Prior checking Opinion on the Consumer Protection Co-operation System ("CPCS") notified by the European Commission on 9 January 2009

Brussels, 4 May 2011 (case 2009-0019)

Table of contents

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

1. Introduction

1.1. Scope of the Opinion

In this Opinion the European Data Protection Supervisor ("**EDPS**") assesses data protection compliance in the Consumer Protection Cooperation System ("**CPCS**") and recommends further improvements to be made, in particular, technical and organizational measures to be taken by the Commission.

The CPCS is an information technology system designed and operated by the Commission pursuant to Regulation (EC) No 2006/2004 on consumer protection cooperation ("**CPC Regulation**"). The CPCS facilitates co-operation among "**competent authorities**" in EU Member States and the Commission in the area of consumer protection. Co-operation is limited to infringements of a pre-defined set of EU directives and regulations. Further, infringements that fall within the scope of the CPC Regulation need to be of a cross-border nature, and need to harm or be likely to harm the "**collective interests of consumers**".

In the framework of their co-operation, competent authorities exchange information including personal data (see Section 1.3 below).[1] The system is aimed to be a secure communication tool which allows competent authorities to exchange information. In addition, the CPCS also records and stores the information exchanged, often for significant periods of time (see Section 3.3). Therefore, it should also be considered as a database.

The recommendations in this Opinion are addressed to the Commission, which has a central role in designing and operating the CPCS and which is subject to the supervision of the EDPS. With that said, many of the recommendations provided in this Opinion - including those on training, data protection Guidelines, information to data subjects and "privacy by design" solutions built into the system architecture - can also facilitate compliance with data protection rules by other users of the system, such as competent authorities in Member States. Therefore, the recommendations set for the Commission should help ensure a high overall level of data protection within the CPCS.

In parallel with the adoption of this prior checking Opinion (pursuant to Article 27 of Regulation (EC) No 45/2001 (the "**Regulation**")[2], the EDPS is issuing another Opinion (pursuant to Article 28(2) of the Regulation) which comments on the legal framework for the CPCS, focusing primarily on the 1 March 2011 amendment to Commission Decision 2007/76/EC[3]. In that Opinion the EDPS takes stock of the progress made thus far and selectively highlights some of the remaining concerns and considerations for the future. The two documents should be considered jointly.

[1] In addition, the Commission also collects and processes personal data of CPCS users (case handlers) as needed for the operation of the system (for example, to allocate usernames and passwords). This processing activity is not subject to prior checking (see Section 2.2 below), and therefore, it is not discussed further in this Opinion.

[2] Regulation (EC) No 45/2001 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, OJ 2001, L 8/1.

[3] Commission Decision of 1 March 2011 amending Decision 2007/76/EC implementing Regulation (EC) No 2006/2004 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws as regards coordination of market surveillance and enforcement activities.

1.2. Description of the processing

The following information flows are foreseen in CPCS to facilitate co-operation:

- **Exchange of information on request** (Article 6 of the CPC Regulation). Upon request from an applicant authority, the requested authority must supply, without delay, any relevant information required to establish whether an infringement has occurred or whether there is a reasonable suspicion that it may occur.
- **Exchange of information without request** (Article 7). Any authority may send a warning message ("**alert**") to its network counterparts in other Member States and to the Commission to inform them about an infringement to consumer protection laws or about a reasonable suspicion of such an infringement. The authority sending the alert may decide to which other Member States it wishes to send its message. That is, not all alerts necessarily go to all Member States.
- **Request for enforcement measures** (Article 8). An applicant authority may request another authority to take all necessary enforcement measures to bring about the cessation or prohibition of an infringement without delay.[4]
- **"Notifications" (Articles 7(2) and 8(6))**. When an authority takes enforcement measures following an alert or receives a request for mutual assistance following an alert, it must notify the enforcement measures or the request to its network counterparts in all other Member States as well as to the Commission (Article 7(2)). An authority must also notify its network counterparts in all other Member States as well as the Commission of any enforcement measures it has taken following an enforcement request and the effect thereof (including whether the infringement has ceased) (Article 8(6)).
- **Co-ordination of market surveillance and enforcement activities** (Article 9). When an infringement harms the interest of consumers in more than two Member States, the competent authorities concerned coordinate their enforcement actions and requests for mutual assistance. In particular, they may conduct simultaneous investigations and enforcement measures.

In addition to these exchanges, non-case-specific information can be exchanged via a "**forum module**". This forum is not designed to exchange personal data (although it cannot be excluded that this may happen; to minimise inadvertent disclosure of personal data on the forum see recommendations in Section 3.2).

1.3. Personal data processed

When exchanging information in CPCS, several structured data fields are provided for users to complete. Some of these are optional others are mandatory. These data fields describe the type of infringement that occurred or is suspected; the seller or supplier responsible for the infringement (including its contact information, IP address, parent company and directors); the potential harm to consumers; as well as other important case-related information.

With regard to the structured data fields, a data field for company directors' name(s) allows linking information to individuals (the directors listed), and thus, involves processing of personal data.

