



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 20 April 2009**

**8849/09**

---

**Interinstitutional File:  
2007/0248 (COD)**

---

**LIMITE**

**TELECOM 76  
MI 160  
COMPET 213  
DATAPROTECT 29  
CONSOM 80  
CODEC 556**

**NOTE**

---

from : Presidency  
to : Coreper  
No. prev. doc. : 8365/09 TELECOM 68 MI 140 COMPET 188 DATAPROTECT 23 CONSOM  
71 CODEC 487  
Nos. Cion prop. : 15387/07 TELECOM 151 MI 298 COMPET 392 CONSOM 133 CODEC 1297  
15422/08 TELECOM 186 MI 427 COMPET 456 DATAPROTECT 88  
CONSOM 170 CODEC 1507

---

Subject : **Review of the Regulatory Framework for electronic communications  
networks and services**

Proposal for a Directive of the European Parliament and of the Council amending  
Directive 2002/22/EC on universal service and users' rights relating to electronic  
communications networks, Directive 2002/58/EC concerning the processing of  
personal data and the protection of privacy in the electronic communications  
sector and Regulation (EC) No 2006/2004 on consumer protection cooperation

- Preparation of the next informal dialogue

---

Delegations will find attached the compromise proposals from the Presidency in view of Coreper on  
21 April 2009.

**Outstanding issues**  
**CITIZENS' RIGHTS DIRECTIVE**  
**COREPER I – 21 April 2009**

<b>Presidency proposal following COREPER 7 April 2009</b>	<b>EP proposal</b>	<b>Presidency compromise proposal 21 April 2009</b>
---	--------------------	---

**ePRIVACY DIRECTIVE**

<b>Art. 5(3)</b>	<b>Art. 5(3)</b>	<b>Art. 5(3)</b>
<p>3. Member States shall ensure that the storing of information, or <u>gaining</u> access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned <del>has given his/her prior consent, which may be given by way of using the appropriate settings of a browser or another application, after having been</del> is provided with clear and comprehensive information in</p>	<p>3. Member States shall ensure that the storing of information, or gaining access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing and is offered the right to <b><u>refuse</u></b> such processing by the</p>	<p>3. Member States shall ensure that the storing of information, or gaining access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing and is offered the right to <b><u>refuse</u></b> such processing by the</p>

<p>accordance with Directive 95/46/EC, inter alia about the purposes of the processing <u>and is offered the right to <b>refuse</b> such processing by the data controller.</u></p> <p>When storing information in the terminal equipment of a subscriber or user on which there was no information already stored by the data controller, the data controller shall display or send an appropriate information message. This information message shall be easily noticeable by the subscriber or user and shall describe the processing and its purposes and inform of the possibility to refuse such processing.</p> <p>This shall not prevent any technical storage or access for the sole purpose of carrying out <u><b>or facilitate</b></u> the transmission of a communication over an electronic communications network, or as strictly necessary in order to <del>provide</del> <u><b>for the provider of</b></u> an information society service</p>	<p>data controller.</p> <p>When storing information in the terminal equipment of a subscriber or user on which there was no information already stored by the data controller, the data controller shall display or send an appropriate information message. This information message shall <del>be</del> <u><b>remain</b></u> easily noticeable by the subscriber or user and shall describe the processing and its purposes and inform of the possibility to refuse such processing.</p> <p>This shall not prevent any technical storage or access for the sole purpose of carrying out <del>or</del> <u><b>facilitate</b></u> the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested</p>	<p>data controller.</p> <p>When storing information in the terminal equipment of a subscriber or user on which there was no information already stored by the data controller, the data controller shall display or send an appropriate information message. This information message shall <del>be</del> <u><b>remain</b></u> easily noticeable by the subscriber or user and shall describe the processing and its purposes and inform of the possibility to refuse such processing</p> <p>This shall not prevent any technical storage or access for the sole purpose of carrying out <del>or</del> <u><b>facilitate</b></u> the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested</p>
---	---	--

explicitly requested by the subscriber or user <b><u>to provide the service.</u></b>	by the subscriber or user to provide the service.	by the subscriber or user to provide the service.
<b>Recital 52a</b>	<b>Recital 52a</b>	<b>Recital 52a</b>
		<p><b><u>(52a) Third parties may desire to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (e.g. certain types of cookies) to those involving unwarranted intrusion into the private sphere (e.g. spyware or viruses). It is therefore of paramount importance that users are provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of giving information and offering the right to refuse should be made as user-friendly as possible. An exception to the obligation to provide information and offering the right to refuse should be limited to those situations where the technical storage or access is necessary for the</u></b></p>

		<p><u>legitimate purpose of enabling the use of a specific service. Such an exception is however not justified where the storage or access has the purpose of merely facilitating the transmission. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's will to accept processing may be expressed by way of using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of the enhanced powers granted to the relevant national authorities under Article 15a of this Directive.</u></p>
--	--	---

Art. 6(7)	Art. 6(7)	Art. 6(7)
<p><u>recital</u> The processing of traffic data for the purpose of ensuring network and information security, including ensuring the availability, authenticity, integrity and confidentiality of stored or transmitted data, by providers of security services</p>	<p><u>recital</u> The processing of traffic data <u>as strictly necessary</u> for the purpose of ensuring network and information security, <u>i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events</u></p>	<p><u>recital</u> The processing of traffic data <u>as strictly necessary</u> for the purpose of ensuring network and information security, <u>i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events</u></p>

<p>when acting as data controllers would, under normal circumstances, be considered to be for the legitimate interest of the data controller within the meaning of Article 7(f) of Directive 95/46/EC. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping denial of service attacks and damages to computer and electronic communication systems.</p>	<p><b><u>or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems</u></b> including ensuring the availability, authenticity, integrity and confidentiality of <del>stored or transmitted data</del>, by providers of security services when acting as data controllers <del>would, under normal circumstances, be considered to be for the legitimate interest of the data controller within the meaning of</del> <b><u>is subject to</u></b> Article 7(f) of Directive 95/46/EC. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping denial of service attacks and damages to computer and electronic communication systems.</p>	<p><b><u>or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems</u></b> including ensuring the availability, authenticity, integrity and confidentiality of <del>stored or transmitted data</del>, by providers of security <b>technologies and</b> services when acting as data controllers <del>would, under normal circumstances, be considered to be for the legitimate interest of the data controller within the meaning of</del> <b><u>is subject to</u></b> Article 7(f) of Directive 95/46/EC. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping denial of service attacks and damages to computer and electronic communication systems.</p>
---	---	---