ARTICLE 29 DATA PROTECTION WORKING PARTY

xxxx/09/EN
WP 163

Opinion 5/2009 on online social networking

Adopted on 12 June 2009

Table of contents

Executive Summary 3
1. Introduction 4
2. Definition of a "social network service (SNS)" and business model 4
3. Application of the Data Protection Directive 5
3.1 Who is the data controller? 5
3.2 Security and default privacy settings 7
3.3 Information to be provided by SNS 7
3.4 Sensitive Data 8
3.5 Processing data of non-members 8
3.6 Third party access 8
3.7 Legal grounds for direct marketing 9
3.8 Retention of data 10
3.9 Rights of the users 11
4. Children and minors 11
5. Summary of obligations/rights 12

Executive Summary

This Opinion focuses on how the operation of social networking sites can meet the requirements of EU data protection legislation. It principally is intended to provide guidance to SNS providers on the measures that need to be in place to ensure compliance with EU law.

The Opinion notes that SNS providers and, in many cases, third party application providers, are data controllers with corresponding responsibilities towards SNS users. The Opinion outlines how many users operate within a purely personal sphere, contacting people as part of the management of their personal, family or household affairs. In such cases, the Opinion deems that the 'household exemption' applies and the regulations governing data controllers do not apply. The Opinion also specifies circumstances whereby the activities of a user of an SNS are not covered by the 'household exemption'. The dissemination and use of information available on SNS for other secondary, unintended purposes is of key concern to the Article 29 Working Party. Robust security and privacy-friendly default settings are advocated throughout the Opinion as the ideal starting point with regard to all services on offer. Access to profile information emerges as a key area of concern. Topics such as the processing of sensitive data and images, advertising and direct marketing on SNS and data retention issues are also addressed.

Key recommendations focus on the obligations of SNS providers to conform with the Data Protection Directive and to uphold and strengthen the rights of users. Of paramount importance, SNS providers should inform users of their identity from the outset and outline all the different purposes for which they process personal data. Particular care should be taken by SNS providers with regard to the processing of the personal data of minors. The Opinion recommends that users should only upload pictures or information about other individuals, with the individual's consent and considers that SNS also have a duty to advise users regarding the privacy rights of others.

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 and 30 paragraphs 1 (a) and 3 of that Directive, and Article 15 paragraph 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. Introduction

The evolution of web communities and hosted services such as social network services ("SNS") is a relatively recent phenomenon, with the number of users of these sites continuing to multiply at an exponential rate.

The personal information a user posts online, combined with data outlining the users actions and interactions with other people, can create a rich profile of that person's interests and activities. Personal data published on social network sites can be used by third parties for a wide variety of purposes, including commercial purposes, and may pose major risks such as identity theft, financial loss, loss of business or employment opportunities and physical harm.

The Berlin International Working Group on Data Protection in Telecommunications adopted the *Rome Memorandum*[2] in March 2008. The Memorandum analyses the risks for privacy and security posed by social networks and provides guidelines for regulators, providers and users. The recently adopted Resolution on Privacy Protection in Social Network Services[3] also addresses challenges brought about by the SNS. The Working Party also takes into account the position paper published by the European Network and Information Security Agency (ENISA) "*Security Issues and Recommendations for Online Social Networks,*"[4] in October 2007 aimed at regulators and providers of social networks.

2. Definition of a "social network service (SNS)" and business model

SNS can broadly be defined as online communication platforms which enable individuals to join or create networks of like-minded users. In the legal sense, social networks are information society services, as defined in Article 1 paragraph 2 of Directive 98/34/EC as amended by Directive 98/48/EC. SNS share certain characteristics:

---

1 Official Journal no. L281 of 23/11/1995, p. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

3 Adopted at the 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg, 17;10.2008, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf

4 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

- users are invited to provide personal data for the purpose of generating a description of themselves or 'profile'.

- SNS also provide tools which allow users to post their own material (user-generated content such as a photograph or a diary entry, music or video clip or links to other sites[5]);

- 'social networking' is enabled using tools which provide a list of contacts for each user, and with which users can interact.

SNS generate much of their revenue through advertising which is served alongside the web pages set up and accessed by users. Users who post large amounts of information about their interests on their profiles offer a refined market to advertisers wishing to serve targeted advertisements based on that information.

It is therefore important that SNS operate in a way which respects the rights and freedoms of users who have a legitimate expectation that the personal data they disclose will be processed according to European and national data protection and privacy legislation.