[4] In this Opinion, "exchange of information on request" and "request for enforcement measures" will sometimes be referred to jointly as "**mutual assistance requests**".

At the time of issuing of this Opinion, the director's name field in the CPCS architecture, although technically available, is not yet in use. Instead, a provisional practice was developed to address the data protection concerns identified in the Opinion of the Article 29 Data Protection Working Group referred to in Section 2.3 below. Accordingly, the names of directors, when uploaded in the CPCS, are currently included in confidential attachments rather than in the specific structured data field foreseen for this purpose.

This means, in practice, that (i) by default, the "Single Liaison Offices" ("**SLO**"s)[5] do not have access to this information; (ii) the Commission has no access to this information and that (iii) not being included in a structured data field, this information is also not searchable in the database.

The practice of using attachments instead of structured data fields is described on page 15 of the document entitled "The Consumer Protection Cooperation Network: Operating Guidelines" endorsed by the CPC Committee on 8 June 2010 ("**CPCN Operating Guidelines**".[6] The Commission is currently awaiting the issuance of this Prior Checking Opinion, and thus, further guidance from the EDPS before starting to use the structured data fields for the directors' names.

Other information processed in the CPCS may, depending on the circumstances of the case, also be considered personal data, and thus, require data protection safeguards.

These may include, among others, the following:

- The infringing seller or supplier may -in some cases- be an individual. In this case, all data relating to his/her business processed in CPCS (e.g. that the business is suspected of an infringement) will constitute his/her personal data protected by the Regulation and, where applicable, by Directive 95/46/EC (the "**Directive**").

- The link between a company's name and an individual can sometimes be very strong and easily re-established (for instance, the company name of a small enterprise may include the surname of the owner while the address of the company may be the same as the private address of the owner). In this case also, the data relating to the business processed in the CPCS are also relevant for the individual[7].

Further, CPCS also contains two non-structured fields for information exchanges:

- a field for "**short summaries**" that is to be filled in as free text[8] and
- a feature to enable attachment of documents.

These may contain personal data, for example, data of employees, complainants or consumers.

[5] As explained below further in Section 1.4, SLOS are specific public authorities designated in each Member State as responsible for coordinating the application of the CPC Regulation.
[6] With regard to access rights, confidentiality flags and search capabilities see Section 1.5 below.
[7] In some Member States the data relating to legal entities are also considered and treated as personal data protected by data protection legislation. In these countries, competent authorities exchanging information in CPCS must ensure the protection of personal data related to companies at least to a certain extent (e.g. with respect to the quality of data or to information or access rights).
[8] The short summaries should not contain personal data (see Section 3.2).

Finally, it cannot be excluded that information exchanged in the forum module may also contain personal data. That said the CPC Data Protection Guidelines (see Section 3.1 below) clearly recommends that enforcement officials should not include personal data in the short summaries and discussion forum.

1.4. Data controllers: roles and responsibilities

The CPCS has several actors involved in various ways in the processing of personal data. There are three "types" of controllers in the CPCS, each with their own specific roles and responsibilities.

- First, each **competent authority** is responsible for its own use of the CPCS (e.g. for the relevance and accuracy of the information it uploads into the system). In its capacity as a user, it thus acts as a controller in the CPCS under national data protection law.
- Second, the CPCS architecture also includes so-called "Single Liaison Offices" ("**SLO**"s). These are specific public authorities designated in each Member State as responsible for coordinating the application of the CPC Regulation.[9] Among their tasks is to route mutual assistance requests to the correct competent authorities. SLOs (each individually) also act as controllers, with respect to their own activities.
- Finally, the **Commission** also has a specific role and specific responsibilities as a controller. The Commission, in particular, plays a central role in defining system functionalities, operates the system, ensures the security of the data exchanged, manages CPCS users and handles technical and security incidents. It is also the only party capable of carrying out some actions (such as deletion of cases). In addition, the Commission has access to some of the personal data exchanged in the system since it is the recipient of alerts as well as notifications.

The EDPS welcomes the fact that:

- The CPC Regulation (in Article 10) clearly specifies that each of the parties mentioned above have their own responsibilities as controllers.
- The CPC Data Protection Guidelines (in Section 3) provide additional details regarding roles and responsibilities.

1.5. Access to information in CPCS

Competent authorities, SLOs and the Commission have access to different categories of information exchanged within the CPCS:

- Competent authorities have access to requests for information and to enforcement requests which are specifically addressed to them; they also have access to alerts (provided that they were selected by the sender as a recipient) and to notifications which fall under their competence.
- SLOs can only read key information on a case to allow them to identify the competent authority to which a request needs to be transferred. They can only access attachments to requests for mutual assistance if these were not "**flagged**" as confidential.[10] They do not have access to alerts and notifications at all.

[9] The co-ordination tasks are defined in Articles 3(d), 9(2), 12(2) and 12(5) of the CPC Regulation.
[10] All attachments are flagged confidential by default. The competent authority uploading the attachment must "unclick" the confidentiality flag if it wishes the content of the attachment to be available to the SLO.

