ARTICLE 29 DATA PROTECTION WORKING PARTY

Brussels, 12 May 2010
D(2010) 7280

Signatories of the "Safer Social Networking Principles for the EU"

Dear Madam, dear Sir,

I am writing to you as chairman of the "Article 29 Data Protection Working Party". The Working Party has been established by Article 29 of Directive 95/46/EC (Data Protection Directive). It consists of all Data Protection Authorities of the European Economic Area and is the independent EU Advisory Body on Data Protection and Privacy.

I welcome the fact that you have signed and adhered to the "Safer Social Networking Principles for the EU". The Working Party supports these principles and any serious effort to effectively self-regulate this area. Furthermore we would like to draw your attention to the Working Party's Opinion 5/2009 on online social networking of 12 June 2009[1].

In this Opinion, the Working Party explains the regulations providers of social network services (SNS) have to comply with under the EU regulatory framework for privacy and data protection. Please note that while the "Safer Social Networking Principles for the EU" to which your company is a signatory addresses some of the issues raised in the Working Paper, it does not cover all of them. Please note that the measures set out in the opinion and below do – unlike the "Safer Social Networking Principles for the EU" – apply regardless of the age of the targeted users of an SNS.

In addition to what is laid out in the opinion, The Working Party would like to highlight the following issues which have emerged since the adoption of the Opinion in June 2009, and specifically from a hearing the Working Party has held on privacy practices of SNS with three providers of such services on 30 November 2009:

- protection of minors/parents' consent: While – with regard to the processing of personal data of minors – providers of SNS need to ensure minors have the consent of their parents before participating in an SNS, the Working Party acknowledges there is not yet a systematic way to verify this consent in a way that is not privacy-intrusive. However, the Working Party encourages providers to continue their efforts in providing a safe online environment for minors.
- third party applications: Providers of SNS need to ensure that it is transparent to users who is the provider of a specific service on a SNS. This goes especially for any services not offered by the provider of the SNS itself, but by other parties ("third-party-applications"). At the same time,

[1] Opinion 163; available in the official languages of the EU; http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm)

providers of any third-party applications must inform users about their identity, and the extent and purposes of any data processing. SNS providers need to take measures to ensure that providers of third-party-applications comply with the applicable legislative framework on privacy. Specifically, providers of SNS need to be able to ban third party applications that do not comply with data protection laws. Providers of SNS should grant users a maximum of control about which profile data can be accessed by a third party application on a case-by-case basis.

The Working Party underlines that there is no legal ground for granting a third party application access to the data of user contacts of the user who installs the application, unless the processing can be considered a purely personal or household activity. For the latter case to be applicable there can be no further processing by the third party than the processing explicitly requested by the user who installs the application and all data, including identifiers of the user's contacts, needs to be deleted after the processing.

- as with SNS, pseudonymous use should also be offered, where appropriate, for third party applications, including the opportunity to use different pseudonyms for different applications.

- default settings for access to profile information and connections list: The Working Party underlines the importance of privacy friendly default settings as described in the opinion (cf. 3.2 Security and default privacy settings, page 7). The Working Party acknowledges the efforts of some SNSes who have implemented a policy that makes users aware of any decision to extend access to their profile.

  Pursuant to the Data Protection Directive, the default privacy settings offered by SNSs should not allow access beyond self-selected contacts and any further access should be an explicit choice by the user. This approach allows for a maximum of control by the user over who has access to his or her profile information and connections list, regardless of the age of a subscribing user (while principle 3 of the "Safer Social Networking Principles" is limited to services targeted at minors).

  Apart from restricting access to their profile content, users should have the right to limit the visibility of their presence on the network.

- use of third party personal data contained in user profiles: Providers of SNS should be aware that there is no legal basis for using personal data of a third party contained in a user profile (e.g. an e-mail-address) for their own marketing purposes, if that third party has not given it free and unambiguous consent.

Sincerely yours,

Jacob KOHNSTAMM
Chairman of the Article 29 Working Party