3. Application of the Data Protection Directive

The provisions of the Data Protection Directive apply to SNS providers in most cases, even if their headquarters are located outside of the EEA. The Article 29 Working Party refers to its earlier opinion on search engines for further guidance on the issues of establishment and use of equipment as determinants for the applicability of the Data Protection Directive and the rules subsequently triggered by the processing of IP addresses and the use of cookies.[6]

3.1 Who is the data controller?

SNS providers

SNS providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the "basic" services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes - including advertising provided by third parties.

Application providers

Application providers may also be data controllers, if they develop applications which run in addition to the ones from the SNS and users decide to use such an application.

Users

In most cases, users are considered to be data subjects. The Directive does not impose the duties of a data controller on an individual who processes personal data *"in the course of a purely personal or household activity"* - the so-called "household exemption". In some instances, the activities of a user of an SNS may not be covered by the household exemption and the user might be considered to have taken on some of the responsibilities of a data controller. Some of these instances are developed below:

---

5 In these cases where SNS provide electronic communications services, provisions of ePrivacy Directive 2002/58 will also apply.

6 WP148, "Opinion 1/2008 on data protection issues related to search engines".

3.1.1. Purpose and nature

A growing trend of SNS is the "*shift from "Web 2.0 for fun" to Web 2.0 for productivity and services*"[7] where the activities of some SNS users may extend beyond a purely personal or household activity, for example when the SNS is used as a collaboration platform for an association or a company. If an SNS user acts on behalf of a company or association, or uses the SNS mainly as a platform to advance commercial, political or charitable goals, the exception does not apply. Here, the user assumes the full responsibilities of a data controller who is disclosing personal data to another data controller (SNS) and to third parties (other SNS users or potentially even other data controllers with access to the data). In these circumstances, the user needs the consent of the persons concerned or some other legitimate basis provided in the Data Protection Directive.

Typically, access to data (profile data, postings, stories…) contributed by a user is limited to self-selected contacts. In some cases however, users may acquire a high number of third party contacts, some of whom he may not actually know. A high number of contacts could be an indication that the household exception does not apply and therefore that the user would be considered a data controller.

3.1.2. Access to profile information

SNS should ensure privacy-friendly and free of charge default settings are in place restricting access to self-selected contacts.

When access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS[8] or the data is indexable by search engines, access goes beyond the personal or household sphere. Equally, if a user takes an informed decision to extend access beyond self-selected 'friends' data controller responsibilities come into force. Effectively, the same legal regime will then apply as when any person uses other technology platforms to publish personal data on the web[9]. In several Member States, the lack of access restrictions (thus the public character) means the Data Protection Directive applies in terms of the internet user acquiring data controller responsibilities[10].

It should be kept in mind that, even if the household exemption does not apply, the SNS user may benefit from other exemptions such as the exemption for journalistic purposes, artistic or literary expression. In those cases, a balance needs to be struck between freedom of expression and the right to privacy.

3.1.3 Processing of third party data by users

The application of the household exemption is also constrained by the need to guarantee the rights of third parties, particularly with regard to sensitive data. In addition, it must be noted that even if the household exemption applies, a user might be liable according to general

---

7 "Internet of the future: Europe must be a key player" speech from Ms Reding, European Commissioner for Information Society and Media during the meeting Future of the Internet initiative of the Lisbon Council, Brussels, 2 February 2009

8 or when it can be argued that no actual selection is being made in accepting contacts, i.e the users accepts "contacts" regardless of the connection they have

9 Such as with publishing platforms that are not SNS, or with self-hosted software.

10 In its Satamedia judgment the ECJ rules inversely in paragraph 44: "*It follows that the latter exception must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals (see Lindqvist, paragraph 47). That clearly does not apply to the activities of Markkinapörssi and Satamedia, the purpose of which is to make the data collected accessible to an unrestricted number of people.*"

provisions of national civil or criminal laws in question (e.g. defamation, liability in tort for violation of personality, penal liability).

3.2 Security and default privacy settings

Secure processing of information is a key element of trust in SNS. Controllers must take the appropriate technical and organisational measures, 'both at the time of the design of the processing system and at the time of the processing itself' to maintain security and prevent unauthorised processing, taking into account the risks represented by the processing and the nature of the data[11].