- The Commission CPCS users have access to alerts[11] and notifications; this access is read only. The Commission has no access to mutual assistance requests.

In addition, as the Commission is in charge of the maintenance and operation of the system, its technicians have read and write access to any data in CPCS including personal data.

With regard to search capabilities, the Commission explained to the EDPS that all structured data fields are searchable. Unstructured data fields, such as attachments and free text fields for short summaries are not searchable. Each CPCS user can only search in data to which it has access (for example, the content of a mutual assistance request can only be searched by the two competent authorities that exchanged the information; the content of an alert can only be searched by the competent authority which has uploaded the alert and by those who have received the alert).

The EDPS welcomes the fact that:

- areas of competencies have been assigned to each competent authority: information is only shared with the authorities responsible for a specific legislative area (i.e. one or more specific measures within the area of consumer protection);
- SLOs route requests to the authorities concerned, thus reducing the risk of error in designating the recipients;
- attachments to mutual assistance requests and alerts are flagged confidential by default;
- the Commission's access is limited to what is required under the CPC Regulation. In particular, the Commission has no access to information exchanged between Member States within mutual assistance requests;
- SLOs have access only to key information on a case to allow them to identify the competent authority to which a request needs to be transferred; and
- search capabilities are linked to rights of access.

With regard to the structured data field for director's names, the EDPS has no objection to against the use of a structured data field (instead of including the directors' names in confidential attachments as is the practice currently).

However, unless the Commission provides justification to the EDPS that access to this data field by the Commission is necessary for the performance of its monitoring tasks under the CPC Regulation, the EDPS recommends that technical measures be implemented into the system to exclude such access.

In addition, to ensure that data regarding individuals linked to a seller or supplier suspected of an infringement will not be retained in the database in a searchable way for an unduly long period of time, the recommendations regarding data retention should also be implemented (see Section 3.3.2 below). In any event, in case of suspected infringements, data relating to directors circulated in an alert should not be searchable following the (*prima facie* six-month) period recommended in Section 3.3.2 below. Further limitations on the search capabilities should also be considered if appropriate.

[11] This is with the exception of attachments to alerts, to which the Commission CPCS users have no access.

2. EDPS competence

2.1. Applicability of Regulation (EC) No 45/2001

Insofar as the Commission's activities are concerned, the notified processing falls under the scope of the Regulation and the supervision of the EDPS (see Articles 1 and 3 of the Regulation)[12].

2.2. Grounds for prior checking

Information exchanges in CPCS include personal data relating to infringements or suspected infringements of consumer protection legislation. These may involve both administrative and criminal offences. Therefore, CPCS is subject to Article 27(2) (a) of the Regulation, which requires prior checking by the EDPS of, among others, "processing of data relating to suspected offences, offences, criminal convictions or security measures".

2.3. Proceedings

On 9 January 2009 the Commission notified the EDPS of the CPCS for "*ex-post*" prior checking[13]. The EDPS issued the Opinion on 4 May 2011, after receipt of the necessary information requested from the Commission[14].

The EDPS notes that the CPCS was already in use before the EDPS was notified, and therefore the EDPS recommendations need to be implemented *ex post*. For the future, the EDPS calls the Commission's attention to the fact that the opinion of the EDPS should be requested and given prior to the start of any processing of personal data.

3. Legal analysis & recommendations

3.1. Legal basis and lawfulness of processing

After adopting the CPC Regulation (see Section 1.1), the Commission further strengthened the legal basis of the CPCS by adopting an implementing decision and a recommendation:

- Commission Decision 2007/76/EC of 22 December 2006 implementing the CPC Regulation, as amended on 17 March 2008 and on 1 March 2011 ("**CPC Implementing Decision**")[15]; and

[12] For each competent authority and SLO, the applicable law is its own national data protection law (in conformity with the Directive) and its activity is supervised by its own national/regional data protection authority.

[13] CPCS was previously reviewed by the Article 29 Data Protection Working Party, which issued, on 21 September 2007, its Opinion 6/2007 (WP 139). The advice in the present Opinion is in conformity with Opinion 6/2007.

[14] Pursuant to Article 27(4) of the Regulation, this Opinion must be delivered within two months, discounting any periods of suspension allowed for receipt of additional information requested by the EDPS. The EDPS requested further information from the Commission on 14 January 2009 and on 24 January 2011. These were provided on 22 December 2010 and on 2 March 2011, respectively. The EDPS sent his draft Opinion for comments on 18 March 2011. At the same time, due to complexity, he has also extended the deadline available to issue his opinion by two weeks. The Commission provided its final comments on 14 April 2011. The deadline to issue the EDPS Opinion was, therefore, 4 May 2011.

[15] Commission Decision 2007/76/EC implementing Regulation (EC) No 2006/2004 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws as regards mutual assistance.

- Commission Recommendation of 1 March 2011 on guidelines for the implementation of data protection rules in the CPCS ("**CPC Data Protection Guidelines**")[16].

