for the sole purpose of carrying out or facilitating the transmission of a communication'. Authors believe this exception could allow, for example, a software feature that searches users' address books to obtain e-mail addresses without requesting these from the users themselves. The addresses would then be used for the purpose of sending (unsolicited) e-mails. The second exception expressly mentioned by the last sentence of para. 3 refers to any technical storage or access 'strictly necessary for the provider in order to provide an information society service explicitly requested by the subscriber or user'. The text refers to tracking devices which are strictly necessary and not simply useful, for instance, screen simulator software which renders downloading certain web pages more user-friendly. Furthermore, is it possible to consider that a software seller needs to install 'spyware' within the user's terminal in order to verify whether there is no contra-indication as regards the functioning of the software to be purchased? Under such circumstances, the opt-out solution, consisting in alerting the user to the installation of the device and the reasons why it is desirable, seems more appropriate. It must be added that the Amending Directive limits the benefit of the exception to the direct provider of the service and therefore excludes the possibility for other information services providers to take advantage of the connection opened by the first one to introduce seamlessly cookies or spyware as it might occur with the so-called transclusive hyperlinks.

[Traffic data]

Article 6

(1) Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

(2) Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

(3) For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred

to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

(4) The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

(5) Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

(6) Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

1. General. This provision governs the processing of traffic data in the context of the provision of a public communications network and of publicly available electronic communications services. It specifies the purposes for which traffic data may be processed, the conditions for such processing and the persons who may legally process the data. Since traffic data are, in principle, confidential by virtue of art. 5 (see comment on art. 5(1)), the present provision allowing the processing of such data for specific purposes should be viewed as derogating from this principle and should be interpreted restrictively. Moreover, the requirements set for traffic data processing in this article are not the only ones applicable. Indeed, the Data Protection Directive applies to all the aspects that are not specifically regulated in the present art. 6. In light of the European legislator's intention to limit the scope of the Directive to the processing of personal data, this provision should indeed only relate to traffic data which are also personal data. There are discussions as to whether IP addresses may be hold as personal data. The Working Party reminded that IP addresses, whether dynamic or permanent, should be seen as personal data since the internet service provider is able to relate such data to its subscribers. Only in cases where, for technical or organisational reasons, an IP address cannot not be attributed to a user or a subscriber (such as in an internet café), it may be considered that IP address is not a personal data (Opinion on the concept of personal data, pp. 16-17). So, the Supreme Court of France considered in a decision (case No. 08-84088) rendered on 13 January 2009, that the registering and subsequent enquiries about IP address of an Internet user suspected of IP infringement do not involve the processing

of personal data since it was strictly forbidden by legislative provisions to the network operator and the Internet access provider to reveal the name of the Internet's subscriber who uses this IP address. Let us conclude to the extent traffic data are also personal data, their data controllers are required to comply with the general requirements stated in the Data Protection Directive such as the obligation to notify the processing to the supervisory authority (art. 18 of the Data Protection Directive) or the condition only to process data that are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (art. 6 of the Data Protection Directive). Recital 30 of the Directive expressly indicates in this regard that 'systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'.

2. Retention of traffic data (para. 1). (a) The erasure rule. Art. 6(1) states that the provider of a public communications network and the provider of publicly available electronic communications services cannot process or store traffic data longer than necessary for the purpose of the transmission of the communication processed. Art. 6(1) clearly authorises the processing of traffic data by these providers for a transmission purpose while it sets limits to such processing. Furthermore, recital 29 of the Directive allows the processing, in individual cases, of traffic data by the service provider where this is necessary in order to detect technical failure or errors in the transmission of communications. The provider of public communications network and the provider of publicly available electronic communications services must erase traffic data or render them anonymous as soon as the retention of the traffic data is no longer necessary to ensure the transmission of a communication. Recital 27 concedes that the exact moment of the completion of the transmission of a communication depends on the type of electronic communications service that is provided. A telephone call will be ended as soon as either of the users terminates the connection while the transmission of an electronic mail is completed as soon as the addressee collects the message, typically from the server of the service provider. According to recital 28, 'the obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict, however, with such procedures on internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services'. The exact intention of the European legislator when inserting such recital is unclear. It is likely that such commentary aims at allowing retention of traffic data for the purpose of caching or log-in procedures in spite of the erasure rule. **(b) Rule applies to traffic data relating to users and subscribers.** This erasure rule applies to traffic data relating to subscribers as well as to traffic data concerning users. Therefore, the processing of data relating to legal persons who are subscribers is subject to the limitations stated in this paragraph. **(c) Exceptions.** Retention and

further processing of traffic data after transmission is completed is however admitted for specific purposes identified in para. 2, 3 and 5 and in art. 15(1).

