ARTICLE 29 DATA PROTECTION WORKING PARTY

01910/2007/EN
WP 139

Opinion 6/2007
on data protection issues related to the Consumer Protection Cooperation System (CPCS)

Adopted on 21 September 2007

TABLE OF CONTENT

WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Article 29, Article 30(1)(c) and Article 30(3) of the above Directive,

having regard to its rules of procedure, and in particular Articles12 and 14 thereof,

HAS ADOPTED THE PRESENT OPINION:

1. INTRODUCTION

This Article 29 Data Protection Working Party ("**Working Party**") Opinion discusses the data protection issues related to the Consumer Protection Cooperation System ("**CPCS**"), an electronic database operated by the European Commission for the exchange of information among consumer protection authorities in Member States and the Commission pursuant to the provisions of Regulation (EC) No 2006/2004 on consumer protection cooperation ("**CPC Regulation**").

The Opinion follows a letter dated 30 March 2007 by the head of Unit B-5, Enforcement and Consumer Redress, of the European Commission's Health & Consumer Protection Directorate-General ("**DG SANCO**") addressed to the Secretariat of the Working Party and requesting the opinion of the Working Party.

The Working Party welcomes that is has been consulted. At the same time, it regrets that the consultation request came only after the adoption of the CPC Regulation, and the adoption of Commission Decision 2007/76/EC of 22 December 2006 ("**CPC Implementing Decision**"), and only once the CPCS had been established, become fully functional, and started to operate. Had it been consulted earlier, the Working Party would have been able to offer insight at a stage where its recommendations would have been easier to take on board.

With that said, overall, the Working Party welcomes the establishment of an electronic system for the exchange of information. Such a streamlined system may not only enhance efficiency of cooperation, but from the data protection point of view, it may also help ensure compliance with applicable data protection laws. It may do so by providing a clear framework on what information can be exchanged, with whom, and under what conditions.

Nevertheless, establishment of the centralized database also creates certain risks. These include, most importantly, that more data might be shared and more broadly than it is strictly necessary for the purposes of efficient cooperation, and that data, including potentially outdated and inaccurate data, might remain in the database longer than it is necessary. The security of a database accessible in 27 Member States is also a sensitive issue, as the system is only as safe as the weakest link in the network permits it to be.

The purpose of this document is to identify the most important data protection concerns that the establishment and operation of the CPCS may entail, and to recommend solutions to alleviate those concerns.

The document is addressed to both the Commission and Member State competent authorities in their capacity as controllers of the CPCS, as will be explained below. Further, the recommendations in this document should also serve to inform any further decision-making of the "**Regulatory Committee**" consisting of Member States representatives, which was established under Article 19 of the CPC Regulation with the mandate to assist the Commission in implementing the CPC Regulation. Finally, this document is also addressed to legislators in Member States who are required under Article 13(4) of the CPC Regulation to "adopt the legislative measures necessary to restrict the rights and obligations under Articles 10, 11 and 12 of Directive 95/46/EC as necessary to safeguard the interests referred to in Article 13(1)(d) and (f) of that Directive."

PART A: DESCRIPTION OF THE SYSTEM

2. MUTUAL ASSISTANCE OBLIGATIONS ESTABLISHED UNDER THE CPC REGULATION

2.1. Purpose of the CPC Regulation: cooperation between consumer protection authorities. The CPC Regulation was adopted to enhance enforcement of consumer protection laws across the Internal Market. The CPC Regulation sets up an EU-wide network of national consumer protection enforcement authorities. It lays down the framework and general conditions under which Member States are to cooperate. Under this new system, each authority is able to call on other authorities of the network for assistance in investigating possible breaches of consumer protection law and in taking action to stop deceptive commercial practices of traders targeting consumers living in other EU countries.

2.2. Scope of the CPC Regulation: intra-Community infringements of specified directives and regulations. The scope of the CPC Regulation is limited to "Intra-Community infringements" of the directives and regulations listed in the Annex to the CPC Regulation. The list, which may be updated when necessary, currently comprises of 15 directives and regulations, including the directives on misleading advertisement, distance selling, consumer credit, television broadcasting, package travel, unfair contract terms, timeshare, e-commerce, and others. To come within the scope of the CPC Regulation, "intra-Community infringements" (i) must be of a "cross-border" nature, and (ii) must harm the "collective interests of consumers".

2.3. Mutual assistance under the CPC Regulation: investigation, enforcement, and alerts. Chapters II and III of the CPC Regulation require competent authorities in Member States to mutually assist each other both with respect to investigations and enforcement. In addition, they are also required to alert other Member States and the Commission of suspected or confirmed intra-Community infringements. Finally, the competent authorities of different Member States are under specific obligation to coordinate their activities when the consumers of more than two Member States are affected by an infringement.

3. PURPOSE, LEGAL BASIS AND ESTABLISHMENT OF THE CPCS

3.1. The purpose the CPCS: a database for information exchange related to mutual assistance. CPCS is an electronic database operated by the European Commission and designed to provide a structured system for the exchange of information between competent

authorities in Member States for the performance of their mutual assistance obligations under the CPC Regulation.

3.2. Outline of processing operations under the CPCS. The users of the system are the Commission and competent authorities in Member States. In addition, a so-called "single-liaison office" is designated in each Member State, for coordinative purposes (see Section 5.3 below).

Data are uploaded into the system by competent authorities. For example, a competent authority may send a request for information or enforcement to another. Or it may send an alert to certain other Member States and the Commission. The information, then, will be stored in the database and may be retrieved by other users to whom the communication is addressed, for example, by the authority requested to carry out an enforcement action, or by the Commission. Deletions are carried out by the Commission, upon request of the authorities in Member States who are obliged to inform the Commission when cases are closed or alerts prove to be unfounded. In cases of confirmed infringements resulting in an enforcement action, data are retained for five years following the notification of the enforcement action. Rules on conservation and deletion are described and further discussed in more detail in Sections 6 and 11 below.

3.3. Legal basis of the CPCS. The legal basis of the CPCS rests on Article 10 of the CPC Regulation, which provides that "the Commission shall maintain an electronic database in which it shall store and process the information it receives under Articles 7, 8 and 9 of the CPC Regulation". In addition, Article 12(3) provides that "requests for assistance and all communication of information shall be made in writing using a standard form and communicated via the database established in Article 10".

These Articles, when read together, require that all mutual assistance requests, alerts, and related communications under Chapters II and III of the CPC Regulation must be routed through the CPCS. [1]

In addition, the CPC Implementing Decision provides that Member States must inform the Commission and other Member States via a "**Discussion Forum**" made available using the CPCS infrastructure, of any investigation and enforcement powers granted to competent authorities in addition to those specifically required under the CPC Regulation.

3.4. CPC Implementing Decision. The provisions of the CPC Regulation applicable to the CPCS entered into force on 29 December 2006. Shortly before that date, the Commission, aided by a Regulatory Committee consisting of Member State representatives, issued an implementing decision.

The CPC Implementing Decision establishes what data fields should be included in the database and what the minimum content of requests, responses, and alerts must be. It also provides for time-limits for certain steps in the mutual assistance procedures and other implementing measures.

[1] Not all cooperative activities and information exchange required under the CPC Regulation have to be carried out using the CPCS database. For example, Chapter IV provides for cooperative activities with respect to the training and exchange of consumer protection enforcement officials. As the information exchange related to these activities fall outside the scope of the CPCS, they will not be discussed in this document.

3.5. Establishment of the CPCS. The design of the system follows the provisions set forth by the CPC Regulation and the CPC Implementing Decision. These two sources specify the main features and detail certain aspects of the database. However, they do not provide a comprehensive set of guidelines for the design, maintenance, operation, and use of the database. The CPCS as it is currently in place was ultimately designed by the Commission, in consultation with Member States and a key user group representing the competent authorities in various Member States.

In technical terms, the Commission built the system and is the operator of the system. The data are hosted on Commission servers and it is the Commission's technicians who maintain the system and ensure its security. In addition, it is also the Commission who may implement any changes in the design of the system, should this be necessary.

The CPCS is already implemented and in use but certain features provided for in the CPC Implementing Decision are blocked: in particular, the data fields regarding company directors currently cannot be used, pending clarification of data protection compliance issues.

4. DATA FLOWS UNDER THE CPCS

The CPC Regulation and the CPC Implementing Decision, taken together, establish in detail the categories of information that may or must be exchanged through the CPCS.