As pointed out in the Opinion on the new measures adopted by the Commission for the application of the CPC Regulation, the EDPS welcomes that the processing is based on a solid legal basis whose founding pillar is a Regulation adopted by the Council and the Parliament. In addition, the EDPS is satisfied that this initial legal instrument has been complemented over time to provide further details and address data protection concerns.

3.2. Data quality

Article 13(1) of the CPC 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 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*".

Considering the broad scope of these provisions, it is essential that data exchanges within CPCS, on the practical level, meet the standards of data quality as required under Articles 4(1) (a), (b), (c) and (d) of the Regulation. In particular, it is imperative that any personal data exchanged should be adequate, relevant, proportionate and accurate; processed fairly and lawfully; and not further processed for incompatible purposes.

Each case is different. Therefore, compliance with the data quality principles needs to be assessed *in concreto*, for each particular case when information is uploaded, retrieved, or otherwise processed by CPCS users. Considering the difficulties of a case by case assessment, and the fact that most CPCS users are not data protection experts, it is of utmost importance that:

- the CPCS system architecture should be built and configured in such a way to facilitate, to the greatest extent possible, compliance with data protection laws; and that
- the users of the system should be adequately trained, guided, and empowered to take decisions concerning data protection.

The EDPS welcomes that the CPC Implementing Decision provides specific sets of mandatory and optional fields for each exchange of information and that these are proportionate taking into account the purposes of the information exchanges.[17]

The EDPS also welcomes the recommendations included in the CPC Data Protection Guidelines that aim to limit the personal data included in the exchanges of information, in particular, that:

- enforcement officials should make an assessment on whether the inclusion of the directors' name is genuinely necessary;
- they should not include personal data in the free-text field for "short summaries";

[16] Commission Recommendation of 1 March 2011 on Guidelines for the implementation of data protection rules in the Consumer Protection Cooperation System (CPCS) (2011/136/EU).
[17] With regard to the "directors" field, please see our specific recommendations in Section 1.5 above.

- they should assess whether to include personal data in the attached documents; if inclusion is not strictly necessary, personal data should be blackened out or removed[18]; and that
- the discussion forum should not serve to exchange case-related data and should not include personal data.

3.2.1. Deletion of erroneous data

The CPC Implementing Decision[19] requires competent authorities to request the Commission to delete erroneous data that cannot be corrected by other means.

The Commission explained to the EDPS that this provision is a "fall-back" solution for a small number of cases where there are no other more suitable mechanisms available to ensure correction or deletion of data. This is sometimes the case with "double entries" when a competent authority mistakenly uploads the same information twice, or in case the uploading authority incorrectly identified the legislative area (e.g. a directive) concerned. In most other situations, the competent authorities themselves are able to correct the data uploaded. For example, they may modify information on the seller or supplier concerned, or correct or delete the data in an attachment.

The EDPS has no objections against the "fall-back" solution described above. However, he emphasises that the system and its interfaces should be designed in such a way to minimise the need to resort to this fall-back option.

Further, the deletion must always be carried out in such a way that an appropriate audit trail should be available to evidence the operation that has been performed (see also Section 3.6).

3.2.2. Towards a data protection module (Privacy by Design)

As noted above, to facilitate the implementation of these recommendations in practice, the EDPS recommends that the CPCS system architecture should be built and configured in such a way to facilitate, to the greatest extent possible, compliance with data protection laws.

The EDPS welcomes that the system architecture already contains certain data protection-friendly features to enhance compliance with data protection requirements, such as a pop-up message informing the case handler uploading an attachment that no personal data should be included in the attachment unless strictly necessary or the general pop up message prompting competent authorities to assess data protection-related aspects before a mutual assistance request or an alert is formally "sent" via CPCS.

If experience shows that further guidance to case handlers is necessary, alternatives to the current pop-up features, or additional technical measures could be developed and form part of a specific "**data protection module**" within the CPCS system architecture. These may include the following "click-through" safeguards:

- when a competent authority fills in the directors' name field, the system could automatically show a warning message asking if the inclusion of this information is

[18] If it is subsequently found that this information is crucial for the purposes of the investigation or enforcement (for example, if it can serve as evidence), it can be requested in a subsequent communication.
[19] See Annex, point 2.1.5, as amended.

absolutely necessary for the case, also requesting specific justification for the inclusion;
- before uploading a short summary, a warning could appear requesting the user to confirm that no personal data has been included in the short summary (other than the trade name of the seller or supplier, if an individual);
- before un-clicking a confidentiality flag, a warning could appear describing clearly what the implication of this decision is; in particular, who will now have access to what information uploaded.

The system should also include guidance on data protection issues, such as those listed above, in the "Help menu" accessible from within the CPCS application.

A feature to enable feedback and communication among competent authorities and the Commission with regard to data protection compliance problems could also be considered, if the need arises. Using this feature, any recipient of information would have the means, through CPCS, to notify the competent authority uploading the information that there has been a data protection compliance problem with regard to the information uploaded. For instance, personal data have been included in the short summaries, or personal data irrelevant to the case has been included in an attachment. Such a feature could help minimise exchange of personal data and facilitate correction of inaccurate or out-dated information.[20]

As discussed further in Section 3.5, the data protection module could also include a coordination mechanism to process and take decisions concerning the fulfilment of data subject access requests.

