Opinion of the European Data Protection Supervisor

on Commission Decision 2011/141/EU amending Commission Decision 2007/76/EC on the Consumer Protection Cooperation System ("CPCS") and on Commission Recommendation 2011/136/EU on guidelines for the implementation of data protection rules in the CPCS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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[1],

Having regard to the request for an opinion in accordance with Article 28(2) of 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[2],

[1] OJ 1995, L 281/31.
[2] OJ 2001, L 8/1.

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

HAS ADOPTED THE FOLLOWING OPINION:

I. Introduction

1. On 1 March 2011, the European Commission adopted a Commission decision amending Commission Decision 2007/76/EC on the CPCS ("Second CPC Amendment")[3]. On the same date, the Commission also adopted a Commission Recommendation on guidelines for the implementation of data protection rules in the CPCS ("CPC Data Protection Guidelines")[4]. Both documents were sent to the EDPS for consultation in accordance with Article 28(2) of Regulation (EC) No 45/2001.

2. 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"). CPCS facilitates co-operation among "competent authorities" in EU Member States and the Commission in the area of consumer protection, with regard to infringements of a pre-defined set of EU directives and regulations. To come under the scope of the CPC Regulation infringements must be of cross-border nature and must harm the "collective interests of consumers".

3. In the framework of their co-operation, CPCS users exchange information, including personal data. These personal data may relate to directors or employees of a seller or supplier suspected of an infringement, the seller or supplier itself (if an individual), as well as to third parties such as consumers or complainants.

4. The system is designed to be a secure communication tool among competent authorities as well as a database. CPCS is used by the competent authorities to request information to help investigate a case[5] or to request assistance with enforcement[6] ("mutual assistance requests"). In addition, competent authorities can also send a warning message ("alert") to inform other competent authorities and the Commission about an infringement or a suspected infringement[7]. CPCS also contains further functionalities including a notification system[8] and a forum to exchange non-case-related data.

5. In this Opinion, the EDPS addresses a number of data protection issues concerning the legal framework for the CPCS, focusing primarily on the newly adopted Second CPC Amendment. In addition, the EDPS also takes stock of the progress made thus far and selectively highlights some remaining concerns and considerations for the future. He also comments on some provisions of the CPC Data Protection Guidelines.

---

[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 mutual assistance (2011/141/EU).

[4] Commission Recommendation of 1 March 2011; Guidelines for the implementation of data protection rules in the Consumer Protection Cooperation System (CPCS) (2011/136/EU).

[5] See Article 6 of the CPC Regulation on "exchange of information on request".

[6] See Article 8 of the CPC Regulation on "request for enforcement measures".

[7] See Article 7 of the CPC Regulation on "exchange of information without request" (or "alert" for short).

[8] See Articles 7(2) and 8(6)) of the CPC Regulation.

6. In parallel with this Opinion (which is adopted pursuant to Article 28(2) of Regulation 45/2001), the EDPS is also issuing a prior checking Opinion in his supervisory capacity (pursuant to Article 27 of the same Regulation) ("Prior Checking Opinion"). The Prior Checking Opinion contains a more detailed description of CPCS as well as the processing of personal data in it. In the Prior Checking Opinion, the EDPS focuses on recommendations for specific measures to be taken at the practical, technical, and organisational level to improve data protection compliance in CPCS. Considering that the CPC Data Protection Guidelines are also closely related to these specific measures, the Prior Checking Opinion also comments on selected provisions of the Guidelines.

II. Legal framework for the CPCS

7. The EDPS is pleased that the CPCS is based on a solid legal basis, in particular, a Regulation adopted by the Council and the Parliament. In addition, the EDPS is satisfied that the legal basis has been complemented over time to provide further details and address data protection concerns. In particular, the EDPS is pleased that Commission Decision 2007/76/EC of 22 December 2006 implementing the CPC Regulation ("CPC Implementing Decision") was adopted and subsequently further amended on 17 March 2008 and recently, on 1 March 2011 via the Second CPC Amendment. He also is pleased that the Commission adopted the CPC Data Protection Guidelines, specifically addressing data protection issues.

8. Although the EDPS regrets that he was not consulted at the time the CPC Regulation and the CPC Implementing Decision were initially adopted, he is pleased that the Commission consulted him on the occasion of the adoption of each of the two amendments to the CPC Implementing Decision as well as with regard to the CPC Data Protection Guidelines. The EDPS also is pleased that the Commission, previously, also consulted the Article 29 Data Protection Working Party ("WP29"), which issued, on 21 September 2007, its Opinion 6/2007 (WP 139). Finally, the EDPS welcomes the fact that reference to these consultations is made in the recitals of the CPC Data Protection Guidelines.

