EUROPEAN COMMISSION
Information Society and Media Directorate-General

Electronic Communications Policy
Implementation of Regulatory Framework (I)

Brussels, 04 October 2011
DG INFSO/B2

COCOM11- 20

LIMITED

COMMUNICATIONS COMMITTEE

Working Document

Subject: Questionnaire on the implementation of the Article 5(3) of the ePrivacy Directive

This is a Committee working document which does not necessarily reflect the official position of the Commission. No inferences should be drawn from this document as to the precise form or content of future measures to be submitted by the Commission. The Commission accepts no responsibility or liability whatsoever with regard to any information or data referred to in this document.

Commission européenne, B-1049 Bruxelles/ Europese Commissie, B-1049 Brussel –Belgium. Telephone: (32-2) 299 11 11.
Office: BU33 4/43. Telephone: direct line (32-2)296 85 00. Fax: (32-2) 296 88 75.
E-mail: infso-cocom@ec.europa.eu

Introduction

On 25 May 2011, the transposition deadline for the revised regulatory framework for electronic communications expired. Among the amended provisions included in the Citizens' Rights Directive is Article 5(3) of the ePrivacy Directive, which concerns the storing and accessing of information on users' terminal devices and affects inter alia, but not exclusively, so-called cookies. To help Member States transpose this provision, the Commission presented a guidance document to COCOM and published it in 2010 (COCOM10-34).

In the meantime, the Directorate-General for Information Society and Media has also facilitated discussions among stakeholders on online behavioural advertising self regulation. The Commission services have announced that they would monitor and evaluate progress on implementation of national self-regulatory schemes, including compliance with EU law in view of further discussions with stakeholders planned for early 2012.

This document includes a questionnaire to be used for the purpose of gathering information on the overall implementation and enforcement of Article 5(3) of the ePrivacy Directive as amended by the Citizens' Rights Directive in the Member States.

Next steps

Member States are accordingly invited to submit their replies to the final questionnaire **by 18 November 2011 at the latest**. A report of Member States' replies will be presented at a forthcoming COCOM meeting.

QUESTIONNAIRE ON ARTICLE 5(3) OF THE ePRIVACY DIRECTIVE

MEMBER STATE: Deutschland (Germany)

Part I: TRANSPOSITION

Transposition of Article 5 (3) of the **ePrivacy Directive,** concerning the storing of information and the gaining of access to information already stored in the equipment of a subscriber or user. If relevant, please specify what transposing measures apply to cookies and which measures to 'spyware' and other malicious software such as web bugs, hidden identifiers, respawning and viruses.

Note: if terms used in those articles are defined elsewhere, please quote those relevant definitions together with the transposition measure. Any other contextual information is welcome.

ACT	**Telemediengesetz (TMG) (Telemedia Law)**
Please quote article	**1. Transparenzanforderungen von Art. 5 Abs. 3 E-Privacy-Richtlinie :** **"**auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält" ("having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing") **Umgesetzt in § 13 Abs. 1 TMG: "**Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. **Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten.** Der Inhalt der Unterrichtung muss für den Nutzer jederzeit

	abrufbar sein." Erläuterung: Die Bezeichnung "automatisierte Verfahren" ist umfassend und bezieht sich auch auf das Speichern von und den Zugriff auf Informationen auf dem Rechner des Nutzers entsprechend Art. 5 Abs. 3 E-privacy-Richtlinie. (Transposed in § 13 Telemedia Law: "The service provider must inform the recipient of the service at the beginning of the session about the nature, scope and purpose of the collection and use of personal data and about the processing of his data in countries outside the scope of Directive 95/46/EC of the European Parliament and of the Council 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 (OJ EC No. L 281 S. 31) in generally understandable form, unless such information has already been provided. **In the case of an automated procedure which permits subsequent identification of the recipient of the service and prepares the collection or use of personal data, the recipient of the service must be informed at the beginning of this procedure.** The content of this information must be accessible by the recipient of the service at any time." Explanation: "Automated procedure" means any procedure including the storing of information or the gaining of access to information already stored, in the terminal equipment of a subscriber or user, according to Art. 5 Par. 3 E-Privacy-Directive.) 2. **Erfordernis der Einwilligung gemäß Art. 5 Abs. 3 E-privacy-Richtlinie** : "Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist wenn der betreffende Teilnehmer oder Nutzer (...), seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder

	Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann." ("Member States shall ensure that the storing of information, or the gaining of 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 has given his or her consent, (...).This shall not prevent any technical storage or access for the sole purpose of carrying out 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 by the subscriber or user to provide the service.") Umgesetzt in § 12 und § 15 TMG:: § 12: "Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat." „Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat." § 15 Abs. 1 Satz 1: „Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten)." Erläuterung: § 12 stellt klar, dass personenbezogene Daten im Zusammenhang mit der Bereitstellung von Telemedien ohne Einwilligung nur verarbeitet werden dürfen, wenn der Gesetzgeber dies ausdrücklich erlaubt. Eine solche gesetzliche Erlaubnis enthält § 15 TMG, der regelt, dass Nutzerdaten bei Inanspruchnahme von Telemedien ohne Einwilligung nur verarbeitet werden dürfen, wenn das für diesen Zweck erforderlich ist. Für die Speicherung und den Abruf von Informationen wie z. B. Cookies bedeutet dies, dass solche Verfahren in Deutschland ohne Einwilligung des Nutzers nur zulässig sind, wenn dies aus technischen Gründen für die Inanspruchnahme erforderlich ist. Im Übrigen dürfen solche Verfahren ohne Einwilligung des

	Nutzers nicht verwendet werden. (Transposed in § 12 and 15 Telemedia Law: § 12: “The service provider may collect and use personal data for the provision of telemedia only to the extent that this Act or another statutory provision referring expressly to telemedia permits it or that the recipient of the service has given his consent.” “The service provider may collect and use personal data for other purposes only to the extent that this Act or another statutory provision referring expressly to telemedia permits it or if the recipient of the service has given his consent.” § 15: “The service provider may collect and use the personal data of a recipient of a service only to the extent necessary to enable and invoice the use of telemedia (data on usage).” Explanation: § 12 clarifies that personal data in connection with the use of information society services can be processed without the concent of the user only in the case of this being permitted expressively by law. Such a permission is regulated in § 15 Telemedia Law, which rules that data on usage can be processed without consent only in the case of this being necessary to enable the use of the information society service. Regarding the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user – like cookies - this means, that such a procedure is only permitted by law, if this is for technical reasons necessary to deliver the service. In all other cases such a procedure is not permitted without the consent of the user.) **3. Sanktionen (Sanctions)** § 16 TMG: “Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig (...) entgegen § 13 Abs. 1 Satz 1 oder 2 den Nutzer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet, (...) entgegen (...) § 15 Abs. 1 Satz 1 (...) personenbezogene Daten erhebt oder verwendet oder nicht oder nicht rechtzeitig löscht (...). Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.” (§ 16 Telemedia Law: “Anyone who deliberately or negligently (...) violates Section 13 (1) Sentence 1