3.2.3. Data protection training and awareness raising

As noted above, a high level of data protection in CPCS requires that system users should receive adequate guidance on how to apply data protection in practice when processing data in CPCS.

In this respect, the EDPS welcomes that the Commission has made efforts, in the CPC Data Protection Guidelines, via organization of workshops, contacting SLOs, and via other means, to raise awareness among case handlers highlighting, among others, the following data protection issues:

- case handlers should minimise the inclusion of personal data (that is, they should only include personal data when this is essential for the purpose of the information exchange);
- they should be aware that the company director field is optional and that they should carefully consider whether including this information in CPCS is strictly necessary [21];
- they should carefully consider whom the recipients of their messages will be and should only disseminate personal data on a need-to-know basis. This applies both with regard to communication to other competent authorities and within a given competent authority;
- they should close cases in a timely manner and request deletion of cases promptly thereafter;

[20] So long as the current "Questions and Answers" (chat) feature in the CPCS enables the competent authorities concerned by a given information exchange to discuss these issues within the CPCS system architecture, a specific communication channel may not be strictly necessary at this time.
[21] The EDPS welcomes the fact that the CPCS interface clearly marks with an asterisk all data fields which are mandatory; and that the director's field is not among these.

- they should be aware of the data subjects´ rights to information and access, and be familiar with the practice to accommodate access requests;
- they should comply with confidentiality and security measures. In this respect, each competent authority should also ensure that only correctly accredited officials have access to the CPCS and that once an official leaves his/her position the authorities should immediately inform the Commission so that the access granted to that user can be immediately revoked.

The EDPS also welcomes the fact that the CPC Data Protection Guidelines highlight the importance of training.

The EDPS emphasises that in order for the recommendations set forth in the CPC Data Protection Guidelines to become reality, they have to be complemented with adequate training plans. CPCS users should be equipped with a good knowledge of relevant data protection issues that they may come across when exchanging data in CPCS. The Commission's awareness raising activities play an important role.

3.3. Retention period

Article 6(e) of the Directive requires 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"*. Article 4(1) (e) of the Regulation contains an equivalent provision.

3.3.1. Facts, legal framework and state of play

There are three time periods that should be considered in the workflow of CPCS cases:

- retention period until case closure: this is the time period that begins the moment a case is initiated and ends when the case is closed in the system;
- retention period from closure to deletion: this is the time period that begins when a case is closed and ends when the information is finally deleted in the system;
- total retention period: this is the sum of the two other retention periods.

The CPC Regulation only provides specific rules for (i) unfounded alerts (which have to be deleted without delay) and for (ii) cases which resulted in successful enforcement (which have to be deleted five years after the closure of the case).

It provides no other specific rules when cases should be closed or information should be deleted from the database. However the lack of clarity may potentially lead to a situation that some cases would never be closed and would never be deleted, or would remain in the database longer than necessary. The Commission has therefore addressed this issue and has provided additional clarity in a number of ways.

Clarifications made in the CPC Implementing Decision

(i) The CPC Implementing Decision provided additional rules with respect to the different types of information flows:

- if an **information request** is "closed", because the information exchanged did not generate follow up actions (such as an enforcement request or alert) or it was established that no intra-Community infringement had taken place, and the competent

authority concerned declares that this is the case, the competent authority must, within seven days, notify the Commission (the Commission, in turn, must delete all related data stored in the database, within seven days of the notification). In all other cases[22], information requests are deleted five years following case closure;

- if an **alert** is founded it will be deleted five years as of the date when it was issued. When an alert proves to be unfounded, the competent authority must, within seven days, withdraw the alert (the Commission, in turn, must delete all related data stored in the database, within seven days of the withdrawal);

- when a **request for enforcement** is closed (following notification that the infringement has ceased), the case-related data are deleted five years after the case was closed;

- when an information request, an alert or an enforcement request contains **erroneous data** that cannot be corrected by other means, it should be deleted within 14 days (2 x 7, calculated as described above).

(ii) Awareness-raising in the CPC Data Protection Guidelines

In addition to the rules described in the CPC Implementing Decision, the CPC Data Protection Guidelines raise awareness about the importance of timely closure of cases.

(iii) Benchmarking in the CPCN Operating Guidelines

The CPCN Operating Guidelines, in point 2.7 under the title "phases and time-lines in a CPC case" discuss typical case flows and recommend that information requests, on average, should be handled within a period of 1 to 3 months, and enforcement requests within a period of 6 to 9 months (except in cases where the national procedure foresees a longer period, for instance in case of an appeal against an administrative decision where a year or more is more realistic).