An important element of the privacy settings is the access to personal data published in a profile. If there are no restrictions to such access, third parties may link all kinds of intimate details regarding the users, either as a member of the SNS or via search engines. However, only a minority of users signing up to a service will make any changes to default settings. Therefore, SNS should offer privacy-friendly default settings which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties. Restricted access profiles should not be discoverable by internal search engines, including the facility to search by parameters such as age or location. Decisions to extend access may not be implicit[12], for example with an "opt-out" provided by the controller of the SNS.

3.3 Information to be provided by SNS

SNS providers should inform users of their identity and the different purposes for which they process personal data according to the provisions laid out in Article 10 of the Data Protection Directive including, but not limited to:

- usage of the data for direct marketing purposes;
- possible sharing of the data with specified categories of third parties;
- an overview on profiles: their creation and chief data sources;
- the use of sensitive data.

The Working Party recommends that:

- SNS providers provide adequate warnings to users about the privacy risks to themselves and to others when they upload information on the SNS;
- SNS users should also be reminded that uploading information about other individuals may impinge upon their privacy and data protection rights;
- SNS users should be advised by SNS that if they wish to upload pictures or information about other individuals, this should be done with the individual's consent[13].

---

11 Article 17 and Recital 46 of the Data Protection Directive.

12 The Report and Guidance on Privacy in Social Network Services ("Rome Memorandum") indicates risks such as "The misleading notion of community", p2, "Giving away more personal information than you think you do", p3. A computer security company warns an important SNS about default access to members within the same geographical location : http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html

13 This could be made easier by introducing tagging management tools within social network websites, e.g. by making available areas in a personal profile to indicate the presence of a user's name in tagged images or

3.4 Sensitive Data

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life is considered sensitive. Sensitive personal data may only be published on the Internet with the explicit consent from the data subject or if the data subject has made the data manifestly public himself.[14]

In some EU Member States, images of data subjects are considered a special category of personal data since they may be used to distinguish between racial/ethnic origins or may be used to deduce religious beliefs or health data. The Working Party in general does not consider images on the Internet to be sensitive data[15], unless the images are clearly used to reveal sensitive data about individuals.

As data controllers, SNS may not process any sensitive data about SNS members or non-members without their explicit consent[16]. If an SNS includes in the profile form of users any questions relating to sensitive data, the SNS must make it very clear that answering such questions is completely voluntary.

3.5 Processing data of non-members

Many SNS allow users to contribute data about other people, such as adding a name to a picture, rating a person, listing the "people I have met/want to meet" at events. This tagging may also identify non-members. However, the processing of such data about non-members by the SNS may only be performed if one of the criteria laid down in Article 7 of the Data Protection Directive is fulfilled.

In addition, the creation of pre-built profiles of non-members through the aggregation of data that is independently contributed by SNS users, including relationship data inferred from uploaded address books, lacks a legal basis.[17]

Even if the SNS had the means to contact the non-user and inform this non-user about the existence of personal data relating to him/her, a possible e-mail invitation to join the SNS in order to access these personal data would violate the prohibition laid down in Article 13.4 of the ePrivacy Directive on the sending of unsolicited electronic messages for direct marketing purposes.

3.6 Third party access

3.6.1 SNS-mediated access

In addition to the core SNS service, most SNS offer users additional applications provided by third party developers which also process personal data.

SNS should have the means to ensure that third party applications comply with the Data Protection and ePrivacy Directives. This implies, in particular, that they provide clear and

---

videos waiting for consent, or setting expiration times for tags that have not received consent by the tagged individual.

14 Member States may lay down exemptions from this rule; see Article 8.2 (a) second sentence and Article 8 4 of the Data Protection Directive.

15 The publication of images on the Internet does however raise increasing privacy concerns as facial recognition technologies improve.

16 consent has to be free, informed and specific

17 Recital 38 of the Data Protection Directive specifies: "*Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection.*" For some SNS, the publication of profiles of non-members allegedly has become an important way of marketing their "services".

specific information to users about the processing of their personal data and that they only have access to necessary personal data. Therefore, layered access should be offered to third party developers by the SNS so they can opt for a mode of access that is intrinsically more limited. SNS should ensure furthermore that users may easily report concerns about applications.

3.6.2 User-mediated third party access

SNS sometimes allow users to access and update their data with other applications. For example users might be able to:

- read and post messages to the network from their mobile phone;
- synchronize the contact data of their friends in the SNS with their address book on a desktop computer;
- update their status or location in the SNS automatically by using another website.