	or 2 by not informing the recipient of the service or by not informing him accurately, completely or in due time, (...) violates (...)Section 15 (1) Sentence 1 (...) by collecting or using personal data or by not deleting it or not deleting it in due time (...) commits an administrative offence. (...) The administrative offence can be punished by a fine of up to fifty thousand euro." **4. Böswillige Verhaltensweisen** ('spyware' and other malicious software such as web bugs, hidden identifiers, respawning and viruses) Solche Verhaltensweisen sind in Deutschland in der Regel verboten. Sie können je nach Ausgestaltung des Einzelfalles insbesondere die Straftatbestände des Ausspähens von Daten (§ 202 a StGB), des Abfangens von Daten (§ 202 b StGB) des Vorbereitens des Ausspähens und Abfangens von Daten (§ 202 c StGB), der Datenveränderung (§ 303 a StGB), der Computersabotage (§ 303 b StGB) und der Störung von Telekommunikationsanlagen (§ 317 StGB) erfüllen. (In Germany such a behaviour would normally be treated as criminal acts. Depending on the single case they may fulfil criminal offences like spying of data (§ 202 a Criminal law), illegal capture of data (§ 202 b Criminal law), preparation of spying or capture (§ 202 c Criminal law), illegal changing of data (§ 303 a Criminal law), Computer sabotage (§ 303 b Criminal law) and disturbing of telecommunication devices (§ 317 Criminal law).
Date of entry into force	Die genannten Vorschriften des Telemediengesetzes waren bereits im 1997 in Kraft getretenen Teledienste-Datenschutz-Gesetz des Bundes und im Mediendienste-Staatsvertrag der Länder enthalten. Sie sind seit 2007 im Telemediengesetz enthalten. Das Strafgesetzbuch wurde 1998 neu gefasst. (The Provisions of the Telemedia law were already part of the federal Teleservices-Data-Protection-Law and the Media-Services-Interstate-Agreement

	of the federal states, which came into force in 1997. Since 2007 they are part of the Telemedia Law. The Criminal law is in force since 1998.)

If transposition has not taken place yet please indicate:

DRAFT ACT:	
draft Wording/Article:	
date of consultation launch	
Foreseen date of entry into force	

Part II: ENFORCEMENT

RELEVANT RULES	1. Can you describe the rules in place to ensure enforcement of the measures aiming at the protection of *subscriber or* users equipment against unauthorised *storing of information, and the gaining of access to information already stored in the terminal equipment* (general administrative rules, data protection act, telecom act)? Please indicate any applicable transitional regime. If applicable, please specify what enforcement rules apply to the various forms of infringements of measures transposing Article 5(3) e.g. cookies, spyware, etc. **Antwort**: Es gibt in Deutschland keine spezifischen Regelungen, die darauf abzielen, die technischen Einrichtungen der Nutzer gegen unberechtigte Speicherung von Informationen zu schützen. Allerdings verletzt der heimliche Zugriff auf informationstechnische Systeme das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dies hat das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 zur Online-Durchsuchung und zur Aufklärung des Internet festgestellt. Das Bundesamt für Sicherheit in der Informationstechnik informiert auf seiner Webseite ausführlich über die Gefahren und Schutzmöglichkeiten im Zusammenhang mit Cookies und schädlicher Software (vgl. https://www.bsi.bund.de/DE/Themen/InternetSicherheit/Gefaehrdungen/AktiveInhalte/DefinitionenundGefahren/definitionenundgefahren_node.html).

	(Answer: There are no such specific rules in Germany. However, according to the decision of the Federal Constitution Court from Feb. 27, 2008 the clandestine access violates the general personal right regarding the basic right on trustworthyness and integrity of information technology. The federal office for IT-Safety provides detailed information on risks and protection measures regarding cookies and malicious software.)
INFORMED CONSENT	2. Is there any guidance specifying how consent can be given? Is there any detail on the type and level of information that must be provided to the subscriber/user? How is the ability to revoke consent ensured? **Antwort** : Die Einwilligung richtet sich nach den datenschutzrechtlichen Bestimmungen. Nach § 13 Abs. 2 Telemediengesetz kann die Einwilligung elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Nach § 13 Abs. 3 TMG hat der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Widerrufsrecht hinzuweisen. Dieser Hinweis muss für den Nutzer jederzeit abrufbar sein. (Answer: Consent is to be given according do data protection laws. § 13 (2) Telemedia law provides, that consent can be declared by electronic means if the service provider ensures that the recipient of the service has consciously and unambiguously given his approval, a record of the approval is kept, the recipient of the service can access the content of the approval at any time and the recipient of the service can revoke the approval at any time with effect for the future. § 13 (3) Telemedia Law provides that the service provider must refer the user to the right to revoke is consent before the user states his approval. This information has to be at any time at the user`s disposal.)
EXCEPTIONS	3. According to Article 5 (3) possible exceptions may apply when the processing *"is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service"*. Are the exceptions to the need to express