9. The EDPS notes that (i) the Commission has carefully considered the EDPS recommendations given in previous informal exchanges as well as those of the WP29 expressed in Opinion 6/2007 and that (ii) many of these recommendations were followed when further developing the legislative framework for the CPCS and/or at the practical, technical, and organisational level. His comments in this Opinion as well as in his Prior Checking Opinion should be considered against this positive background.

III. Data protection issues with respect to the Second CPC Amendment

3.1 Retention of personal data in CPCS

3.1.1 Introduction

10. As a preliminary remark, the EDPS points out that the issue of case closures and retention periods has not been adequately and comprehensively addressed in the CPC Regulation.[9]

[9] See also Opinion 6/2007 of the Article 29 Data Protection Working Party (referred to in Part II above).

11. Indeed, the CPC Regulation only lays down two specific rules regarding deletion of data and provides none with respect to case closures.[10] First, it requires that if an alert "proves to be unfounded", the competent authority should withdraw it, and the Commission should without delay remove the information from the database. Second, it requires that when a competent authority notifies, under Article 8(6) of the CPC Regulation, that an infringement has ceased, the stored data should be deleted five years after the notification.

12. The CPC Regulation does not establish the purpose of the five-year retention period. Neither does it provide any further specifications on how and when it should be assessed whether an alert is "unfounded". In addition, the CPC Regulation is also silent on how long information should remain in the database in cases not covered by the two specific rules just mentioned (e.g. the Regulation does not specify how long mutual assistance requests are retained in the database if they have not led to successful enforcement action which would have stopped the infringement).

13. The EDPS is pleased that the CPC Implementing Decision, as amended, and the CPC Data Protection Guidelines attempt to provide further clarifications. That being said, the EDPS remains concerned about several aspects of the rules for case closures and data retention in the CPCS, as discussed below in Sections 3.1.2 to 3.1.4.

14. The EDPS recommends that these concerns be addressed at the next revision of the legal framework for the CPCS, via a further amendment of the CPC Implementing Decision, or, preferably, via an amendment to the CPC Regulation itself.

15. Until such time as such legislative action will be possible, the EDPS recommends that the concerns regarding retention periods be addressed at the practical, technical, and organisation level and also be clearly set forth in the "Consumer Protection Cooperation Network: Operating Guidelines" referred to in Section 3.1.2 below.

3.1.2 Timely case closures

16. The Second CPC Amendment fails to set a final date by which a case involving a mutual assistance request (information request or enforcement request) must be closed.

17. In the Prior Checking Opinion the EDPS takes note of a number of pragmatic measures that the Commission is currently taking to help ensure that dormant cases are closed in a timely manner.

18. In this Opinion, the EDPS recommends that maximum timeframes should be established for requests for information and requests for enforcement. These should be specified in the legislative framework when it will be reviewed next. The timeframes should be linked to the type of case as well as to actual activity. At the same time, the rules should also provide flexibility to the competent authorities to extend the case for good reason, to ensure that cases are not closed prematurely even if a complex case takes longer than average to close.

19. To do this, the EDPS recommends using as point of departure the document entitled the "Consumer Protection Cooperation Network: Operating Guidelines" endorsed by the CPC Committee on 6 December 2010. The Operating Guidelines, in point 2.7 under the

[10] See Article 10(2) of the CPC Regulation.

title "*phases and time-lines in a CPC case*", discuss typical case flows and provide that information requests, on average, should be handled within a period of one to three months. Handling enforcement requests, according to the Operating Guidelines, should be feasible within a period of six to nine months on average (except in case of injunctions or in case of an appeal against an administrative decision where a year or more is more realistic).

3.1.3 Alerts

20. The Second CPC Amendment introduced a new paragraph to point 2.2.2 of the Annex to the CPC Implementing Decision to require that "founded" alerts should be removed from the database five years after they are issued (as for "unfounded" alerts, the existing provisions already required deletion once "*an alert proves to be unfounded*").

21. To put this new provision into context, the EDPS emphasises that one of his key concerns is to ensure that personal data do not remain in the CPCS database longer than necessary. This is a sensitive issue in particular with respect to alerts (which have a larger number of recipients than bilateral exchanges), and among alerts, in particular with respect to those regarding suspected infringements. In practice, the lack of a clear time-limit for keeping the alert open would mean that some alerts could remain outstanding for an unduly long period of time (so long as they are not clearly proved to be unfounded). Such actions based on unconfirmed suspicions would pose significant risks to the fundamental right of data protection, as well as to other fundamental rights such as the presumption of innocence.