4.1. General provisions and confidentiality. With a general aim, the CPC Implementing Decision provides that when issuing a request for mutual assistance or an alert, a competent authority must supply all information at its disposal that may be useful for other competent authorities to fulfil the request efficiently or ensure a proper follow-up to the alert.

In turn, when responding to a request for information, the requested authority must supply any information specified by the applicant authority which is necessary to establish whether an intra-Community infringement has occurred or whether there is a reasonable suspicion that it may occur. Similarly, when responding to a request for enforcement, the requested authority must inform the applicant authority of the actions taken or planned and the powers exercised to address the request. In either case, if a competent authority refuses to comply with a request, it must include in its response a statement of grounds for that refusal.

In all cases, the applicant and requested authorities must indicate whether any of the information supplied must be given confidential treatment (see also Section 5.4 below).

4.2. Alerts and feedback. Article 7(1) of the CPC Regulation provides that "when a competent authority becomes aware of an intra-Community infringement, or reasonably suspects that such an infringement may occur, it shall notify the competent authorities of other Member States and the Commission, supplying all necessary information, without delay". Further, Article 7(2) provides that "when a competent authority takes further enforcement measures or receives requests for mutual assistance in relation to the intra-Community infringement, it shall notify the competent authorities of other Member States and the Commission".

In practical terms, Article 7 requires the exchange of two types of information:

- **Alerts**: a warning message sent by an authority to chosen network counterparts in other Member States and the Commission to inform them about the existence of an infringement to consumer protection law or a reasonable suspicion of such an infringement; and

- **Feedback–information:** when competent authorities take further enforcement measures or receive requests for mutual assistance, they inform the Commission and other network counterparts of the request received or enforcement action taken.

Pursuant to the CPC Implementing Decision, the CPCS should contain the following data fields for alerts:

(i) type of intra-Community infringement,
(ii) status of intra-Community infringement (verified, reasonable suspicion),
(iii) legal basis,
(iv) short summary,
(v) estimated number of consumers likely to be harmed and estimated financial detriment,
(vi) any requirement for confidential treatment, and
(vii) attached documents (in particular relating to statements and other evidence).

In addition, the alerts also contain the details of the seller or supplier responsible for an intra-Community infringement or a suspected intra-Community infringement, as described below in Section 4.6.

4.3. Enforcement cooperation. Article 8(1) of the CPC Regulation provides that "a requested authority shall, on request from an applicant authority, take all necessary enforcement measures to bring about the cessation or prohibition of the intra-Community infringement without delay."

As a practical matter the information exchange under Article 8 includes:

- **Requests for enforcement:** request from one authority to another to take appropriate action to stop a confirmed infringement.

Considering the requirements of Article 12(3) of the CPC Regulation, responses are also given through the CPCS and any related communications also take place through the CPCS, via messages sent through the system.

The CPC Implementing Decision requires that the applicant authority must provide the requested authority at least with: (a) an identification of the seller or supplier against whom the measures are requested; (b) details of the conduct or practice concerned; (c) legal qualification of the intra-Community infringement under the applicable law, and its legal basis; and (d) evidence of harm to the collective interests of consumers, including if possible an estimate of the number of consumers likely to be harmed.

The CPC Implementing Decision further provides that the CPCS should contain the following data fields for enforcement requests:

(i) location of consumers likely to be harmed,
(ii) name of product or service,
(iii) COICOP code,
(iv) legal basis,
(v) advertising or sales medium involved,

(vi) type of intra-Community infringement,
(vii) status of intra-Community infringement (verified, reasonable suspicion),
(viii) estimated number of consumers likely to be harmed and estimated financial detriment,
(ix) proposed time-table for a response,
(x) attached documents (in particular relating to statements and other evidence) and any requirement for confidential treatment,
(xi) indication of the assistance requested,
(xii) reference to alert (if applicable),
(xiii) list of requested authorities and Member States concerned, and
(xiv) request for a competent official to participate in investigation (Article 6(3) of the CPC Regulation).

4.4. Co-ordination of market surveillance activities[2]. Article 9(1) of the CPC Regulation provides that "competent authorities shall coordinate their market surveillance and enforcement activities. They shall exchange all information necessary to achieve this." Article (9)(2) adds that "when competent authorities become aware that an intra-Community infringement harms the interests of consumers in more than two Member States, the competent authorities concerned shall coordinate their enforcement actions and requests for mutual assistance via the single liaison office. In particular they shall seek to conduct simultaneous investigations and enforcement measures." Article 9(3) adds that "the competent authorities shall inform the Commission in advance of this coordination and may invite the officials and other accompanying persons authorised by the Commission to participate."

In practice, the information exchange under Article 9(2) involves situations where the competent authorities of at least three countries are involved. In this case, information can be exchanged to detect whether an infringement has taken place. The Commission is also informed of, and it may, if requested by the competent authorities, participate in the investigations.

4.5. Exchange of information on request. Article 6(1) of the CPC Regulation provides that "a requested authority shall, on request from an applicant authority ..... supply without delay any relevant information required to establish whether an intra-Community infringement has occurred or to establish whether there is a reasonable suspicion it may occur." Article 6(2) further provides that "the requested authority shall undertake, if necessary with the assistance of other public authorities, the appropriate investigations or any other necessary or appropriate measures ..... in order to gather the required information."

Article 6 is not specifically referred to in Article 10 which requires certain information exchanges to take place exclusively through the CPCS. However, by virtue of Article 12(3), which requires that "requests for assistance and all communication of information shall be made in writing using a standard form and communicated via the database established in Article 10", all information exchange under Article 6 should also be made using the CPCS.

In practice, information exchange under Article 6 includes

- **Requests for information:** request from an authority to another to provide information relevant to establish whether an infringement of consumer protection law has occurred or that there is a reasonable suspicion that it may occur.

[2] Article 3(i) of the CPC Regulation defines market surveillance activities to mean "the actions of a competent authority designed to detect whether intra-Community infringements have taken place within its territory."

Considering the requirements of Article 12(3), responses are also given through the CPCS and any related communications also take place through the CPCS, via messages sent through the system.

The CPC Implementing Decision requires that the applicant authority must at least (a) inform the requested authority of the nature of the suspected intra-Community infringement and its legal basis; (b) provide sufficient elements to identify the conduct or practice under investigation; and (c) specify the information requested.

The CPC Implementing Decision also lists those information fields that the CPCS should contain with respect to requests for information. These are identical to those listed with respect to requests for enforcement under Section 4.3 above.

4.6. Details of the seller or supplier responsible for an intra-Community infringement or a suspected intra-Community infringement. The CPC Implementing Decision provides that the CPCS should include the following data entries with respect to the seller or supplier responsible for the infringement or suspected infringement:

(i) name,
(ii) other trading names,
(iii) name of parent company, if any,
(iv) type of business,
(v) address(es),
(vi) E-mail address,
(vii) telephone number,
(viii) fax number,
(ix) website,
(x) IP address, and
(xi) name(s) of company director(s), if any.

4.7. Discussion forum. As noted in Section 3.3 above, the CPCS also includes a so-called "Discussion Forum". This forum is established pursuant to the CPC Implementing Decision with the sole purpose of exchanging information regarding additional enforcement powers that competent authorities may have been granted. The forum, as its name suggests, is an unstructured discussion forum and there are no specific data fields mandated by the CPC Implementing Decision.

4.8. Processing of staff data. The Commission also processes a limited amount of personal data (names, contact information, languages spoken) of the staff working for the competent authorities and of the single liaison offices of Member States. The processing operations relating to staff data, however, constitute a marginal aspect of the CPCS. In addition, this processing operation is also inherent in managing any database with multiple users. For this reason, these data processing operations will not be further discussed in this document.

5. ACCESS TO DATA IN THE CPCS

5.1 The Commission's access to data

The Commission's access to data under the CPC Regulation. As described in Section 4 above, under the CPC Regulation, the Commission should have access to:

- alerts (Article 7(1)),
- feedback information (Articles 7(2), 8(6) and 10(2)), and
- in certain cases also to other case-related information (Articles 8(5), 9(3) and 15(5)).[3]

However, according to the CPC Regulation, the Commission is not to receive:

- requests of information under Article 6, and
- requests for enforcement under Article 8.

These requests for mutual assistance are addressed to competent authorities in Member States only.