(iv) Annual review of state of play

The Commission also carries out an annual review of state of play to encourage timely case closures. In particular, it prepares a list of cases, which also highlights cases that have been opened for a period substantially longer than the average case-handling period (benchmarking is against the timelines set in the CPCN Operating Guidelines, as noted above). These are then communicated to SLOs, who, in turn, are requested to contact the competent authorities concerned.[23]

(v) Periodic update of state of play between competent authorities concerned with a mutual assistance request

Finally, point 2.1.3 of the CPC Implementing Decision requires that the requested competent authority update the applicant competent authority on the investigative or enforcement actions it has taken to comply with the request on a regular basis as appropriate but at least every three months.

[22] Except for erroneous data, as noted below.

[23] The Commission also plans to include a "time-stamp" feature in the database to certify, at the time of the annual review, that the personal data uploaded in the database is still accurate. The EDPS welcomes this plan.

3.3.2. EDPS assessment and recommendations

As shown above, the Commission has made significant progress in clarifying the rules for data retention in CPCS. It has also taken steps to ensure that cases are closed in a timely manner.

(i) Timely case closures

With respect to case closures, considering the relatively low number of information exchanges that currently take place in CPCS (since 2007, 300 new cases were opened on average every year, including alerts), the EDPS notes that the measures described above could be considered sufficient to minimise the data protection concerns that may arise from the risks that a significant amount of outdated and/or unused personal data may remain in the database for long periods of time.

In case the measures described above prove to be insufficient to ensure timely case closures in the future (for reasons of an increased amount of information exchanges via CPCS or otherwise), the EDPS recommends that the Commission should consider additional measures. These may include, among others, automatic deletion of cases which remained inactive despite repeated warning messages.

(ii) Alerts

With respect to alerts, the EDPS is concerned that alerts will remain in the system for five years unless specifically declared "unfounded" and withdrawn by the issuing competent authority.

As it will be further discussed in the EDPS Opinion on the new measures adopted by the Commission for the application of the CPC Regulation, considering the risks of retaining data regarding unconfirmed suspicions for a long period of time, the EDPS recommends that all alerts should be deleted within shorter time-frames. This should be the case at least in cases where they do not generate further follow-up action, via CPCS or otherwise. In his Opinion on the new measures adopted by the Commission, the EDPS recommends that alerts should be deleted at the latest within six months following their upload (unless another, more appropriate retention period can be justified).

(iii) Retention period for closed mutual assistance requests

The "standard" retention time applied in CPCS following case closure (subject to specific exceptions) appears to be five years both for information requests and enforcement requests.

Neither the CPC Regulation nor the CPC Implementing Decision explains the purpose of or necessity for the retention of data for such a long period of time. To provide some explanation, the CPC Data Protection Guidelines note that "*during the retention period authorised enforcement officials working for the competent authority that originally dealt with a case may consult the file in order to establish links with possibly repeated infringements which contributes to a better and more efficient enforcement*"[24].

[24] The CPC Data Protection Guidelines also add that "*the purpose of the retention period is to facilitate cooperation between public authorities responsible for the enforcement of the laws that protect consumers' interests in dealing with intra-Community infringements, to contribute to the smooth functioning of the internal market, the quality and consistency of enforcement of the laws that protect the consumers' interest, the*

In this regard, the EDPS recommends that the Commission should:

- clarify further what is the purpose of the five-year data retention;
- evaluate whether a shorter retention period would achieve the same objectives; and
- evaluate whether all information currently foreseen needs to be retained or whether a subset of that information would suffice (e.g. it should be considered whether retaining Article 8.6 notifications only would be sufficient; it should also be specifically evaluated whether retaining the directors' names or attachments that may contain additional personal data are necessary; a distinction should also be made between data relating to suspected infringements and "proven" infringements).

Additional recommendations and considerations regarding the retention period are provided in the EDPS Opinion commenting on the new measures adopted by the Commission for the application of the CPC Regulation. As above mentioned, the two sets of comments are complementary and therefore, should be considered jointly.

3.4. Information to be given to the data subject

Competent authorities are obliged under Articles 10 and 11 of the Directive to provide data subjects with certain information on processing, without being specifically requested by the data subjects.[25] Corresponding provisions of the Regulation (Articles 11 and 12) establish similar requirements for the Commission with respect to personal data it processes. The CPC Data Protection Guidelines recommend a "layered" approach to notice provision. According to this approach:

- the Commission should provide on its EUROPA webpage dedicated to the CPCS a comprehensive privacy notice where the workings of the CPCS as well as the data protection safeguards applied within the CPCS are explained in clear and simple language; this should also include, but should not be limited to, a data protection notice under the Regulation regarding the Commission's own responsibilities;
- competent authorities (individually or via their SLOs) should also provide data protection notices, e.g. on their webpages, with content as required under their respective national data protection laws. This information should include a link to the Commission's webpage containing its data protection notice but should also give further details including contact information for the competent authority concerned as well as any national restrictions on the right of access or information.

The Commission has also prepared and provided to the EDPS a draft data protection notice.

The EDPS welcomes the provisions set forth in the CPC Data Protection Guidelines as well as the preparation of a user-friendly and informative draft data protection notice. At the same time, he also calls for further measures to ensure that data subjects are effectively informed about the processing of their personal data.