22. Against this background, the EDPS is pleased that a retention period has been established for alerts. However, the EDPS considers that the Commission has not provided adequate justification to show that a five-year retention period would be proportionate. The EDPS recommends that the Commission carries out a proportionality assessment and reassesses the length of the retention period for alerts. In principle, all reported alerts should be deleted from the database much earlier, unless an alert on an infringement or a suspected infringement has led to a mutual assistance request and the cross-border investigation or enforcement action is still ongoing. The retention period should be long enough to allow each authority who receives the message to establish whether it wishes to take further investigative steps or enforcement action, and whether it wishes to send a mutual assistance request via CPCS; however, it should be sufficiently short to minimise the risks that alerts could be misused for blacklisting or data mining.

23. In this perspective, the EDPS recommends that the Commission should revise the legal framework to ensure that alerts should be deleted at the latest six months following their upload, unless another, more appropriate retention period can be justified.

24. This should help ensure, in particular, that in cases where the suspicion has not been confirmed (or even investigated further), innocent individuals linked to the suspicion would not be kept on a "black-list" and "under suspicion" for an unduly long period of time, which would not be in conformity with Article 6(e) of Directive 95/46/EC.

25. This limitation is also necessary to ensure the principle of data quality (see Article 6(d) of Directive 95/46/EC) as well as other important legal principles. This may not only result in a more adequate level of protection for the individuals, but at the same time, should also allow enforcement officials to more effectively focus on relevant cases.

3.1.4 Retention period for closed mutual assistance requests

26. The Second CPC Amendment added a new paragraph to point 2.15 of the Annex of the CPC Implementing Decision to require that *"[a]ll other information relating to requests for mutual assistance pursuant to Article 6 of [the CPC Regulation] shall be removed from the database five years after the closure of the case".*

27. Read together with the existing text, the revised point 2.15 requires retention for five years after case closure of all information exchanges under Article 6 except:

- where erroneous data were deleted,
- where the information exchange did not generate an alert or an enforcement request, or
- where it was established that no infringement has taken place in the meaning of the CPC Regulation.

28. Indeed, as explained in the Prior Checking Opinion, 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.

29. The text of the CPC Implementing Decision as amended by the Second CPC Amendment, does not appear to be fully consistent with the CPC Regulation. In particular, Article 10(2) of the CPC Regulation makes a distinction between, on one hand, information exchanged that leads to successful enforcement (i.e. cases where the infringement has ceased as a result of the enforcement actions taken), and, on the other hand, information that has not lead to successful enforcement. For the former, a five-year retention period is foreseen once the case has been closed. For the latter, no specific provisions are set forth (except that unfounded alerts should be withdrawn and deleted).

30. In other words, the CPC Regulation requires a five year retention period after case closure only on condition that enforcement actions were taken and they have been successful to make infringement cease.

31. Although the EDPS has doubts regarding the purpose and proportionality of retention of any data for five years until after the case is closed (see his comments further in this Section 3.1.4), the distinction between cases that ended with successful enforcement and cases that did not has some logic from the data protection point of view. In particular, retention of data regarding mere suspicions for a long period of time has a higher potential to be inaccurate, and also risks violating other important legal principles. Therefore, it can be said, in general, that retention of such data for a long period of time is more likely to raise data protection issues than retention of data regarding actual wrongdoings, which have been adequately proven and resulted in enforcement action.

32. Contrary to the CPC Regulation, the CPC Implementing Decision, as amended, appears to allow, at least in some cases, the five-year retention period to apply also to information that did not lead to successful enforcement actions.

33. For instance, according to the CPC Implementing Decision, an information request that led to an alert but did not lead to enforcement action appears to stay in the system for five years as of the "closure of the case".

34. The CPC Regulation and the CPC Implementing Decision, thus, each appears to follow a somewhat different approach. The CPC Implementing Decision, whilst mirroring, to some extent, the provisions of the CPC Regulation, also introduces important additional rules for retention. While clarification of the rules, in itself, is welcome, the EDPS questions the lawfulness of establishing longer retention periods where this was not already required in the CPC Regulation. This would impose further restrictions on the fundamental right to data protection, and would do so in implementing legislation, contrary to the CPC Regulation and applicable data protection laws.