The Commission's access to data under the Commission's Issue Paper. Pursuant to the description in the Issue Paper, Commission officials who are responsible for monitoring the application of one or more legislative acts falling under the scope of the CPC Regulation, and only for cases falling under those acts, are given read-only access to follow-up information regarding enforcements actions under Article 8.6 of the CPC Regulation. The Commission's Issue Paper does not mention feedback information regarding either information requests or alerts (Articles 7(2) and 10(2)), although presumably these information flows are also built into the database.

The Commission Issue Paper also mentions that access to all other information in the database is given to Commission officials working in the unit responsible for the application of the CPC Regulation. They currently use such data solely to monitor application of the CPC Regulation, in particular, to extract data for statistical purposes. At first reading, this suggests that contrary to the provisions of the CPC Regulation, these specific Commission officials have unlimited access to the CPCS, including information requests and enforcement requests exchanged between competent authorities in Member States and all data "flagged" confidential (see Section 5.4 below). Additional information provided by DG SANCO during the preparation of this Opinion, however, confirmed that this is not the case. DG SANCO specifically confirmed that no Commission officials have access to information requests or enforcement requests exchanged between competent authorities in Member States, and that the Commission's access to data "flagged" confidential is limited, as described in Section 5.4 below.

Finally, according to the Issue Paper, Commission officials may also participate in coordinated investigations or enforcement actions under Article 9(3) of the CPC Regulation. These officials have full access to case-related information.

5.2. Access to data by competent authorities. When competent authorities upload information in the system in the form of alerts, information requests or enforcement requests, it is up to them to decide which other competent authorities to give access to the information uploaded. For example, the Belgian competent authorities may send an alert that appears to be relevant to Belgium, France, and Luxembourg and not to other Member States, to only France

[3] If the Commission participates in cross-border investigations involving more than two countries, pursuant to Article 9(3) upon invitation from competent authorities, it will receive case-related information. In addition, under Articles 8(5) and 15(5), the Commission also has access to certain information relating to mutual assistance requests in those cases where it needs to help settling disputes between requesting and requested authorities.

and Luxembourg. The same applies to feedback information and any other communication they make through the database.

5.3. Access to data by single liaison offices. Pursuant to the CPC Regulation, mutual assistance requests (including both requests for information and enforcement requests) are sent through the single-liaison offices of the applicant and requested authority's Member States. Information communicated as a result of a request is to be communicated directly to the applicant authority and simultaneously to the single liaison offices of the applicant and requested authorities. In case of cooperation involving more than two Member States, single liaison offices play an additional coordinative role. In all these cases, single liaison offices may have access to personal data, insomuch as they are included in mutual assistance requests and responses to such requests. However, single liaison offices have no access to information flagged confidential (see Section 5.4).

In addition, it is to be noted that many single liaison offices may be wearing two hats: on one hand, they carry out their coordinative functions as single liaison offices, and on the other hand, they are also acting as competent authorities with respect to certain consumer protection infringements. In this latter capacity they have access to data the same way as any other competent authority.

5.4. Information "flagged" as confidential. Article 13(3) of the CPC Regulation provides that the information stored in the CPCS, the disclosure of which would undermine: (i) the protection of the privacy of the individual, (ii) the commercial interests of a person, (iii) court proceedings and legal advice, or (iv) the purpose of inspections or investigations, must be confidential, unless its disclosure is necessary to bring about the cessation or prohibition of an intra-Community infringement and the authority communicating the information consents to its disclosure.

The CPC Implementing Decision, as described in Section 4, requires that the authorities uploading information or enforcement requests or alerts must indicate whether the information is to be treated confidentially. Similarly, the requested authority, when supplying information, must also indicate whether the information is to be treated confidentially. The CPC Implementing Decision also requires that the CPCS includes specific data fields to indicate that data exchanged should be given confidential treatment. According to the Commission Issue Paper, a competent authority may wish to flag information confidential, for example, when it attaches a document to its message and this attachment contains confidential information.

As between the Commission, competent authorities and single liaison offices, the CPC Implementing Decision provides that flagging data "confidential" also means that single liaison offices will not have access to data which has been given confidential treatment. DG SANCO clarified during the preparation of this Opinion that its intention is to limit the Commission's access to "flagged" information the same way. [4]

In addition, according to the Commission Issue Paper, certain documents in certain cases also cannot be disclosed to "bodies having a legitimate interest in the cessation or prohibition of intra-Community infringements" designated based on the provisions of the CPC Regulation to assist competent authorities in enforcement matters. Pursuant to the CPC Implementing

[4] This is with certain exceptions. Confidential information, if necessary, may be used in cases where the Commission resolves disputes and in cases where the Commission participates in an investigation (see Articles 8(5), 9(3) and 15(5) of the CPC Regulation).

Decision, disclosure of any information to these bodies should be subject to the prior approval of the applicant authority, specifying the nature and details of the information that may be disclosed to that body.

Confidential treatment, however, does not prevent that confidential data could be shared between the competent authorities or could be transferred to courts or other public authorities. For now, the text of the CPC Regulation and the CPC Implementing Decision also does not limit the Commission's access to such data.

6. CONSERVATION PERIODS UNDER THE CPC REGULATION AND THE CPC IMPLEMENTING DECISION

6.1. Withdrawal of alerts. Article 10(2) of the CPC Regulation provides that "where a competent authority establishes that a notification of an intra-Community infringement made by it pursuant to Article 7 has subsequently proved to be unfounded, it shall withdraw the notification and the Commission shall without delay remove the information from the database."

In practice, this means that the competent authority which posted an alert under Article 7 must withdraw the alert and the information must be deleted from the database as soon as the competent authority establishes that the alert was unfounded.

6.2. Cases closed following enforcement. Under Article 8(6), "the requested authority shall notify without delay the applicant authority, the competent authorities of other Member States and the Commission of the measures taken and the effect thereof on the intra-Community infringement, including whether it has ceased." Article 10(2) then provides that "the stored data relating to the intra-Community infringement shall be deleted five years after [this] notification."

In practice, this means that the requested authority must notify the Commission about the enforcement actions taken and the information must be deleted from the database five years after this notification.

6.3. Cases closed following requests for information. The CPC Implementing Decision provides that the requesting authority must notify the Commission and remove the information from the database following a request pursuant to Article 6, if (a) the information exchanged does not generate an alert or a request pursuant to Article 8, or if (b) it is established that no intra-Community infringement has taken place.

In practice, this means that the requesting authority must notify the Commission if the information request will not result in further cooperative action, such as sending of an enforcement request or an alert, or if it is established that no infringement under the CPC Regulation took place. The information must then be deleted from the database.

7. THE SECURITY ARCHITECTURE OF THE CPCS

7.1. The Commission's Data Centre. The Commission provides the technical infrastructure for the CPCS system including the technical back-up and help-desk. The collected data are stored in host computers of the Data Centre of the Directorate General of Informatics in Luxemburg. Operation of this server is carried out pursuant to the Commission’s security

decisions and provisions established under the Directorate of Security. The general European Commission IT and telecommunication safeguard system applies.

The CPCS environment is protected by intrusion detection systems and against virus, spam and other types of threats. It is secured by a firewall proxy and also a reverse proxy placed and maintained by the Commission's DIGIT Telecom Centre. All transactions are encrypted through https channel. The system follows the backup/recovery rules of the EC Data Centre.

7.2. TESTA-II network. Information is not exchanged via the internet, but through the secure telecommunications network TESTA II, which interconnects Community institutions and bodies with national authorities. TESTA II is a closed, private network. The Commission provides security until the national contact points of TESTA-II. The access to this backbone is done through identified points of connection. All traffic on this network is encrypted. The migration to s-TESTA, which is currently ongoing, will provide added security.

From the national contact points to the users it is the respective Member State's responsibility to build out physically the connection and supervise its security. Each Member State must guarantee that only authorized personnel can access TESTA. The network does not have any "window" to the internet. It is accessible only for the predefined users and only through those computers that are physically connected to the network and situated in the offices of national authorities and the Commission.

7.3. Access to data. Different access profiles are defined for the operation of the CPCS. These profiles are determined by the access rights to the data stored in the database. Users are notified by the competent authorities to the Commission. Each authority has at least one user, but may have more registered users. Access to the CPCS is only given to a well-defined, traceable group of users. Every access is nominative, linked to one individual and no functional users are permitted.

A login/password is requested to enter the application. The request for a new login name is issued by the single liaison office of the respective country. The Commission creates the login and initial password which is transmitted to the user through the single liaison office. The initial password has to be changed at first login by the user. The new password is a strong password, that is, the length is minimum 8 characters long, and must contain at least alphabetical and numerical characters. There are plans to further improve the security of this system and as of later this year require at least three types of characters out of four families (normal letter, capital letter, number, special sign).