First, with respect to the draft data protection notice, the EDPS recommends the following:

- Section 3.1 of the draft (Data processed by the network authorities) should be amended in light of Section 1.3 of this Opinion, to more comprehensively describe the

monitoring of the protection of consumers economic interests and to contribute to raising the standard and consistency of enforcement".

[25] Unless some of the exceptions mentioned in Article 13 of the Directive apply.

types of personal data processed, which are not limited to directors' names and information in attached documents;

- Section 5.2 (Competent controller for data stored and processed by the Commission) should be amended in light of Section 1.4 of this Opinion, to more accurately describe the roles and responsibilities of the Commission, which extend beyond processing contact information for case handlers and includes, for example, the Commission's responsibility as the operator of the system;
- Section 9.2 (Recourse), bullet-point two, should be amended so as not to suggest that complaints should also be filed to the EDPS against activities carried out by the competent authorities and SLOs. These complaints should be handled by the competent data protection authorities in Member States;
- further changes in the draft may also be necessary to reflect the additional safeguards provided elsewhere in this Opinion (e.g. regarding retention periods and the procedure for rights of access to data subjects);
- once a revised draft has been prepared, the Commission should post its data protection notice on its website at a prominent location and in such a manner that it can be easily found by data subjects (normally at the top of the home screen).

Second, the EDPS recommends that the Commission should play, to the extent feasible, in its capacity as the operator of CPCS, a proactive role in raising awareness about the importance of notice provision among competent authorities (or SLOs) to help encourage notice provision at national level.

The EDPS particularly welcomes and encourages workshops and similar initiatives, which have been held in the past. It is also good practice to make the links to national/local data protection notices available on the Commission's CPCS website (and to link local notices, in turn, to the Commission's notice). In this respect, the EDPS also emphasises the importance of the coordinative role that SLOs may play in providing notice in each Member State.

Finally, the EDPS emphasises that while providing information via the internet is crucial, this information, unless directly brought to the attention of the data subjects concerned, cannot entirely substitute for a notice provided directly to the data subjects.

Therefore, the Commission should raise awareness, to the extent practicable, among competent authorities, about best practices for direct notice provision. For example, an opportunity to provide notice may be at the stage during the investigation when the investigating authority informs the representatives of a suspected business that they are being investigated. On this occasion, the suspect could also be told that personal data may be exchanged via CPCS and a link to an online data protection notice (or a copy of the notice) could be provided.

3.5. Rights of the data subject

Article 12 of the Directive and the corresponding Article 13 of the Regulation require controllers to provide access to data subjects, upon request, to their personal data, to correct errors, and to delete data under certain circumstances. Under Article 13 of the Directive and Article 20 of the Regulation, certain exceptions may apply.

3.5.1. Restrictions on rights of access

The existence of this right - and any potential exceptions - may have important implications. Importantly, under the general rules, the data subject has the right to know if his/her business

activity has been reported as a suspected infringement. The use of this right, however, could - depending on the circumstances - interfere with an on-going investigation.

Under Article 13(4) of the CPC Regulation, Member States shall adopt legislative measures that, pending an investigation, could restrict - among others - the access rights of the data subjects (in compliance with the Directive). The Commission may also apply specific restrictions (in compliance with the Regulation).

On the basis of the foregoing, when deciding upon an access request, a competent authority will apply its own national law (which should be in compliance with the Directive). Considering that there are at least two participants to each information exchange in CPCS, and in the absence of complete harmonisation of national laws and procedures on data protection and on consumer legislation and its enforcement, it is possible that one authority would allow access to the data subject to his/her personal data whilst the other would restrict access to the same data.

To minimise the potential conflicts and inconsistencies that may arise in such a situation, a coordinated approach is desirable: coordination should ensure that, on one hand, the rights of the data subjects are fully respected, and on the other hand, that appropriate exceptions deriving from national legislation are taken into account when relevant, and legitimate needs to restrict access are observed. This is not only important for data protection, but also helps ensure that competent authorities in different Member States will have trust that their legitimate needs to restrict information are respected when data they provided are transferred to another Member State.

In the absence of (or while awaiting) further harmonisation, the EDPS welcomes the fact that the CPC Data Protection Guidelines seek to provide clarifications and encourage a coordinated approach.

The EDPS, in particular, welcomes that the Guidelines recommend that granting the request of a data subject should be carried out only after consulting those authorities whose investigations may be compromised by access provision.

The EDPS also recommends taking a nuanced approach. In particular, rather than seeking a formal approval from the other authorities concerned, the competent authority which is deciding on the access request should take into account in its decision-making (to the extent appropriate under its own national law) the fact that providing access may jeopardise the investigation carried out by another competent authority in another Member State.

At the same time, the EDPS would also emphasise that careful consideration of the impact on investigations carried out in other Member States (the "prudence" principle as suggested by the Commission) should not lead to a "race to the bottom" with regard to data protection and to accommodating the laws of the Member State with the most restrictive regime regarding access rights.