	informed consent further specified in national law? **Antwort**: Auf die Ausführungen in Teil I wird verwiesen. Das TMG enthält keine weiteren Spezifikationen. (Answer: See answers in part I. There are no further specifications in the Telemedia law)
COMPETENT AUTHORITY AND COMPLAINTS	4. Which is/are the competent authority/authorities responsible for enforcement? To whom should users and subscribers complain? How do competent authorities handle complaints from citizens? **Antwort**: Die Aufsicht im Bereich des Telemediendatenschutzes, d. h. auch im Hinblick auf die Anforderungen nach Art. 5 Abs. 3 E-Privacy-Richtlinie liegt bei den Ländern, die auch die jeweiligen Verfahren im Umgang mit Beschwerden regeln. Die Aufsicht wird von folgenden Behörden wahrgenommen (vgl. http://www.datenschutz.hessen.de/adr_priv.htm): (Answer: Law enforcement in the area of Telemedia-Data-Protection also with regard to the requirements of Art. 5 (3) E-Privacy-Directive lies in the competence of the federal states which also provide for the procedures to handle complaints. Law enforcement is done by the following competent authorities:) Baden-Württemberg: Der Landesbeauftragte für den Datenschutz in Baden-Württemberg Jörg Klingbeil Urbanstraße 32, 70 182 Stuttgart Postfach 10 29 32, 70025 Stuttgart Telefon: (0711) 615541-0 Telefax: (0711) 615541-15 poststelle@lfd.bwl.de http://www.baden-wuerttemberg.datenschutz.de Bayern: Landesamt für Datenschutzaufsicht Promenade 27 (Schloss) 91522 Ansbach Tel.: (0981) 53 1300 Fax : (0981) 53 5300 poststelle@lda.bayern.de http://www.lda.bayern.de Berlin: Berliner Beauftragter für Datenschutz und Informationsfreiheit Dr. Alexander Dix An der Urania 4 - 10

	10787 Berlin Telefon: (030) 13 889 - 0 Telefax: (030) 215 5050 mailbox@datenschutz-berlin.de http://www.datenschutz-berlin.de Brandenburg: Die Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg Dagmar Hartge Stahnsdorfer Damm 77, 14532 Kleinmachnow Telefon: (033203) 3560 Telefax: (033203) 35649 Poststelle@LDA.Brandenburg.de http://www.lda.brandenburg.de Bremen: Die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen Dr. Imke Sommer Arndtstr. 1, 27570 Bremerhaven Postfach 10 03 80, 27503 Bremerhaven Telefon: (0421) 361 20 10 Telefax: (0421) 496 18 495 office@datenschutz.bremen.de http://www.datenschutz.bremen.de http://www.informationsfreiheit.bremen.de Hamburg: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Prof. Dr. Johannes Caspar Klosterwall 6, Block C 20095 Hamburg Telefon: (040) 428 54-4040 Telefax: (040) 428 54-4000 mailbox@datenschutz.hamburg.de http://www.datenschutz.hamburg.de Hessen: Der Hessische Datenschutzbeauftragte Prof. Dr. Michael Ronellenfitsch Gustav-Stresemann-Ring 1, 65189 Wiesbaden Postfach 31 63, 65021 Wiesbaden Telefon: (0611) 14 08-0 Telefax: (0611) 14 08-900 poststelle@datenschutz.hessen.de http://www.datenschutz.hessen.de Mecklenburg-Vorpommern: Der Landesbeauftragte für Datenschutz und