The Commission's Issue Paper emphasises that the combination of the measures mentioned above with a private network puts the access to CPCS at an adequate security level taking into account the nature of the data stored and transferred through the CPCS.

Further extension of security at national level is already possible. If a country decides to use, for example, crypto-chip-based authentication equipment it can be integrated easily on national level because the procedures to access the system are decided at Member State level and they are responsible for the operation and security of the system from the national TESTA-II contact points.

PART B: ANALYSIS

8. DATA CONTROLLERS, APPLICABLE LAWS AND SUPERVISORY AUTHORITIES

8.1. The competent authorities and the Commission are designated as controllers by the CPC Regulation. Article 2(d) 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 ("**Directive 95/46/EC**") and Article 2(d) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ("**Regulation (EC) No 45/2001**") both provide that in case the purposes and means of the processing of personal data are determined by Community law, the controller may be designated by Community law.

This is the case of the CPCS, where the purposes and means of the processing are defined by the CPC Regulation and where Article 10 specifically provides that the Commission and competent authorities each act as controllers in relation to their specific responsibilities under the CPC Regulation.

In particular, Article 10 provides the following: "In relation to their responsibilities to notify information for storage in the database and the processing of personal data involved therein, the competent authorities shall be regarded as controllers in accordance with article 2(d) of Directive 95/46/EC. In relation to its responsibilities under this Article and the processing of personal data involved therein, the Commission shall be regarded as the controller in accordance with Article 2(d) of Regulation (EC) No 45/2001."

8.2. Competent authorities as controllers. Each competent authority is a controller with respect to its own data processing activities as a user of the system for its own purposes, as provided in the CPC Regulation. It should comply with its own national data protection laws and is subject to the supervision of its own national data protection authorities.

8.3. Single-liaison offices as controllers. As discussed in Sections 5.3 and 5.4, single liaison offices also receive information, unless it is flagged confidential, in order to carry out their coordinative roles with respect to routing information and enforcement requests. While doing so, they should comply with their own national data protection laws and are subject to the supervision of their own national data protection authorities.

8.4. The Commission's sui generis role. The CPC Regulation designates the Commission as a controller with respect to its own tasks and responsibilities. With that said, considering the tasks and responsibilities of the Commission, which include both (i) the operation of the CPCS for the benefit of competent authorities in Member States and (ii) the Commission's own use of the CPCS, the Commission appears to have a *sui generis* role, which cannot be easily categorised. It is important that the *sui generis* nature of this role should be recognized and that the tasks and responsibilities for data protection compliance should be clearly allocated among the Commission and competent authorities.

The Commission's activities are governed by Regulation (EC) No 45/2001 and subject to the supervision of the European Data Protection Supervisor ("**EDPS**").

9. LEGAL BASIS

9.1. Applicability of Directive 95/46/EC and Regulation (EC) No 45/2001. The CPCS is used for processing of data of sellers and suppliers who are suspected of certain infringements of consumer protection laws. These sellers and suppliers may be corporate entities, but, importantly from the data protection perspective, they may also be natural persons. In addition, the CPC Implementing Decision specifically provides data fields for the exchange of information regarding directors of the suspected sellers or suppliers. Finally, personal data relating to other individuals, for example, owners or employees of the sellers or suppliers, complainants, officials, or witnesses may also be included in attachments and short summaries, which are also specifically provided for in the CPC Implementing Decision. Therefore, there is no doubt that the use of CPCS involves processing of personal data as defined in Article 2(a) of Directive 95/46/EC and corresponding provision of Regulation (EC) No 45/2001.

9.2. Legal basis and lawfulness of the processing. Article 7(c) of Directive 95/46/EC provides that personal data may be processed if "processing is necessary for compliance with a legal obligation to which the controller is subject". In addition, Article 7(e) also allows processing if "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed". Articles (5)(a) and (b) of Regulation (EC) No 45/2001 contain similar provisions.

Article 7(c): legal obligation on controllers. As discussed in Section 3.3, the establishment of the CPCS is required by the CPC Regulation. The CPC Regulation also imposes an obligation on all competent authorities to exchange data with respect to mutual assistance exclusively through the database. The CPC Regulation is directly applicable to competent authorities in all Member States.

Article 7(e): performance of a public interest task. The CPCS helps fight cross-border infringements of European consumer protection laws, in particular, by facilitating the coordination of activities of the various competent authorities in different Member States. This serves public interest. The issue of "necessity" is discussed in Section 10.1 below.

Based on the foregoing, the Working Party is satisfied that Articles 7(c) and (e) of Directive 95/46/EC can be regarded as an appropriate legal basis for the processing.

10. DATA QUALITY

10.1. Purpose limitation, no further use for incompatible purpose. Pursuant to Article 6(1)(b) of Directive 95/46/EC, personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". Regulation (EC) No 45/2001 provides a similar requirement.

Purpose limitation set by the CPC Regulation. Article 13(1) of the CPS Regulation provides that "information communicated may only be used for the purposes of ensuring compliance with the laws that protect consumers' interests." Article 13(2) adds to this that "competent authorities may invoke as evidence any information, documents, findings, statements, certified true copies or intelligence communicated, on the same basis as similar documents obtained in their own country."

The Working Party welcomes the purpose limitation set to the use of the data. It emphasizes, however, that the permissible purposes and any limitations of use must be more specifically defined at the operational level. For this reason, the Working Party makes the following recommendations:

Use by competent authorities should be limited to case-specific cooperation. There is an inherent danger that large electronic databases of this kind may be used to systematically search for individuals and profile them based on search results. Considering that such use is not specified in the CPC Regulation, and no safeguards are provided in this respect, the Working Party recommends that the information in the database should only be used in connection with investigation or enforcement of the specific case with respect to which a mutual assistance request or alert was communicated in the first place, unless additional uses are specifically provided for in a new CPC Implementing Decision, and adequate data protection safeguards are established.

The purposes for which the Commission may use the data should be clearly specified. In some cases the Commission uses the data for purposes specified in the CPC Regulation, in particular, to assist competent authorities in case of certain disputes, or to participate itself in coordinated investigations involving more than two countries (see Section 10.2 below). These are all permissible uses defined in the CPC Regulation.

For the most part, however, the CPC Regulation does not explicitly specify what should be the purpose of the Commission's use and access to data. This is the case with respect to both alert and feedback information. Presumably the Commission is intended to have access to these data so that it could (i) monitor the application of the CPC Regulation, (ii) monitor the application of specific consumer protection legislation covered by the CPC Regulation (the directives and regulations listed in its Annex), and (iii) could compile statistical information in connection with carrying out these duties. These uses are permissible. The Commission, however, should make sure that the personal data contained in the alert and feedback information it receives are not used for additional, non-specified purposes. These should be clearly specified in a new CPC Implementing Decision and the CPCS system architecture should also be re-configured accordingly.

10.2. Necessity and proportionality

Pursuant to Article 6(1)(c) of Directive 95/46/EC personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".

Pre-defined, optional data entries; limited access to the database. The Working Party welcomes, first, that the CPC Implementing Decision establishes a defined list of data fields that may be included in the database. Second, the Working Party also welcomes that the Decision does not require all data-fields to be completed every time, but beyond certain essential minimum requirements, it leaves it up to the competent authority uploading the data to decide which data field it will complete and in what level of detail. Third, the Working Party welcomes that only competent authorities designated by each Member State have access to the CPCS, and within such authorities, only specific named officials.

Proportionality analysis on a case by case basis. The Working Party is also satisfied that the list of the data fields, overall, appears to be reasonable and not excessive for the purposes sought by the CPCS (exceptions and concerns will be noted below).

That being said, it is not possible for the Working Party to determine in advance whether the use of all data fields is appropriate in all specific cases. In addition, some data fields are so broadly defined that it is almost entirely up to the specific enforcement official uploading data in any given case to determine how much personal data will be included in the database. For example, an attachment may contain copies of invoices containing customer names and bank account numbers, or a list of customer email addresses where a spammer sent its messages. Whether such data are appropriate to be included in the database will depend on the particular case.

Therefore, the Working Party notes that the "necessity" and "proportionality" of the data processing has to be analysed *in concreto*, for each particular case when information is uploaded or retrieved and used.