In view of the above, the EDPS recommends that the Commission should:

- adopt its own rules on how it applies any restrictions on access requests that are addressed to it;
- follow-up with Member States to gather information about how restrictions are applied in the Member States;

- help ensure, to the extent possible, a coordinated approach along the lines described above; and
- help communicate the results of this exercise, among competent authorities and towards data subjects.

3.5.2. Procedure allowing data subjects to exercise their rights

In addition to clarification whether any exceptions are available, it is also crucial to ensure that data subjects can exercise their rights in an easily available, simple way.

Considering the number of controllers (Commission, SLOs, various competent authorities), the fact that each may have access to different sets of personal data stored in CPCS, and the multiplicity of national data protection laws that may apply, the allocation of responsibilities for enabling data subjects to exercise their rights of access is particularly complex. This is all the more true as provision of access by a CPCS user in one Member State may have an effect on the confidentiality of investigations in another Member State, as shown above. Therefore, access provision may require collaboration between different parties.

In practice, a data subject may wish to request access, rectification and deletion of their personal data from any of several sources:

- from the competent authority which uploaded the data;
- from another competent authority with access to the information;
- from the Commission.

It is also possible that a data subject may request access from a controller which has no access at all to the requested information (for example, because an alert was not sent to it or it was not involved in a coordinated investigation).

The CPC Data Protection Guidelines specify that the Commission may only grant a request for data to which the Commission (i.e. the CPCS users at the Commission) has access (In most cases this is limited to alerts and notifications; see Section 1.4).

The EDPS welcomes the clarifications in the Guidelines. With that said, further clarifications would be necessary. In particular, the process for implementing the exercise of access rights should be further defined in practical terms to ensure that data subjects' requests will be fulfilled in an effective way, in a simple, foreseeable and timely-manner, and with the least amount of administrative burden and difficulty posed either for the controllers involved or for the data subjects.

The procedure should also be transparently described in a data protection notice easily available to data subjects. It must be made very clear to whom data subjects should submit their requests, who will be deciding on the request, and based on what applicable law.

Finally, as a matter of practicality, the coordination should also ensure, whenever possible, that data subjects do not need to submit a separate request to all competent authorities using CPCS who might have access to their personal data. Considering that currently there are over three hundred competent authorities registered in CPCS, this may pose an excessive burden to the exercise of a fundamental right.

To minimise the administrative burden and ensure smooth cooperation, the EDPS recommends that coordination should be supported by an IT tool, which may form part of the

data protection module referred to in Section 3.2.2. This functionality, in particular, could be used to handle and route access requests in cases where giving access to the data may have an effect on two or more competent authorities' investigations. In addition, it can also help to route requests to other relevant competent authorities in case the competent authority that was contacted by the data subject does not have access to all data relating to him/her in CPCS. This functionality may become particularly useful if the use of CPCS increases and the number of access requests grow.

That being said, the EDPS does not exclude other methods of coordination (without the use of an IT tool), so long as the procedure laid down provides a workable solution for data subjects to exercise their rights. Integration of functionality in the CPCS application may then be considered as a second step if a need arises for more efficient coordination. To ensure that, if and when the need arises, further developments are implemented, the EDPS recommends that the Commission should keep statistics on the number of access requests submitted to the competent authorities with regard to data exchanged via CPCS. This should also include the length of time required to fulfil the requests.

3.6. Confidentiality and security of processing

[...]

4. Conclusions

The EDPS welcomes the fact that CPCS is grounded on a legal basis such as the CPC Regulation and that this legislative text has been complemented over time with the CPC Implementing Decision and the CPC Data Protection Guidelines, which provide more details with regard to the processing as well as specific data protection safeguards. The EDPS also acknowledges the work done at the practical level, with regard to the security and functionalities of CPCS.

On the whole, the EDPS finds no reason to believe that there is any breach of the Regulation, provided that the recommendations in this Opinion are implemented, namely:

- concerning data quality, (i) the CPCS system architecture should continue to be configured in such a way to facilitate, to the greatest extent possible, compliance with data protection laws; and (ii) the Commission should continue its activities to help ensure that the users of the system should be adequately trained, guided, and empowered to take decisions concerning data protection;
- with regard to the retention period, (i) unless an investigation or enforcement action is ongoing, alerts should be withdrawn and deleted within an appropriate time period from their issuance (the EDPS recommends a period of six months unless another, more appropriate retention period can be justified); the Commission should: (ii) clarify further what is the purpose of the five-year data retention period; (iii) evaluate whether a shorter retention period would allow achieving the same objectives; and (iv) evaluate whether all information currently foreseen needs to be retained or a subset of the information would suffice;
- the Commission should revise and make prominent its draft privacy notice on the website and raise awareness about the importance of notice provision among competent authorities (or SLOs) to help encourage notice provision at national level;

- further measures should be taken to facilitate the exercise of data subjects' rights to access, rectification and deletion of their data. To facilitate coordination, a data protection module within the CPCS could be considered;
- *[...]*.

Done in Brussels, 4 May 2011

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor

[signed]