International Working Group
on Data Protection
in Telecommunications

675.40.11

The Granada Charter of Privacy in a Digital World[1]

47th meeting, 15-16 April 2010, Granada (Spain)

The international community has been dealing with questions of the information age for a long time. In the course of recent decades the following international documents have been adopted[2]:

- European Convention on Human Rights of 4 November 1950
- OECD Guidelines on the protection of privacy and transborder flows of personal data of 23 September 1980
- Council of Europe Convention No. 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data
- United Nations Guidelines for the regulation of computerised personal data files, adopted by the General Assembly Resolution 45/90 of 14 December 1990
- European Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Charter of Fundamental Rights of the European Union of 7 December 2000
- European Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
- APEC privacy framework of November 2004
- Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data of 5 November 2009[3]

In the interactive world individuals are no longer merely users, but they are also net citizens with inalienable rights. Moreover, they are also responsible for the contents they are publishing about themselves and others. Privacy and data protection are crucial elements of a democratic information society. The following principles should help users, providers and public authorities to facilitate a free flow of information whilst respecting the dignity, privacy and data protection of individuals. It is evi-

[1] Due to incompatibilities with the national legal situation in Sweden the Swedish Data Protection Board has abstained from the adoption of this working paper.

[2] In addition the following guidelines and resolutions have been published: International Working Group on Data Protection in Telecommunications, http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf, 13-14 September 2000, Berlin; International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services – "Rome Memorandum" (http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491), 3-4 March 2008, Rome; International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy Protection in Social Network Services (http://www.bfdi.bund.de/cae/servlet/contentblob/416902/publicationFile/24968/2008SocialNetwork.pdf), Strasbourg, 17 October 2008; International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy Protection an Search Engines (http://www.bfdi.bund.de/cae/servlet/contentblob/416912/publicationFile/24983/ConferenceOfInternationalDataProtectionCommissioners2006-ResolutionSearchEngines.pdf), London, 2-3 November 2006

[3] Adopted by the International Conference of Data Protection and Privacy Commissioners on 5 November 2009; cf. http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24464/20091.pdf

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

dent that tensions may occur between these principles and other important values such as freedom of expression, security and property rights. In each case every measure to enforce these competing objectives must be balanced with those of data protection and privacy.

Subscribers to and Users of Communications Services should

1. be careful when publicising personal data related to themselves or to other individuals and be aware that it is much more difficult to remove data from the Internet than to release it
2. undertake all appropriate efforts - for example obtain prior consent - to ensure the rights of any other person prior to the disclosure or publication of that person's information and to respect his or her decision to withdraw given consent
3. have the fundamental right to have their lawful use of communications services private, unobserved, not intercepted and not monitored
4. have the opportunity to use services anonymously or under a pseudonym and to use encrypted communications, especially when signing in and out
5. have the right to control the amount of personal information and the uses to which such personal information may be put
6. have the right to be informed as to any proposed processing or secondary uses of their personal data and - as appropriate - to give explicit consent (opt-in) and subsequently withdraw consent (opt-out) to all such proposed disclosures or secondary uses
7. have the right to opt-in to and subsequently opt-out of the collection and use of any data concerning their use of the services.

Information and Communications Service Providers should

1. ensure that users of communications services are provided with facilities which meet the requirements on use identified above
2. ensure that such facilities are easy to use and well described in user guidance
3. respond promptly and accurately to all requests from individuals for details about the information which is processed about them and to whom such information may be disclosed and provide them with electronic means such as online access to the personal data relating to them
4. ensure that any information collected about users is the minimum needed to provide a service and is not retained for longer than necessary for that service to be provided
5. set up specific safeguards to protect sensitive information such as traffic and location data
6. guarantee the secrecy of communications
7. implement appropriate technical and organisational measures to safeguard the security of their services
8. inform subscribers or registered users of communications services in any case where there is a particular risk of a security breach, of such a risk and any possible remedies, and when a privacy breach has actually occured.

Public Authorities[4] should

[4] This includes, as appropriate, legislators

1. be open and transparent as to the processing of all personal information
2. refrain from any observation, interception or monitoring of communications unless it is strictly necessary for law enforcement purposes based on a specific legal basis
3. ensure that individuals of all generations and literacy are able to have access to the skills necessary to enable them to participate fully in the digital communications age
4. ensure that anyone who is not able or does not wish to participate in the use of electronic information and means of communication has the opportunity to access public services without disproportionate disadvantage
5. enforce user rights and the right of privacy and data protection in the use of interactive services and give the data subjects effective remedies.