In particular, competent authorities must ensure with respect to each upload of information that (i) they only upload as much personal information as is strictly necessary to achieve the purposes of efficient co-operation, and (ii) they share information only with those competent authorities of other Member States which need to have access to the information. In addition, they must also ensure that they keep personal data in the database no longer than it is necessary to achieve the purposes of the cooperation.

Training of enforcement officials, guidelines to database use, technical means to remind of compliance. This is an assessment that enforcement officials must carry out each time they transfer or otherwise process information. Enforcement officials responsible for CPCS should be made aware of the importance of a serious case-by-case proportionality analysis. In order to ensure that the Commission and competent authorities process data in accordance with the data quality principle, the Working Party recommends that the Commission, as the operator of the system, issues a set of guidelines ("**CPCS Guidelines**") addressed to enforcement officials with access to the CPCS describing the rules to follow towards ensuring compliance with data protection rules. The CPCS Guidelines must be written in such a way that they would be easily understood by people without specific data protection background. The Guidelines may, for example, take the form of Frequently Asked Questions posted on the CPCS and made available to all users. The Guidelines should cover all data protection aspects of the CPCS, but special emphasis should be given to the issue of case-by-case proportionality analysis.

Although the CPCS Guidelines would be prepared by the Commission, with respect to most processing operations (e.g. uploading information onto CPCS, designating recipients of alerts), it will ultimately be the competent authorities who remain responsible under their national laws for compliance with data protection requirements, including for carrying out a case-by-case proportionality analysis. Therefore, to achieve a high level of compliance, the content of the Guidelines and data protection elements should also be fully integrated into any training provided to enforcement officials regarding the use of the CPCS.

Finally, to the extent technically feasible and operationally practical, the technical features of the CPCS should be modified to prompt enforcement officials to assess data protection aspects each time they access the database. Again, these features should not be limited to the proportionality aspect.

Information regarding directors. The CPC Regulation does not specifically suggest or require that information regarding the directors of sellers or suppliers suspected or convicted of infringements should be included in the database. The CPC Implementing Decision, however, requires establishment of data fields for directors' names with respect to any information exchange the same way as it requires an entry for the address and telephone number of the seller or supplier.

The Working Party acknowledges that exchanging information about the seller's or supplier's directors may be necessary in certain cases. For example, the same individuals may use a series of corporate entities as vehicles to carry out fraudulent activities. Therefore, enforcement officials may have a legitimate need to exchange information regarding these individuals.

However, the Working Party emphasises that this exchange, at the same time, also raises serious privacy concerns. Indeed, including information regarding directors in the CPCS may lead to a serious privacy violation and may, in some situations, be tantamount of accusing them of being "guilty by association" and could have a damaging effect on their reputation and business prospects. The Commission itself took notice of this problem, and have, thus far, decided to block this feature on the database. For this reason, the Working Party recommends that the CPCS Guidelines specifically provide that enforcement agents must assess in each case whether inclusion of a given director's name is proportionate or not.

Information regarding consumers, complainants, and other third parties in "short summaries" and "attachments". Among the data fields that may be used in case of alerts, information requests, and enforcement request, the CPC Implementing Decision includes a data field for "attached documents". In addition, in case of alerts, the CPC Implementing Decision also foresees "short summaries".

It is possible that the attached documents or short summaries may contain personal data of complainants, consumers, witnesses, employees, owners, officials, or other third parties. For example, an attachment may contain copies of invoices containing customer names and bank account numbers, or a list of spammed personal email addresses.

The communication of some of these documents, including personal data may be justified in certain circumstances. However, the Working Party recommends that whenever possible, personal data should be omitted from the short summaries and obliterated or otherwise removed from the attached documents (for example, by blackening out the name, address or credit card number of the data subject). In case of doubt regarding the necessity of transferring information or documents with personal data in them, the Working Party recommends that the personal data should be removed. In case it subsequently turns out that the recipient needs an integral copy of a document after all, for example, for evidentiary purposes, it will always have the opportunity to specifically request the missing information from the party that initially provided the document. These recommendations should be clearly specified in the CPCS Guidelines.

Personal data in the "Discussion Forum". As noted in Section 3.3 above, the CPC Implementing Decision provides that Member States must inform the Commission and other Member States via a "Discussion Forum" made available using the CPCS infrastructure of any investigation and enforcement powers granted to competent authorities in addition to those specifically required under the CPC Regulation. During the preparation of this Opinion,

DG SANCO explained that the discussion forum is intended to be used only for exchange of information with respect to issues such as new enforcement powers, best practices, and therefore, it is unlikely that personal data would be included in the exchange of information. In any event, it is important to emphasise that the Discussion Forum should not serve for exchanging case-related data, and as a rule, should not include personal data. This should also be clarified in the CPCS Guidelines.

"Reasonable" suspicion. The Working Party also emphasises that data with respect to suspected infringements may only be included in the database if such "suspicions" are "reasonable". Whereas the interpretation of the term "reasonable suspicion" is left to Member States to be defined, the Working Party emphasises that no data can be included in the CPCS if there is not at least significant intelligence, or some evidence that an infringement has indeed occurred. Another matter for the CPCS Guidelines to discuss.

Commission's access rights should be more limited. Although the language of the Commission's Issue Paper initially raised doubts in this respect, it appears that the Commission's current access to data does not go beyond what is required under the CPC Regulation.

The Working Party welcomes this and emphasizes the importance that the Commission's access should be strictly limited to what is required under the CPC Regulation. In particular, the Commission should have no access to communications between Member States relating to requests of information under Article 6 or requests for enforcement under Article 8. DG SANCO's plans to limit (with certain exceptions) the Commission's access to information flagged confidential are also welcome.

As discussed in Section 5.1, feedback information with respect to both information requests and enforcement requests are specifically required to be provided to the Commission under Articles 7(2) and 8(6) of the CPC Regulation. This feedback information presumably contains sufficient high-level information to enable the Commission to monitor the implementation of the CPC Regulation and to retrieve and compile aggregate statistical information. Therefore, further systematic access to all case-related data of information requests and enforcement requests should not be necessary, even for purposes of extracting statistical information.

The new CPC Implementing Decision should specifically limit the Commission's access to what is required under the CPC Regulation and strictly necessary to carry out its tasks. In addition, it must also be ensured that the CPCS system architecture should be designed accordingly.

Access by competent authorities should be limited on a need-to-know basis. The CPCS is currently set up allowing each competent authority to freely designate the addressees of the alert messages. Therefore, it cannot currently be excluded that a competent authority would circulate alerts more widely than strictly necessary for purposes of the alert, "for information only". Competent authorities must be aware that they must assess on a case by case basis the proportionality of the transfer to all recipients and should not circulate information more broadly than is necessary for the purposes of efficient cooperation. Another matter for the CPCS Guidelines and system architecture.

During the preparation of this Opinion, DG SANCO also explained that it plans to build the system in such a way that feedback information pursuant to Articles 8.6 and 7.2 will be sent

to all authorities responsible for the enforcement of the laws related to the consumer protection directive or regulation in question (e.g. directive on e-commerce or time-sharing). The Working Party recommends that the issue of recipients and the content of feedback information are regulated at the level of the new CPC Implementing Decision, after a careful assessment of the proportionality of the proposed approach.

10.3. Accuracy. Article 6(1)(d) of Directive 95/46/EC requires that personal data must be "accurate and, where necessary, kept up to date", and "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified." Regulation (EC) No 45/2001 provides for similar requirements.

As will be discussed in Section 11 regarding conservation period, the CPCS as currently designed does not contain sufficient safeguards that potentially outdated data will not be kept in the database for long periods of time, for example, if cases drag on without any actions being taken, or if the competent authority "forgets" to notify the Commission about the closure of a specific case.

In this respect the Working Party is of the opinion that a periodic review of the information by the competent authority which supplied the information would contribute towards the accuracy of the data stored in CPCS. To encourage users to carry out such an evaluation, a reminder feature may be built into the database, alerting users periodically, for example, every six month or once a year, to verify the accuracy of the information that they uploaded. Any information, then, can be visibly and electronically tagged with a stamp evidencing that the verification has been carried out. Any other comments could also be added regarding the status of the case.

11. CONSERVATION PERIOD

Article 6(1)(e) of Directive 95/46/EC provides that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed".

Establishment of the conservation periods as described in Section 6 above raise significant data protection concerns. Indeed, without the necessary safeguards and limitations, the CPCS risks becoming a giant database containing outdated and inaccurate information held for long periods of time and used by competent authorities to fish for information for purposes not specified in the CPC Regulation.