SNS publish the way this software can be written in the form of an "Application Programming Interface" ("API"). This enables any third party to write software to perform these tasks, and allow users to freely choose between several third party providers[18]. When offering an API that enables access to contacts' data, SNS should:

- provide for a level of granularity that lets the user choose an access level for the third party that is only just sufficient to perform a certain task.

When accessing personal data via third party's API on behalf of a user, third party services should:

- process and store data no longer than necessary to perform a specific task;
- perform no operations on imported user contacts' data other than personal usage by the contributing user.

3.7 Legal grounds for direct marketing

Direct marketing is an essential part of the SNS business model; different marketing models can be used by SNS. Nevertheless, marketing using users' personal data should comply with relevant provisions of both Data Protection and ePrivacy Directive[19].

Contextual marketing is tailored to the content that is viewed or accessed by the user[20.]

Segmented marketing consists in serving advertisements to targeted groups of users[21]; a user is placed in a group according to the information he has directly communicated to the SNS[22].

Finally, *behavioural marketing* selects the advertisements based on the observation and analysis of the users' activity over time. These techniques may be subject to different legal requirements, depending on the applicable legal grounds and the characteristics of the

[18] While "API" is a broad technical term, here API refers to access on behalf of a user, i.e. users need to give their login credentials to the software, so that it can act on their behalf.

[19] The Working Party intends to address the different aspects of online advertising in a separate document in the near future.

[20] e.g. if the page which is displayed mentions the word "Paris", the advertisement could concern a restaurant in this city

[21] each group being defined by a set of criteria

[22] e.g. when he registered with the service

techniques used. The Working Party recommends not using sensitive data in behavioural advertising models, unless all legal requirements are met.

Whatever model or combination of models is used, advertisements can either be served directly by the SNS (the SNS provider acts here as a broker) or by a third party advertiser. In the first case, personal data of the users do not need to be disclosed to third parties. In the second case however, the third party advertiser might process personal data about the users e.g. if it processes the IP address of the user and a cookie that was placed on the user's computer.

3.8 Retention of data

SNS fall outside the scope of the definition of electronic communication services provided in Article 2 letter c) of the Framework Directive (2002/21/EC). SNS providers may offer additional services that fall under the scope of an electronic communications service such as a publicly accessible email service. Such a service will be subject to the provisions of the e-Privacy Directive and the Data Retention Directive.

Some SNS allow their users to send invitations to third parties. The prohibition on the use of electronic mail for the purposes of direct marketing does not apply to personal communications. In order to comply with the exception for personal communications, an SNS must comply with the following criteria:

- no incentive is given to either sender or recipient;
- the provider does not select the recipients of the message;[23]
- the identity of the sending user must be clearly mentioned;
- the sending user must know the full content of the message that will be sent on his behalf.

Some SNS also retain identification data of users who were banned from the service, to ensure that they cannot register again. In that case, these users must be informed that such processing is taking place. In addition, the only information that may be retained is identification information, and not the reasons why these persons were banned. This information should not be retained for more than one year.

Personal data communicated by a user when he registers to a SNS should be deleted as soon as either the user or the SNS provider decides to delete the account[24]. Similarly, information deleted by a user when updating his account should not be retained. SNS should notify users before taking these steps with the means they have at their disposal to inform users about these retention periods. For security and legal reasons, in specific cases, it could be justifiable to store updated or deleted data and accounts for a defined period of time in order to help prevent malicious operations resulting from identity theft and other offences or crimes.

When a user does not use the service for a defined period of time, the profile should be set to inactive, i.e. no longer visible to other users or the outside world, and after another period of time the data in the abandoned account should be deleted. SNS should notify users before taking these steps with whatever means they have at their disposal.

---

[23] i.e. the practice by some SNSs to send invitations indiscriminately to the entire address book of a user is not allowed

[24] According to Article 6 para 1e) of the Data Protection Directive, data must be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."*

3.9 Rights of the users

SNS should respect the rights of the individuals concerned by the processing according to the provisions laid out in Articles 12 and 14 of the Data Protection Directive.

Access and rectification rights of users are not limited to the users of the service but to any natural person whose data are processed[25]. Members and non-members of SNS must have a means to exercise their right of access, correction and deletion. The homepage of SNS sites should clearly refer to the existence of a "complaint handling office" set up by the SNS provider to deal with data protection and privacy issues and complaints by both members and non-members.

