



AGENDA ITEM 8 : Protection of Privacy and Personal Data in Electronic Communications

**Country Session: The Republic of TURKEY
13-14 July 2006**



Content

- Legislation
- Security
- Confidentiality
- Personal Data
- Use of Traffic Data
- Use of Location Data
- Public Subscriber Directories
- Unsolicited Communications
- Spy-ware and cookies
- Data retention
- Forthcoming Issues



LEGISLATION



Legislation-I

- Turkish Criminal Code (2004)

- By-law on Personal Information Processing and Privacy in the Telecommunications Sector (2004)



Legislation-II

- The aim of by-law:
 - To ensure processing of personal information and protection of privacy.

- By-law:
 - Reflects developments in electronic communications services
 - Provides an equal level of protection
 - Technology neutral



SECURITY



Security-I

- Operators must take appropriate measures to guarantee security of services.

- These measures include technical and organizational aspects.



Security-II

In case of a particular risk in the network, service providers inform the subscribers:

- concerning such risk,
- scope of the measures,
- any possible remedies.



Confidentiality

- Listening, tapping, storage, stopping and supervision of communications by third parties are strictly prohibited.
- Except:
 - if the permission of all the parties involving in communication is taken
 - the cases depending on laws and court orders.
- Tapping, storage and supervision of related traffic data not consistent with the aim of the service are also strictly prohibited.



Personal Data

- Recording personal data illegally shall be punished.

- Distribution or obtaining the personal data or submission to unauthorized persons shall be punished.



TRAFFIC DATA



Use of Traffic Data-I

- Processing of traffic data is limited with people working in a department
 - performing billing,
 - organizing traffic,
 - dealing with customer relationships,
 - fraud detection,
 - marketing electronic telecommunications services,
 - providing value added services.

- Traffic data can be given to a court or an authorized real or legal entity for dispute resolutions related with interconnection and billing.



Use of Traffic Data-II

- Operators can use traffic data for marketing and value added services:
 - With the permission of users,
 - Within the scope and period required for marketing,
 - By informing users about the period of the process.

- Permission can be withdrawn by users at any time.



Itemised billing

- Subscribers have a right to receive non-itemised bills.
- Subscribers have a right to receive itemised bills.



LOCATION DATA



Use of Location Data-I

- Processed only
 - When they are made anonymous.
 - If there is no application from subscribers for not using their location data.

- Give subscribers full information about:
 - Type of location data.
 - Time and purpose of the processing of location data.



Use of Location Data-II

- At any time, subscribers or users can withdraw their consent to the processing.

- For the purpose of responding to emergency calls:
Information including location data and identity of the caller line shall be kept and made accessible.



PUBLIC SUBSCRIBER DIRECTORIES



Public Subscriber Directories-I

- Operators inform subscribers about the purpose of publishing written and electronic subscriber directories.
 - Free of charge,
 - Prior to registration.

- Subscribers are always free to request correction, verification or exclusion of their subscriber information in the directories without charge.



Public Subscriber Directories-II

- Further consent is required for other than access to personal information based on names and surnames of subscribers.
- Subscribers other than natural persons have an equal rights as a natural person.



Unsolicited Communications

- In the event of using the automated calling systems for direct marketing:
 - Subscribers have a right to refuse receiving further messages.
 - Refusing the messages by a simple way and without charge.

- Electronic mails if,
 - Sent for direct marketing and
 - Disguising the identity of sender or
 - Not providing the recipient a valid address, shall be blocked.



Spy-ware and cookies

- A person who impedes a data-processing system or makes damage to the system shall be punished.

- A person who harms, destroys, alters or prevents to access data in a data-processing system and put data in or transfer data from data-processing system shall be punished.



Data retention

- If a subscriber requests tracing of malicious or nuisance calls, operators shall store and make available the data containing the identification of the calling subscribers for a year.

- This provision includes:
 - Mobile operators
 - Fixed operators
 - Long distance operators.



Forthcoming Issues

- Draft Electronic Communications Law

- Revision of Secondary Legislation
 - 2006/24 EC Directive provisions will be considered.



Thank you...