11.1. Five year retention period following enforcement. Most importantly, the CPC Regulation requires a five-year mandatory retention period for data related to infringements where an enforcement measure was taken, without, however, specifying the purpose of the retention of data for such a long period of time. This mandatory retention period risks transforming the CPCS into an all-European database of blacklisted companies. Natural person sellers or suppliers, as well as directors, employees, or others persons involved and included in the database could be deemed persons "not to be trusted" based on, sometimes, merely some association with an infringing company. Whether this was the intention of the legislators, cannot be known. However, it is clear that they neither made such intention explicit, nor provided the necessary data protection safeguards to ensure that data can be safely used for these additional purposes.

The Working Party here reiterates its regrets that it had not been consulted in time before the adoption of the CPC Regulation. Had it been consulted at that time, it would have expressed its serious concerns about the proportionality of the five year time-limit and would have also insisted that the purposes for which data should be retained would be clearly specified.

The Working Party maintains these concerns and would welcome a change in the CPC Regulation. Considering, however, that the Working Party has to express its Opinion on this matter after the facts have been established, the Working Party recommends, as a practical measure, that until such time as the legislators amend the CPC Regulation to either specify the purpose of such retention or to no longer require it, the Commission and competent authorities interpret the five-year data retention requirement the narrowest possible way, and, at the same time, introduce a minimum set of safeguards. This should mean, among others, a data-protection-friendly clarification and resolution of the following issues:

- What is the purpose of the five-year data retention in the first place?

- To what data does the five-year period apply?

- When does information need to be notified for deletion?

These questions should be answered so as to ensure that only the minimum amount of personal data required for efficient cooperation are retained. The answers should be formalized in a new CPC Implementing Decision and changes should also be implemented in the CPCS system architecture.

11.2. Cases that are "forgotten" or otherwise not notified for deletion. The CPC Regulation and the CPC Implementing Decision place an obligation on competent authorities to notify the Commission once cases are closed, or the competent authority establishes that an alert is unfounded. However, there are several loopholes that need to be closed. These include the following:

- A competent authority may simply decide not to close an open case even if no investigative measures have been taken, and no new information came to light in the case for a long period of time. In other words: cases sometimes simply drag on.

- A competent authority may also close the case, but "forget" to notify the Commission that the data related to the case needs to be deleted from the database.

- A requested authority may end up not taking an enforcement measure, and therefore, not notify the Commission, nevertheless, the infringement ceases, due to other reasons (for example, due to initiation of a lawsuit by third parties).

To address these concerns, the Working Party recommends that the "logic" of retention-deletion should be reversed: cases should be presumed to be closed after a certain, reasonable amount of time following the sending of the information or enforcement request, and data should be deleted from the CPCS at that time, after alerting the competent authorities involved, and offering a possibility to confirm that the case is still ongoing. Prolongation should be granted for a specific period of time only, and thus, the necessity of storage would be periodically reassessed. In case of failure to request prolongation, all case-related information should be deleted.

To ensure that information will not get "mistakenly" deleted, repeated alerts and reasonable "grace periods" may be built into the system to cater for the situation when a competent authority fails to reply promptly. During the preparation of this Opinion, DG SANCO explained that it is already in the process of establishing a system to ensure that competent authorities would be reminded periodically, perhaps every 6 or 12 months, if some of their cases appear to be "dormant". The Working Party welcomes this initiative and encourages that these plans be further developed to more fully address the recommendation made in this Opinion.

11.3 Conservation of data outside the CPCS. Finally, the Working Party points out that in this document, it does not discuss the issue for how long a competent authority may keep the data exchanged through the system outside the system, for example, in a hard copy printout attached to the case file dealing with the specific case. However, it calls the competent authorities' and the Commission's attention to the fact that data protection laws and principles equally apply to storing information outside the CPCS.

12. PROCESSING OF SENSITIVE DATA

12.1. Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. Article 8 of Directive 95/46/EC prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Article 10 of Regulation (EC) No 45/2001 contains a similar prohibition.

No such data are systematically processed in the CPCS, although processing is not specifically prohibited under the CPC Regulation or the CPC Implementing Decision and it is possible that such data may, on occasion, be included in the information exchanged. For example, data relating to a customer's sensitive data may be included in an attachment as evidence with respect to purchases of specific products or services.

The Working Party recommends that the CPC Implementing Decision should be modified to make processing of this special category of data explicitly prohibited, while allowing, if necessary, certain narrowly defined exceptions.

12.2. Data relating to offences, suspected offences and security measures. Article 8(5) of Directive 95/46/EC establishes that "[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations that may be granted by the Member State under national provisions providing suitable specific safeguards. Member States may provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of official authority"

CPCS systematically includes data relating to offences and suspected offences, in particular activities in breach of consumer protection legislation. These may involve both administrative and criminal offences. Administrative sanctions, criminal convictions, judgments in civil cases and security measures may also be included in the database.

In the present case, processing of such data is authorized by the CPC Regulation, which is directly applicable in Member States. The Working Party, however, emphasizes, that the CPC Regulation should not be regarded as granting a blanket and unconditional authorization to process this type of sensitive data. The use of the data must be limited to the specific purposes of mutual assistance, as described in the CPC Regulation.

12.3. National identity number. Article 8(7) of Directive 95/46/EC provides that Member States "shall determine the conditions under which national identification number or any other identifier of general application may be processed". In turn, Article 10(6) of Regulation (EC) No 45/2001 provides that "the European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body".

None of the CPC Regulation, the CPC Implementing Decision or the Commission's Issue Paper suggests that any national identification numbers would be systematically used through the system. Importantly, the CPC Implementing Decision, when specifying the various data fields which are to be used to identify a seller or supplier, while mention other data, such as address and telephone numbers, does not provide for a specific entry for national identification numbers. With that said, it cannot be excluded that an enforcement official of a competent authority could not upload national identification numbers of certain persons, for example, natural person sellers or suppliers, directors or employees, complainants, witnesses, or other parties involved.

Considering the sensitive nature, at least in some Member States, of national identity numbers, the Working Party recommends that unless identification is strictly necessary, and cannot reliably be carried out by other means (for example, by using address, job title, or other identifier), the use of national identity numbers should be avoided in the CPCS. In any event, should national identity numbers be used in these exceptional circumstances, any restrictions under national data protection laws must be fully taken into account when uploading or further processing these data.

13. EXEMPTIONS AND RESTRICTIONS

Article 13(4) of the CPC Regulation provides that for the purpose of applying the CPC Regulation, "Member States shall adopt the legislative measures necessary to restrict the rights and obligations under Articles 10, 11 and 12 of Directive 95/46/EC as necessary to safeguard the interests referred to in Article 13(1)(d) and (f) of that Directive. The Commission may restrict the rights and obligations under Articles 4(1), 11, 12(1), 13 to 17 and 37(1) of Regulation (EC) No 45/2001 where such restriction constitutes a necessary measure to safeguard the interests referred to in Article 20(1)(a) and (e) of that Regulation."

This provision does not replace the pre-existing heterogeneous system whereby restrictions on rights of data subjects, in particular, their information rights and rights of access, varied pursuant to the different legislative exemptions adopted Member State by Member State. This may be understandable considering the existing differences among Member States in matters involving criminal, administrative or judicial procedures and access to documents in connection with such procedures. However, the lack of harmonization in this regard also makes data protection compliance and cooperation among Member States regarding granting access to data subjects particularly difficult, as it will be shown in Section 15 below. To

facilitate a common understanding and encourage national legislators to build on a common set of principles, the Working Party makes the recommendations noted below.

13.1. Exemptions and restrictions to be set by Member States. Article 13(1)(d) provides that restrictions may be permissible when they constitute a necessary measure to safeguard "the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions". Article 13(1)(f) further provides that the same exception applies to "monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority" under Article 13(1)(d).

The Working Party recommends that Member States, when adopting measures to restrict the rights and obligations under Articles 10, 11 and 12 of Directive 95/46/EC, take into account that such restrictions must be limited to what is strictly necessary to safeguard the interest referred to in Article 13(1)(d) and (f) of Directive 95/46/EC.

First, any restriction should apply only with respect to the data subjects' information rights under Articles 10 and 11 of Directive 95/46/EC or to their rights of access, rectification, erasure, or blocking under Article 12. Restriction of any other rights listed under Article 13 of Directive 95/46/EC, in particular, the principles relating to data quality or the requirement of notification to the data protection authorities, is not permissible.