35. In accordance with the foregoing, the EDPS recommends that the Commission should review the legal framework and reconsider whether the five year retention period should apply to any other cases beyond those where a successful enforcement has taken place as it is specified in the CPC Regulation.

36. Further, the EDPS is pleased that the CPC Data Protection Guidelines aim to specify the purpose of the retention after case closure, an important issue that both the CPC Regulation and the Second CPC Amendment failed to address. In particular, the CPC Data Protection Guidelines provide 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*".[11]

37. However, whilst this clarification is welcome, in the absence of further justification of the necessity of this access, the EDPS is not convinced of the proportionality and sufficiency of this purpose to justify the five-year retention period. Therefore, 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 allow achieving the same objectives; and
- evaluate whether all information currently foreseen needs to be retained or a subset of the 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).

3.2 The Commission's access to data in CPCS

38. The EDPS is pleased that (by introducing a new point 4.3 to the Annex of the CPC Implementing Decision) the Second CPC Amendment clarifies the Commission's access to data in CPCS and that such an access is clearly and specifically limited to what is required under the CPC Regulation. In particular, the EDPS is pleased that the Commission has not been given access to confidential communications among competent authorities in Member States, such as mutual assistance requests.

[11] See Section 8 of the Guidelines, "*Some additional guidance; Why is the data retention period set at 5 years?*" 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 monitoring of the protection of consumers economic interests and to contribute to raising the standard and consistency of enforcement*".

39. This clarification and limitation is particularly important, considering that lack of clarity might have led to a situation where the Commission would have been able to access information, including personal data, which are destined solely for competent authorities in Member States.

40. As described in Section 5 of the CPC Data Protection Guidelines, "*the purpose of the Commission's access is to monitor the application of the CPC Regulation as well as the consumer protection legislation listed in the Annex to the CPC Regulation and to compile statistical information in connection with carrying out these duties*".

41. This does not mean that the Commission should have access to any and all data exchanged among Member States within CPCS.

42. Indeed, the EDPS emphasises that access to databases such as CPCS falls within the definition of processing personal data. Under Article 5(a) of Regulation 45/2001, which is relevant to the Commission's access rights in the CPCS, institutions may only process personal data if this is necessary for the performance of a task in the public interest, and further provided that the processing is based on the Treaties or secondary legislation.

43. The EDPS understands these requirements -which follow directly from the right to data protection as enshrined in Article 8 of the European Convention of Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union- to mean that the Commission can only have power to access the information systems of Member States if this is laid down in specific legal provisions, founded on a fully adequate legal basis (normally the ordinary legislative procedure). Legal certainty and transparency are the two underlying values which explain why a specific and secure legal basis for the Commission's access is a particularly important guarantee of ensuring the fundamental rights of individuals with respect to data protection.

44. Neither the Commission's general monitoring power as "guardian of the Treaty" nor the obligation of Member States to ensure loyal cooperation is sufficiently precise to give the Commission access to databases containing personal data. Loyal cooperation entails that Member States should -under certain conditions- provide the Commission with information when asked to do so or when they are required to provide information under a specific rule. However, it does not entail that the Commission should have access to their databases.

45. In this context, the EDPS also emphasises that the CPC Regulation excludes the possibility for the Commission's access to the information contained in mutual assistance and enforcement requests. Article 6 and Article 8 of the CPC Regulation designate only the requested authority, and not the Commission, as recipients of these data.

3.3 Special categories of data in CPCS

46. The EDPS is pleased that the Second CPC Amendment introduced, in point 4.4 of the Annex to the CPC Implementing Decision, a provision to address the processing of special categories of data in CPCS. The EDPS particularly is pleased that the provision limits such processing to cases where the fulfilment of the obligations under the CPC Regulation would be "*otherwise impossible*" and that processing of such data is subject to the further condition that the processing should be "*permitted under Directive 95/46/EC*".

IV. Privacy by design and accountability

47. After discussing, in Part III, the specific issues raised by the Second CPC Amendment, the EDPS, in Parts IV to VI, wishes to call the Commission's attention to a few other points that should be considered for the further development of the legal framework for the CPCS.

4.1 Privacy by design

48. The EDPS has been encouraging the Commission and other EU institutions for some time to adopt technological and organisational measures integrating data protection and security as a fundamental part of the design and implementation of their information systems ("privacy by design")[12].