3. Traffic data processing for billing purposes (para. 2). (a) Purposes of processing allowed. Traffic data relating to users and subscribers may be processed for billing purposes and interconnection payment. Processing for billing purposes seems perfectly logical since traffic data are precisely identified as data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof (see art. 2). **(b) Selection of the traffic data.** Only the traffic data in the possession of the service provider which are necessary to carry out the billing and payment procedures may be stored and further processed longer than permitted under para. 1. The traffic data processed will thus need to be selected with regards to the type of billing carried out. For instance, non-itemised billing will not require as much data as itemised billing. **(c) Duration of the retention.** Moreover, traffic data can only be retained for the period during which the bill may lawfully be challenged or payment pursued. This period may vary between Member States as no precise time limit is defined in the Directive. The Working Party issued a recommendation to Member States in this regard. The Working Party considers that this should ordinarily involve a routine storage period for billing of maximum 3 to 6 months, with the exception of particular cases of dispute where the data may be processed for a longer period (Opinion on storage of traffic data for billing purposes, pp. 6-7). **(d) Information requirement (para. 4).** *Content of the information.* Art. 6(4) goes beyond the regime of the Old Directive in requiring from the service provider to supply specific information to the subscriber or user in respect of the use of their data for billing purposes and interconnection payment. The service provider must indeed inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing, as well as of the purposes of processing, i.e. the purposes of billing and/or interconnection payment. *Moment of the information.* Although para. 4 does not indicate when the information needs to be provided, it is reasonable to consider that the information should be supplied prior to carrying out the related processing. This position is also supported by the fact that prior information is the rule under art. 9 of the Data Protection Directive. In line with this, the explanatory memorandum of the Proposal for the Directive explains that 'the information obligation aims at empowering the subscribers to control and, where necessary, to object to ongoing data processing'. Recital 26 goes even further and states that service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done. This implies that service providers should not only provide initial information but also update the information when there is a change in the data processed or the duration of processing. *Subject of the information.* Art. 6(4) indicates that the service providers may inform either the subscriber or the user. In many cases it will however be impossible to inform the user when he/she is not known to the service provider. In some cases, such as in respect of internet access services, there might also be several users for a same service.

4. Traffic data processing for the purpose of marketing electronic communications services and for the provision of value added services (para. 3). (a) Purposes of processing allowed. Art. 6(3) allows the provider of a publicly available electronic communications service to retain and further process traffic data relating to subscribers and users for the purpose of marketing electronic communications services or of providing value added services. The marketing of electronic communications services may potentially concern services provided by the provider of a publicly available electronic communications service as well as services provided by third parties. Indeed, where the text of the Old Directive envisaged the processing of traffic data by the provider of a publicly available electronic communications service for the marketing of its own electronic communications services, the wording of the Directive uses the neutral terminology of 'marketing electronic communications services'. The Directive also extends the possibility of processing traffic data to the provision of 'value added services'. A definition of value added services is provided in art. 2, note 2 b). **(b) Selection of the traffic data.** Only the traffic data which are necessary for such services or marketing can be stored and processed for the period necessary to carry out these activities. The data should be erased or made anonymous after the provision of the service. **(c) Consent.** *Requirement of the consent of the user or of the subscriber.* Traffic data can only be processed for the purpose of marketing electronic communications services or of providing value added services provided that the subscriber or user to whom the data relate has given his or her prior consent. This would imply that in any case the service provider would need to identify whose data are processed (the subscriber's or the user's) and manage to obtain the consent of the data subject. Recital 31 seems however to be more nuanced when it states that 'whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will not only depend on the data to be processed and on the type of service to be provided but also on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it'. If we consider the example of an internet access provider offering customised services including value added services, it will be likely more appropriate to ask the consent from the subscriber at the moment of the subscription for the service if the content of the service cannot actually be adapted afterwards in consideration of the person using it (the subscriber or the user). On the other hand, when value added services can be customised by the user itself (for instance, by the GPS user or the voice telephony services users), there is no reason for not seeking to obtain his/her consent. *Definition of 'consent'.* As, mentioned in the comment of art. 2(2)(f), the consent of a user or subscriber referred to in the Directive has the same meaning as the data subject's consent as defined

and further specified in the Data Protection Directive, regardless of whether the latter is a natural or a legal person. According to recital 17, consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an internet website. *Right of withdrawal.* Moreover, users or subscribers must be given the possibility to withdraw their consent for the processing of traffic data at any time. This does not only mean that the user or subscriber has the right to withdraw his/her consent at any time but it also requires that he/she is given the effective possibility to do so. The withdrawal prevents the service provider from processing the data subject's data in the future. **(d) Information.** *Content of information.* In addition, the service provider must, in respect of para. 4, inform the subscriber or user of the types of traffic data which are processed, and of the duration and purposes of such processing. *Moment of information.* The information must be provided prior to obtaining the consent. *Subject of information.* With regard to the informed consent requirement, the duty of information appears to entail that at least the person who has to consent to the use of its data either for marketing purposes or for the provision of value added services will need to receive the information.

5. Other purposes of processing (para. 5). Art. 6(5) implicitly admits purposes of processing that are not envisaged under art. 6(1), (2) and (4). It indeed considers that persons handling customer enquiries or fraud detection are entitled to process traffic data. This explicit reference to activities not mentioned in the above paragraphs of art. 6 suggests that processing of these purposes is allowed. It is remarkable that while evoking these purposes, the Directive does not provide for any specific conditions with respect to the connected processing. The processing of these data will however be subject to the conditions set in the Data Protection Directive as far as they are personal data. With respect to fraud detection, it is moreover likely that only internal fraud with regard to the electronic communications services is concerned and not criminal investigation, which is reserved to public authorities (see comment on art. 15). Recital 29 appears to be even more restrictive and only to consider the processing of certain traffic data for fraud detection as it indicates that 'traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service'.