	Informationsfreiheit Mecklenburg- Vorpommern Reinhard Dankert Schloss Schwerin Johannes- Stelling- Straße. 21 19053 Schwerin Telefon: (0385) 59494- 0 Telefax: (0385) 59494- 58 datenschutz@mvnet.de http://www.lfd.m- v.de Niedersachsen: Der Landesbeauftragte für den Datenschutz Niedersachsen Hans- Joachim Wahlbrink Brühlstr. 9, 30169 Hannover Postfach 221, 30002 Hannover Telefon: (0511) 120- 4500 Telefax: (0511) 120- 4599 poststelle@lfd.niedersachsen.de http://www.lfd.niedersachsen.de Nordrhein-Westfalen: Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein- Westfalen Ulrich Lepper Kavalleriestraße 2 - 4, 40213 Düsseldorf Postfach 20 04 44, 40102 Düsseldorf Telefon: (0211) 38424- 0 Telefax: (0211) 38424- 10 poststelle@ldi.nrw.de http://www.ldi.nrw.de Rheinland-Pfalz: Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Edgar Wagner Hintere Bleiche 34, 55116 Mainz Postfach 30 40, 55020 Mainz Telefon: (06131) 208- 2449 Telefax: (06131) 208- 2497 poststelle@datenschutz.rlp.de http://www.datenschutz.rlp.de Saarland: Unabhängiges Datenschutzzentrum Saarland Judith Thieser Landesbeauftragte für den Datenschutz und Informationsfreiheit Fritz- Dobisch- Str. 12 66111 Saarbrücken

	Telefon: (0681) 94781-0 Telefax: (0681) 944781-29 poststelle@datenschutz.saarland.de http://www.datenschutz.saarland.de Sachsen: Der Sächsische Datenschutzbeauftragte Andreas Schurig Bernhard-von-Lindenau-Platz 1, 01067 Dresden Postfach 12 09 05, 01008 Dresden Telefon: (0351) 4935-401 Telefax: (0351) 4935-490 saechsdsb@slt.sachsen.de http://www.datenschutz.sachsen.de Sachsen-Anhalt: Landesverwaltungsamt Sachsen-Anhalt Referat Justitiariat An der Fliederwegkaserne 13 06130 Halle (Saale) Tel.: (0345) 514-0 Fax: (0345) 514-3799 poststelle@lvwa.sachsen-anhalt.de http://www.landesverwaltungsamt.sachsen-anhalt.de Schleswig-Holstein: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Dr. Thilo Weichert Holstenstraße 98, 24103 Kiel Postfach 71 16, 24171 Kiel Telefon: (0431) 988 1200 Telefax: (0431) 988 1223 mail@datenschutzzentrum.de http://www.datenschutzzentrum.de Thüringen: Thüringer Landesverwaltungsamt Weimarplatz 4, 99423 Weimar Postfach 2249, 99403 Weimar Telefon: (03 61) 37 70 0 Telefax: (03 61) 37 73 71 90 poststelle@tlvwa.thueringen.de http://www.thueringen.de/de/tlvwa/ Oberste Aufsichtsbehörde: Innenministerium des Landes Thüringen Steigerstraße 24 99096 Erfurt Tel.: 0361/37 900 Fax: 0361/37 93 111 poststelle@tim.thueringen.de http://www.thueringen.de/de/tim/

ENHANCED POWERS	5. Have powers been granted to competent authorities (for example orders to cease, powers to impose monetary penalties for breaches, issuing of warnings about failing to comply). Please specify. Have such powers been enhanced on the occasion of the transposition? **Antwort:** Siehe hierzu die Ausführungen in Teil I (Sanktionen). Die Verhängung von Sanktionen ist Angelegenheit der zuständigen Aufsichtsbehörden (Frage 4). (Answer: See details in Part I (sanctions). Decision on sanctions belongs to the competent law enforcement authorities (question 4).)
INTERNAL GUIDANCE	6. Has any guidance been developed for enforcement? Where is such guidance available? Please specify issues covered. **Antwort**: Siehe hierzu die Ausführungen unter 4. (Answer: See answer to question 4)
TRAINING	7. Is there any training provided/foreseen for civil servants dealing with enforcement of these rules? **Antwort**: Siehe hierzu die Ausführungen unter 4. (Answer: See answer to question 4)
CHALLENGES	8. Do you see any enforcement challenges, regarding e.g. consent or other issues, cross-border issues, which would hamper the effective implementation in you country as of today? If any such issues exist, how do competent national authorities intend to resolve them? **Antwort**: Es bestehen keine Hindernisse seitens der Datenschutzaufsichtsbehörden, die gesetzlichen Anforderungen gegenüber in ihrem Zuständigkeitsbereich niedergelassenen Diensteanbietern durchzusetzen. (Answer: There are no such enforcement challenges.)
INTERNATIONAL COOPERATION	9. Are there specific procedures in place for assuring international cooperation if needed? Could you describe specific limitations to your jurisdiction which can have an impact on enforcement? **Antwort**: Es bestehen keine spezifischen Beschränkungen, die Einfluss auf die Durchsetzung haben. Die deutschen Datenschutzbehörden arbeiten über den Düsseldorfer Kreis zusammen (vgl. http://www.datenschutz.de/aufsicht_privat/). Auf die Antwort zu Frage 4 wird verwiesen.