Second, neither Directive 95/46/EC nor Regulation (EC) No 45/2001 provides for a blanket, systematic rule depriving all data subjects whose data may be processed in connection with criminal offences and breaches of ethics for regulated professions of their information and access rights. The adoption of restrictive measures should not arbitrarily, disproportionately, and systematically restrict data subjects' information rights or their right to access their personal data.

Any restrictions may only be permissible if the provision of information to data subjects, or allowing them right of access would jeopardize the purposes of "prevention, investigation, detection and prosecution". In other words, using the terminology of Article 13(3) of the CPC Regulation, any restriction may only be permissible if granting rights to data subjects would "undermine the purpose of inspections or investigations".

Although general legislative guidance is welcome as to when this may be the case, it requires a case by case analysis on the facts of each case whether the restriction of access of information rights is permissible. Further guidance should be given in the CPCS Guidelines referred above.

Third, exceptions to the data protection rights only apply temporarily, so long as they are necessary to safeguard the purposes of "prevention, investigation, detection and prosecution".

Fourth, data subjects must be informed of the principal reasons on which the restriction is based and of their right to have recourse to national data protection authorities. The provision of information can be deferred for as long as such information would deprive the restriction of its effect.

Finally, and in any event, the Working Party recommends that any restrictions would be clearly indicated on the privacy statements of each competent authority.

13.2. Exemptions and restrictions to be set by the Commission. The CPC Regulation provides similar possibilities for the Commission to restrict the rights of data subjects.

However, the Commission's rights are broader than that of Member States. In particular, the Commission may also restrict the provisions of Regulation (EC) No 45/2001 regarding data quality, and may retain traffic data relating to users upon termination of the call or other connection.

The Working Party points out that all observations noted above with respect to the restrictions that may be applied by competent authorities in Member States equally apply to the Commission.

In addition, the Working Party is concerned about the possibility provided in the CPC Regulation for the Commission to restrict the provisions of Regulation (EC) No 45/2001 regarding (i) data quality and (ii) the retention of traffic data.

The possibility for restrictions on fundamental principles, such as the principles relating to data quality must be strictly limited to cases where such restriction is indispensable. Indeed, the Working Party has difficulty imagining a situation when such restrictions would be necessary in the context of cooperation between consumer protection authorities on matters such as misleading advertisement, package travel, or timeshare even when they involve fraudulent activities.

As for the possible retention of traffic data by the Commission, the Working Party fails to understand for what purpose this provision could conceivably be invoked, considering that all traffic data in CPCS relates to data exchanged among competent authorities and there is no reason for the Commission to retain any traffic data with respect to these communications over and above what is otherwise permissible (for example, retention for six months to allow verification of authorized use). Until the content of the data itself is in the database, it is legitimate to store certain traffic data such as "date of upload" in the system. Once content of the communication is deleted, for example, once an alert is withdrawn, there is no need to retain any traffic data.

14. INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Pursuant to Articles 10 and 11 of Directive 95/46/EC, controllers are required to inform data subjects of the fact that their data are being processed. Similar requirements are also set forth in Regulation (EC) No 45/2001. Individuals also need to be informed of, among others, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to. The right of information is essential in and of itself. In addition, it also enables individuals to exercise other rights: if individuals are not aware that their personal information is being processed, they will not be able to exercise other rights such as the right of access and rectification.

None of the CPC Regulation, the CPC Implementing Decision or the Commission Issue Paper provides any provisions regarding the information rights of the data subjects (except as noted in Section 13 with respect to restrictions). The Working Party recommends a layered approach to notice provision.

14.1. Comprehensive privacy notice on the Commission's CPCS webpage. First, the Commission, on its webpage dedicated to the CPCS, should provide a comprehensive privacy notice including all items required under Articles 11 and 12 of Regulation (EC) No 45/2001. This notice should also provide a description of the CPCS, the roles of the Commission and

the competent authorities, at the level of detail at least comparable to the explanations provided in this document. The Working Party also recommends that the Commission's privacy notice specifically sets forth how data subjects can exercise their rights of access and what restrictions there are to such rights, without, however, explaining in detail the various specific restrictions in place in different Member States. The privacy statement must be drafted in a clear and simple language that must be understandable by data subjects who have no background in data protection.

14.2. Privacy notice on the web pages of competent authorities. In addition, each competent authority should provide a privacy notice on its webpage. In this respect, the Working Party also notes that in addition to the requirements under Directive 95/46/EC, Article 4(8) of the CPC Regulation specifically provides that "each competent authority shall make known to the general public the rights and responsibilities it has been granted under this Regulation". The privacy notice should include reference and link to the Commission's privacy notice and further details specific to that particular authority or Member State. Any country-specific limitations on the rights of access or information must, for example, be set forth on these notices. Notice provision may be coordinated by the single liaison office among the competent authorities within a specific country.

14.3 Notice given directly to data subjects. At the latest at the time of uploading personal data, and unless a restriction may be applied (see Section 13), notice must also be given to data subjects by means other than the privacy notice on the website. A recommended approach may be to include a brief reference to the CPCS and a link to the relevant privacy notices on the Internet in any correspondence exchanged with the data subject (seller, director, complainant, witness, etc).

If such individual notice provision proved impossible or would involve a disproportionate effort (for example, if the competent authority would not have the contact information of the data subject), individual notice can be omitted. As noted in Section 13, the provision of information may also be deferred if the information rights are temporarily restricted.

15. THE DATA SUBJECTS' RIGHT OF ACCESS TO DATA

Article 12(a) of Directive 95/46/EC, in relevant part, requires that data subjects should be able to obtain from the controller (i) confirmation as to whether data relating to them are being processed, the purposes of such processing, categories of data concerned, and recipients, (ii) communication in an intelligible form of the data undergoing processing and of their source.

In addition, Article 12(b) requires that data subjects should be able to obtain from the controller as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46/EC, in particular because of the incomplete or inaccurate nature of the data. Regulation (EC) No 45/2001 contains similar provisions.

None of the CPC Regulation, the CPC Implementing Decision or the Commission Issue Paper provides any provisions regarding data subjects' rights of access. Indeed, this is a complex issue, considering the various actors involved in the data processing activities.

Several competent authorities, as well as the Commission each have access to certain personal data uploaded to the system. Often several actors have access to the same information. For

example, usually two, sometimes more, authorities have access to information and enforcement requests. A number of authorities, as well as the Commission may have access to alert information. Data subjects may approach different authorities to require rights of access.

The situation is all the more difficult, as rules regarding restrictions on access vary Member State by Member State, as discussed above in Section 13. Considering that there may be different restrictions set on rights of access in the different Member States, it is possible that one Member State would allow access to the same data, whereas another would not. Therefore, it is indispensable that competent authorities cooperate with respect to each access request they receive.

The Working Party's recommendations below describe two situations, which require specific coordinative measures to ensure compliance: (i) where information is requested from one competent authority but granting access to the data may affect the investigative or enforcement activities of the other, and (ii) where the data subjects address their access requests to the Commission.

15.1. Coordination as between competent authorities. The Working Party recommends that if granting access to personal data may affect the investigation or enforcement procedure carried out by other competent authorities, the competent authority to whom the access request has been submitted should request the opinion of the other competent authorities before granting access.

Access then should be granted only if the other competent authorities involved had been given the opportunity to state their positions, and any objection to granting access based on a specific exemption under their national data protection laws had been considered. If the authorities failed to respond within a reasonable time or failed to raise objections, the authority to whom the access request has been submitted may decide based on its own national law alone whether an exemption applies or whether access should be granted. If the authorities are not in agreement as to whether access should be granted, the authority which supplied the information should be the one to ultimately set the criteria for access provision.

Similar cooperative mechanism should apply with respect to rectification, erasure or blocking.

The Working Party, however, emphasises that this coordination procedure should not be used to arbitrarily deny access to data subjects, or to artificially prolong the time necessary to grant right of access. In addition, in case an access right is denied, it must be made clear on what grounds it was denied and whether the data subject may contact another competent authority instead to access the data.

15.2. Coordination as between the Commission and competent authorities. It is possible that data subjects may turn to the Commission requesting right of access to their data.

In this respect, first of all, it must be emphasized that the Commission can only provide access to data to which the Commission itself has legitimate access to. Therefore, the Commission will not be under an obligation to provide access to information requests, enforcement requests and related communications. In these cases, it needs to direct the data subjects to the authorities which have access to the information.