49. Although he welcomes and recognises that some measures have been taken in this direction, the EDPS recommends that the Commission should make a comprehensive assessment what further privacy by design safeguards could be incorporated into the CPCS system architecture. Among others, the following should be considered and implemented as necessary:

- privacy by design solutions to guide system users to take "adequate" data protection decisions (see Section 3.2 of the Prior Checking Opinion);
- measures to facilitate timely closure and deletion of cases (*idem*, Section 3.3);
- procedures to facilitate information and access rights of data subjects (*idem*, Section 3.5);
- clear procedures for any modification carried out directly at database level, logging access, the rationale of the action and the approval at adequate level (*idem*, Section 3.6); and
- "encrypted" storage of information in the database so that IT operators cannot access it (at least for some of the data such as confidential attachments) (*idem*, Section 3.6).

4.2 Accountability

50. Further, in accordance with the principle of "**accountability**"[13], the EDPS also recommends the establishment of a clear framework for accountability that ensures data protection compliance and provides evidence thereof, such as:

- adopting and updating, as necessary, a data protection policy to be approved at the highest level of management within DG SANCO. This data protection policy should also include a security plan (see Section 3.6 of the Prior Checking Opinion)[14];

[12] See Section 7 of the EDPS Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union" issued on 14 January 2011 (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

[13] *Idem*.

[14] The Commission should also consider, as necessary, carrying out at least a partial data protection and privacy impact assessment focusing on the purpose, length and modalities of the retention period and possibly, discuss other outstanding issues that have not yet been comprehensively addressed.

- carrying out periodic audits to assess continued adequacy of and compliance with the data protection policy (including auditing the security plan, *idem*, Section 3.6);
- making public (at least partially) the results of these audits to reassure stakeholders with respect to data protection compliance; and
- notifying data breaches and other security incidents to the Commission DPO, affected data subjects (and other stakeholders and authorities when relevant).[15]

V. Transfer of personal data beyond the European Union

5.1 Bilateral arrangements

51. 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 that (i) the competent authority that originally communicated the information has given its consent and that (ii) the transfer is in accordance with applicable EU data protection law.

52. Articles 25 and 26 of Directive 95/46/EC subject transfers to third countries to certain additional conditions. These conditions are aimed at ensuring that the data will be adequately protected abroad. In addition, they also provide for a number of exceptions. Implementation and interpretation of these provisions of Directive 95/46/EC may differ from one Member State to another.

53. In light of the above, the EDPS can accept the safeguards included in the CPC Regulation, namely, that any third country transfer is subject to both (i) the consent of the competent authority that originally communicated the information and (ii) applicable EU data protection law.

54. The EDPS also is pleased that the CPC Data Protection Guidelines recommend that -unless the third country ensures an adequate level of protection- any bilateral assistance agreement should provide for adequate data protection safeguards and -where this is required- the agreement should also be notified to the relevant data protection supervisory authorities.

55. That being said, the arrangements laid down in the CPC Regulation are not ideal. Their application is complex: a competent authority deciding whether to transfer information to a third country would need to take into account not only its own country's bilateral arrangement with the third country, its own country's data protection laws, and its own assessment of the adequacy of the data transfer to the third country in question based on its own country's data protection laws, but would also need to take into account whether or not the other competent authorities involved that contributed to the file (and there may be several of them) have given their consent, based on their own data protection laws.

56. From the data protection point of view, this complexity leads to uncertainties as to the rights of the data subject, and in particular, uncertainties whether and on what conditions his or her data are transferred abroad. Data subjects are also not benefitting, to the fullest extent possible, from a solid and harmonised European data protection law. In addition, from the point of view of the competent authorities, this complexity is also likely to hinder cooperation among competent authorities, and poses an administrative burden.

[15] See Section 6.3 of the EDPS Opinion of 14 January 2011 referred above.

57. In light of the above, the EDPS encourages the conclusion of EU-wide agreements that provide for adequate data protection safeguards while at the same time also help avoid the application of heterogeneous criteria and the resulting increased administrative burden on competent authorities.

5.2 EU-wide agreements

58. In addition to the possibility foreseen in Article 14 for bilateral cooperation, Article 18 of the CPC Regulation on international agreements also provides that the "*Community shall cooperate with third countries and with the competent international organisations"* and that *"the arrangements for cooperation, including the establishment of mutual assistance arrangements, may be the subject of agreements between the Community and the third countries concerned*".

59. For the reasons set forth in Section 5.1 above, the EDPS supports the Commission in its initiative to negotiate and conclude EU-wide agreements, with adequate data protection safeguards, harmonised at the EU level, to replace the existing bilateral arrangements.