	(Answer: There are no specific limitations to law enforcement. The German data protection authorities cooperate in the Düsseldorf Circle. See answer to question 4.)
PRACTICE	10. Can you describe your experience with the application of these rules in your country, if any? Please specify any measure taken so far in practice related to cookies, as well as to 'spyware' and other malicious software such as web bugs, hidden identifiers, and viruses. **Antwort**: Siehe hierzu die Ausführungen unter 4. (Answer: See answer to question 4)

Part III: SELF REGULATION

DEPLOYMENT	11. Is self-regulation expected to contribute to the effective application of the rules transposing Article 5(3)? If so, can you describe any self regulatory initiative ongoing at national level (e.g. scope, stakeholders involved, methods to provide information and consent, enforcement)? Are competent national authorities involved e.g. co-regulation? **Antwort**: Selbstregulierung erscheint als wichtiger Beitrag zur Umsetzung von Art. 5 Abs. 3 und wird daher befürwortet. Das gilt besonders im Hinblick auf eine europäische Organisation der Selbstregulierung. Die deutsche Werbewirtschaft baut in Zusammenarbeit mit europäischen Partnern derzeit eine Selbstregulierung insbesondere im Zusammenhang mit der Verwendung von Cookies für Zwecke des Online Behavioural Advertising auf. Dazu befindet sich der Deutsche Datenschutzrat Online-Werbung (DDOW) derzeit in der Gründungsphase. Beteiligt sind der Zentralverband der deutschen Werbewirtschaft (ZAW), der Bundesverband Digitale Wirtschaft (BVDW), der Verband deutscher Zeitschriftenverleger (VDZ), der Bundesverband Deutscher Zeitungsverleger (BDZV), der Verband Privater Rundfunk und Telekommunikation (VPRT), der Deutscher Dialogmarketing Verband (DDV), der Handelsverband Deutschland (HDE), der Gesamtverband der Kommunikationsagenturen (GWA) und der Bundesverband der Deutschen Industrie (BDI). (Answer: Self-regulation seems to be important to contribute to the transposition of Art. 5 (3) and is therefore to be supported specially with regard to an

	organisation on the European level. The German advertising industry is cooperating with European partners to develop a self-regulation specially regarding the use of cookies for purposes of online behavioural advertising. Therefore a german data protection council for online advertising (DDOW) is ongoing to be founded. Participants are the central association of the advertising industry (ZAW), the federal association digital economy (BVDW), publishers associations journals and newspapers (VDZ, BDZV), the association private broadcasting and telecommunication (VPRT), the German dialogue-marketing association (DDV), the commercial association Germany (HDE), the general association communication agencies (GWA) and the federal association of the German industry (BDI).)
PROGRESS	12. Which is the current state of play regarding any self-regulation initiative? What is the timeframe for any such solution to be effectively available for users and subscribers? **Antwort** : Der DDOW soll zum Anfang des Jahres 2012 seine operative Arbeit aufnehmen. (Answer: The DDOW is intended to be operable by the beginning of 2012.)
EVALUATION	13. How do competent national authorities intend to evaluate the contribution of self regulatory solutions? **Antwort** : Hierzu gibt es bislang keine Überlegungen. (Answer: To this point there are no considerations yet.)