Article 6 para 1 letter c) of the Data Protection Directive requires the data to be *"adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"*. In this context, it can be observed that SNS may need to register some identifying data about members but does not need to publish the real name of members on the Internet. Therefore, SNS should consider carefully if they can justify forcing their users to act under their real identity rather than under a pseudonym. There are strong arguments in favor of giving users choice in this respect and in at least one Member State, this is a legal requirement. The arguments are particularly strong in the case of SNS with wide membership.

Article 17 of the Data Protection Directive requires that the controller implements appropriate technical and organizational security measures to protect personal data. In particular, such security measures include access control and authentication mechanisms which can still be implemented if pseudonyms are used.

4. Children and minors

A large proportion of SNS services are utilised by children/minors. The Working Party's Opinion WP147[26] focused on the application of data protection principles in the school and educational environment. The Opinion emphasised the need for taking into account the best interest of the child as also set out in the UN Convention on the Rights of the Child. The Working Party wishes to stress the importance of this principle also in the context of SNS.

Some interesting initiatives[27] have been undertaken by Data Protection Authorities world wide which focus mostly on awareness-raising regarding SNS and possible risks. The Working Party encourages further research on how to address the difficulties surrounding adequate age verification and proof of informed consent in order to better address these challenges.

Based on the considerations made so far, the Working Party believes that a multi-pronged strategy would be appropriate to address the protection of children's data in the SNS context. Such a strategy might be based on:

- awareness raising initiatives, which are fundamental to ensure the active involvement of children (via schools, the inclusion of DP-basics in educational curricula, the creation of ad-hoc educational tools, the collaboration of national competent bodies);

---

25 e.g. instance, it is the case if this person's email address was used by the SNS service to send him an invitation

26 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf

27 For example, the Portuguese "Dadus" initiative http://dadus.cnpd.pt/, the Danish Chat Check Badge, http://www.fdim.dk/

- fair and lawful processing with regard to minors such as not asking for sensitive data in the subscription forms, no direct marketing aimed specifically at minors, the prior consent of parents before subscribing, and suitable degrees of logical separation between the communities of children and adults;

- implementation of Privacy Enhancing Technologies (PETs) - e.g. privacy-friendly settings by default, pop-up warning boxes at appropriate steps, age verification software);

- self-regulation by providers, to encourage the adoption of codes of practice that should be equipped with effective enforcement measures, also disciplinary in nature;

- if necessary, ad-hoc legislative measures to discourage unfair and/or deceptive practices in the SNS context.

5. Summary of obligations/rights

Applicability of EC Directives

1. The Data Protection Directive generally applies to the processing of personal data by SNS, even when their headquarters are outside of the EEA.

2. SNS providers are considered data controllers under the Data Protection Directive.

3. Application providers might be considered data controllers under the Data Protection Directive.

4. Users are considered data subjects vis-à-vis the processing of their data by SNS.

5. Processing of personal data by users in most cases falls within the household exemption. There are instances where the activities of a user are not covered by this exemption.

6. SNS fall outside of the scope of the definition of electronic communication service and therefore the Data Retention Directive does not apply to SNS.

Obligations of SNS

7. SNS should inform users of their identity, and provide comprehensive and clear information about the purposes and different ways in which they intend to process personal data.

8. SNS should offer privacy-friendly default settings.

9. SNS should provide information and adequate warning to users about privacy risks when they upload data onto the SNS.

11. Users should be advised by SNS that pictures or information about other individuals, should only be uploaded with the individual's consent.

12. At a minimum, the homepage of SNS should contain a link to a complaint facility, covering data protection issues, for both members and non-members.

13. Marketing activity must comply with the rules laid down in the Data Protection and ePrivacy Directives.

14. SNS must set maximum periods to retain data on inactive users. Abandoned accounts must be deleted.

15. With regard to minors, SNS should take appropriate action to limit the risks.

Rights of Users

16. Both members and non-members of SNS have the rights of data subjects if applicable, according to the provisions of Article 10 – 14 of the Data Protection Directive.

17. Both members and non-members should have access to an easy-to-use complaint handling procedure set up by the SNS.

18. Users should, in general, be allowed to adopt a pseudonym.

Done at Brussels, on 12 June 2009

For the Working Party
The Chairman
Alex TÜRK