The situation is different with respect to information to which the Commission has legitimate access to, for example, alert information or feedback information. In this respect the Working

Party recommends that the Commission, if an access request has been submitted to it, requests the opinion of the competent authority which supplied the information in the first place. Access then should be granted only if the supplying partner has been given the opportunity to state its position, and any objection to granting access based on a specific exemption under its national data protection laws have been observed. If the supplying partner fails to respond within a reasonable time or fails to raise an objection, the Commission may decide based on Regulation (EC) No 45/2001, whether an exemption applies or whether access should be granted.

In addition to contacting the competent authority which supplied the information, the Commission must also give the opportunity to express their concerns to all other competent authorities whose investigative or enforcement activities may be jeopardized. However, if the authorities are not in agreement as to whether access should be granted, the authority which supplied the information should be the one to ultimately set the criteria for access provision.

Similar cooperative mechanism should apply with respect to rectification, erasure or blocking.

16. MEASURES FOR REDRESS

Without prejudice to the availability of administrative remedies before the national data protection authorities or the EDPS, Article 22 of Directive 95/46/EC requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him under applicable data protection laws. Article 23, in particular, requires Member States to provide that any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

According to the Working Party's analysis of the CPCS actors, as described in Section 8, the Commission, single liaison offices and competent authorities are each considered as controllers with respect to their own tasks and responsibilities and will each be liable in connection with their own roles, tasks, and responsibilities.

17. SECURITY

Pursuant to Article 22 of Regulation (EC) No 45/2001, the controller must implement appropriate technical and organizational measures to ensure the level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. Directive 95/46/EC requires similar security measures.

The Commission, which is the operator of the CPCS and a controller designated under the CPC Regulation, is subject to the provisions of Regulation (EC) No 45/2001.

Considering, on one hand, that national data protection laws are to a large extent harmonized based on Directive 95/46/EC, and on the other hand, taking into account that such harmonization is not complete, and certain differences exist among the different Member States as to the acceptable level of security, the Working Party recommends that the security provisions of Regulation (EC) No 45/2001 should be interpreted in line with best practices in Member States. Member States should also be encouraged to increase security of access by competent authorities.

Should there be a security breach or breach of confidentiality, data subjects may complain to the EDPS who has supervisory powers over the Commission pursuant to the provisions of Regulation (EC) No 45/2001. The EDPS may also carry out a security inspection or audit of the database on its own initiative. This may take place both within the framework of and outside the prior checking procedure noted in Section 18 below.

18. NOTIFICATION AND PRIOR CHECKING

18.1. National data protection authorities. In application of Articles 18 to 20 of Directive 95/46/EC, competent authorities in several Member States have to notify their processing operations under the CPCS to national data protection authorities. In some Member States it is possible that the processing operations may also need to be prior checked by the national data protection authorities.

In Member States providing for such a procedure, the processing operations are subject to prior checking by the national data protection authority on grounds that they are likely to present a specific risk to the rights and freedoms of the data subjects. This is the case, for example, where national law requires the processing of data relating to criminal offences or suspected offences to be prior checked. The evaluation of whether such processing operations fall under prior checking requirements depends on national legislation and the practice of the national data protection authority.

18.2. Prior checking by the EDPS. The information exchanged contains personal data regarding offences, suspected offences, criminal convictions, and possibly also security measures. Considering the nature of the data and the role of the Commission in the present case, the database should be subject to prior checking under Article 27(2)(a) of Regulation (EC) No 45/2001.

In addition, the processing also falls under Article 27(2)(b) of Regulation (EC) No 45/2001, which provides that processing operations which "evaluate personal aspects relating to the data subject, including his or her (...) conduct" should be subject to prior checking by the EDPS. Indeed the data included in CPCS may be used to evaluate the conduct of the individuals (traders, directors, perhaps also staff members or others) who are alleged to be involved in wrongdoings in order to determine the appropriate measures to take (investigatory or enforcement measures).

The prior checking is all the more necessary as (i) the details of the database were not set up in a high-level Parliament and Council regulation or directive, (ii) the EDPS did not advise legislators during the legislative process, and (iii) the Commission is designated as a controller under the CPC Regulation.

As the system is already is use, the EDPS will have to carry out the prior checking review "ex post".

18.3. Coordination of notification and prior checking procedures. Considering that the competent authorities as well as the Commission are all controllers, and that in some Member States there are several competent authorities, the Working Party recommends that the prior checking procedures be coordinated among the national data protection authorities and the EDPS so that a consistent approach may be developed.

19. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 14(2) of the CPC Regulation provides that information communicated under the CPC Regulation "may also be communicated to an authority of a third country by a competent authority under a bilateral assistance agreement with the third country, provided the consent of the competent authority that originally communicated the information has been obtained and in accordance with Community legislation regarding the protection of individuals with regard to the processing of personal data."

Pursuant to Article 25 of Directive 95/46/EC, transfers to a third country may take place only if the third country in question ensures an adequate level of protection. Article 26 of Directive 95/46/EC provides for certain derogations from this principle. These include Article 26(1)(d), which provides that "the transfer is necessary or legally required on important public interest grounds". Article 26(2) further provides that Member States may also authorize transfers where the controller adduces adequate safeguards, in particular, by way of appropriate contractual clauses.

Implementation and interpretation of these provisions may vary Member State by Member State. Therefore, the Working Party welcomes that the CPC Regulation specifically makes any third country transfer subject to the consent of the competent authority that originally communicated the information.

The Working Party further recommends Member States to ensure that the bilateral assistance agreements with third countries will be revised to provide for adequate data protection safeguards.

20. CONCLUSIONS

In conclusion, the Working Party is satisfied that the CPCS has an appropriate legal basis, is established for lawful purposes, and may, provided that the recommendations of the Working Party will be fully taken into account, serve as a data-protection compliant tool to help cooperation among competent authorities and the Commission.

With that said, the Working Party reiterates that it regrets that it had not been consulted at an earlier stage of the procedure, prior to the adoption of the CPC Regulation, the CPC Implementing Decision, and the start of the operation of the CPCS.

For the time being, working with the text of the CPC Regulation as is, the Working Party recommends several measures that should be taken by the Commission and the competent authorities to improve data protection compliance. In some cases, taking the measures may require recourse to the regulatory procedure and issuance of a new CPC Implementing Decision with the aid of the Regulatory Committee. Other recommendations may be implemented at a more operational level, by the Commission, through the CPCS Guidelines and training provided to enforcement officials, and changes in the CPCS system architecture.

The Working Party also emphasizes that while operating and using the system, competent authorities and the Commission must be aware of the special nature of their co-controlling relationship, the diversity of applicable data protection laws and supervisory authorities, and must make sure that they fully cooperate to ensure compliance with data protection laws.

The Working Party recommends, in particular, the following:

- Enforcement officials working for competent authorities should assess on a case by case basis compliance with data protection principles.

  - To assist them in their decision-making the Commission should prepare and make available the CPCS Guidelines.

  - Whenever possible, the CPCS technical features should also be redesigned to include reminders and other technical measures to help data protection compliance.

  - Data protection elements should be integrated into the training of enforcement officials.

- The purposes for which competent authorities and the Commission may access the database should be limited and clearly specified. Commission should have no access to information and enforcement requests (except high-level feedback information) and its access to information "flagged" confidential must also be limited to cases where such access is necessary and proportionate.

- Enforcement officials should limit inclusion of personal data to the extent strictly required for purposes of efficient cooperation. This applies, in particular, to information regarding directors, as well as to all other personal data in attachments and short summaries.

- Enforcement officials should also not circulate alerts or mutual assistance requests more widely than strictly necessary.

- Steps should be taken to periodically verify the accuracy of data uploaded in the database.

- Enforcement officials should periodically revise whether retention of the information continues to be necessary. The logic of retention-deletion should be reversed: following a reminder (or possibly, repeated reminders and reasonable grace periods), data should be automatically deleted, unless competent authorities confirm that they have not yet closed the case.

- Individuals must be informed of their data being uploaded in CPCS, via a layered approach, which includes website notices but also information provided directly to the data subjects concerned. This right should not be limited systematically, as restrictions to a fundamental right cannot be applied systematically. The same applies to the right of access. An efficient cooperation mechanism must also be established to provide access to data subjects.

- Security measures should be taken in accordance with best practices in Member States.

- The CPCS must be submitted for prior checking to the EDPS, as well as to data protection authorities in some Member States. Certain other national data protection authorities must be notified. Prior checking procedures must be coordinated.

Done at Brussels, on 21st September 2007

For the Working Party

The Chairman
Peter Schaar