6. Persons entitled to process traffic data in framework of paras. 1, 2, 3 and 4 (para. 5). (a) The service provider's personnel. Art. 6(5) identifies the categories of personnel of the service provider who may carry out the processing. It further specifies that the processing must be restricted to what is necessary for the purposes of the sectors of activities mentioned. The processing of traffic data must be restricted to persons acting under the authority of the service provider and who need to process the data in the framework of their function, namely, handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications

services or the provision a value added service. As stated above, the right to process traffic data for the purpose of marketing electronic communications services or of providing value added services is only granted to the provider of publicly available electronic communications services and not to providers of the public communications networks. Therefore only the personnel acting under the authority of the providers of publicly available electronic communications services is entitled to process traffic data for this purpose. **(b) Communication to third parties.** Art. 6(5) does not envisage a possible communication of traffic data by the service provider to a third party. Recital 32 seems however to allow the communication of traffic data to a third party providing value added services when it states that 'where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data'. Art. 6(5) could be construed as allowing such communication provided that the value added service provider remains under the authority of the electronic communications service provider. Such interpretation would however create a level of protection for traffic data which is stronger than the one granted under art. 9 to location data, being more sensitive than traffic data. Indeed, communication of location data to a value added services provider is expressly allowed (see art. 9, note 3 b)). It is therefore reasonable to consider that traffic data may be forwarded to a provider of value added service without requiring that the latter remains under the authority of the service provider. In case of such a forwarding of data, the user or subscriber would need to receive specific information about the processing of the data without prejudice to the application of all other rules arising from the Data Protection Directive as to a communication of personal data (especially art. 6(b) of the Data Protection Directive). **(c) Subcontracting of services.** Art. 6(5) considers the processing of traffic data by persons acting under the authority of the service provider but does not envisage as such the subcontracting of part of or of the whole processing carried out by the service provider on traffic data to a processor (in the sense of art. 17 of the Data Protection Directive). Indeed the terms 'under the authority of' do not refer to the characteristics of a subcontracting of data processing to a processor. Art. 17(3) of the Data Protection Directive indeed does not strictly require the processor to act under the authority of the data controller but only specifies that the parties agree in a contract that the processor shall only act on instructions of the data controller. However, recital 32 explicitly regulates that 'where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in the [Data Protection Directive]'. Therefore, the communication of traffic data in

the framework of a processing agreement for the provision of value added services is not excluded. For instance, an internet service provider could subcontract a value added service consisting in an assistance to navigate on internet to a processor and, in this framework, could transfer the internet addresses requested by its subscriber. In such a case, the service provider is also required to inform the users and subscribers about the forwarding of their data before they give their consent where such consent is required (i.e., in case of provision of value added services).

7. Communication of traffic data to competent bodies (para. 6). According to para. 6, para. 1, 2, 3 and 5 apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes. This paragraph introduces an additional purpose, the settlement of disputes, of processing allowing the service provider to disclose traffic data to competent bodies and the competent bodies to process traffic data where such processing is in conformity with the applicable legislation. The consequences of the use of the terms 'without prejudice' are not very clear: would this paragraph allow the storage of data longer as permitted under paragraphs 1, 2, 3 and 5 in view of a possible communication to a competent body?

[Itemised billing]

Article 7

(1) Subscribers shall have the right to receive non-itemised bills.

(2) Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

General. Art. 7(1) gives the subscriber the right to obtain itemised bills for all services covered by the Directive and not only for voice telephony services as it was the case with the Old Directive or the Universal Service Directive (Booklet 1-4). The significance of this provision is unclear as it might mean that the offer of an itemised billing is only optional and submitted to the condition of the subscriber's request. Art. 7(2) encourages the Member States to take national measures in order to 'reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers'. *Consumers' v Privacy concerns – Possible solutions.* On that point precisely, consumer protection interests might diverge substantially from privacy concerns. The problem is delicate insofar the subscriber might be different from the user, for example, within a family or a company. In that context the itemised bill might be a way to have a look at the activities

of an employee or a spouse or child. To solve this delicate problem, recital 33 does suggest certain methods like the use of optional services and payment mechanisms (e.g. prepaid calling cards to be inserted in the terminal equipment) which will permit use of the terminal equipment anonymously and without traces in the bill. Furthermore, at the request of the Working Party, the same recital makes reference to the French solution enacted by Decree No. 2002-36 of 8 January 2002 which requires voice telephony service providers to offer a service option whereby the last four digits of the called numbers do not appear on the bill.

[Presentation and restriction of the calling and connected line identification]

Article 8

(1) Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

(2) Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

(3) Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

(4) Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification of the calling user.

(5) Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

(6) Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in Paragraphs 1, 2, 3 and 4.

1. General. This article regulates in detail the conditions under which information about the participants in a telephone conversation may be disclosed