60. His support for such EU-wide agreements, however, is conditional upon the commitment of the Commission and EU legislators to ensure the highest level of protection for the personal data exchanges with third countries. The implications of international cooperation agreements with third countries must be carefully considered from the data protection point of view, clear rules must be established to govern these exchanges and adequate data protection safeguards must be provided, on a basis of a consultation of the EDPS and, where appropriate, of national data protection authorities.

61. Although Article 18 of the CPC Regulation does not specifically address the issue of direct access to the CPCS by third country authorities, this may be technically possible. The EDPS does not wish to discourage that new functionalities would be included in the CPCS to allow competent authorities in third countries strictly limited and selective access via a specifically designed mechanism (communication channel and interface). This could indeed increase the efficiency of the cooperation.

62. With that said, such a direct access has its own risks and therefore, its data protection implications and the necessary technical/organisational arrangements and safeguards must be specifically addressed. Any such technical functionality should be built using "privacy by design" principles. Security should also be a clear priority. Finally, the EDPS should be consulted, as well as, where appropriate, national data protection authorities.

VI. "Consumer data protection rights" and reinforced cooperation, via the CPCS, of data protection authorities

63. Provided that the EDPS recommendations (including also those in his Prior Checking Opinion) are followed, the EDPS is confident that CPCS can be an effective and data-protection-friendly tool for cross-border enforcement against infringements of rights of the consumers in the internal market.

64. With the development of electronic commerce and the growing use of electronic communications networks by consumers of various products and services, more and more individuals' data will be processed when they are acting as consumers. Consumers

may, thus, also increasingly face infringements of their rights with respect to data protection. Consequently, there is also a need for data protection authorities to effectively cooperate to stop such infringements.

65. Among the most common cases of a breach of "consumer data protection rights" are unsolicited commercial communications (spam), identity theft, illegal profiling, unlawful behavioural advertising and data breaches (security breaches).

66. Given that the number of cases of a cross-border nature is likely to increase in the information society, the EDPS encourages the Commission to consider possible legislative measures to protect "consumer data protection rights", and to reinforce trans-border cooperation among competent authorities: data protection as well as consumer protection authorities.

67. In particular, and while also considering other possible options, it should be carefully considered whether to allow data protection authorities tailor-made access to CPCS, in order to cooperate among themselves as well as with other competent authorities which already have access to CPCS.

68. Access by data protection authorities should be clearly limited to what is necessary to carry out their tasks within their areas of competence and according to the synergies identified. Of course, it should also be ensured that the framework for the participation of data protection authorities should be designed to take due account of their independence.

VII. Conclusions

69. The EDPS is pleased that CPCS is founded on a legal basis, which also provides specific data protection safeguards. To address any remaining data protection concerns, the EDPS notes that the recommendations summarised below should be considered when the legal framework for the CPCS will be next reviewed.

70. In the interim, additional measures taken at the practical, technical and organisational level (as recommended in the Prior Checking Opinion) may provide a partial interim solution to address these concerns. Awaiting legislative changes, some changes may also be introduced via the CPCS Operating Guidelines.

71. With regard to the retention period, the EDPS recommends that (i) mutual assistance requests should be closed within specifically designated time-limits; (ii) unless investigation or enforcement is ongoing, alerts should be withdrawn and deleted within six months of issuance (unless another, more appropriate retention period can be justified); and (iii) the Commission should clarify and reconsider the purpose and proportionality of keeping all data relating to closed cases for five additional years.

72. Further, the EDPS is pleased that the Second CPC Amendment clarifies the Commission's access to data in CPCS. In particular, the EDPS is pleased that the Commission has no access to confidential communications among competent authorities in Member States, such as mutual assistance requests.

73. The EDPS also is pleased that the Second CPC Amendment introduced a provision to address the processing of special categories of data in CPCS.

74. As additional points, the EDPS recommends that the Commission should re-assess what additional technical and organisational measures to take to ensure that privacy and data protection are "designed" into the CPCS system architecture ("privacy by design") and that adequate controls are in place to ensure data protection compliance and provide evidence thereof ("accountability").

75. Further, if an EU-wide agreement between the European Union and any third country is to be concluded to govern consumer protection cooperation, the implications of these arrangements must be carefully considered, clear rules must be established to govern these exchanges and adequate data protection safeguards must be provided.

76. Finally, the EDPS recommends that the Commission should explore the possible synergies that might arise if data protection authorities were enabled to join the user community of CPCS to cooperate to help enforce "consumer data protection rights".

Done at Brussels, 5 May 2011

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor