RECOMMENDATIONS

COMMISSION RECOMMENDATION

of 1 March 2011

guidelines for the implementation of data protection rules in the Consumer Protection Cooperation System (CPCS)

(2011/136/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation) ([1]) (hereinafter referred to as 'the CPC Regulation') aims at enhancing the enforcement cooperation of consumer protection laws within the single market, establishes an EU-wide Network of national public enforcement authorities (hereinafter referred to as the 'CPC Network') and lays down the framework and general conditions under which Member States enforcement authorities are to cooperate to protect the collective economic interest of consumers.

(2) Cooperation between national enforcement authorities is vital for the single market to function effectively and under the CPC Network each authority is able to call on other authorities for assistance in investigating possible breaches of EU consumer protection laws.

(3) The aim of the Consumer Protection Cooperation System (hereinafter referred to as the 'CPCS') is to enable public enforcement authorities to exchange information concerning possible breaches of consumer protection laws within a safe and secure environment.

(4) The exchange of information by electronic means between Member States needs to comply with the rules on the protection of personal data laid down in 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 ([2]) (hereinafter referred to as the 'Data Protection Directive') and Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ([3]) (hereinafter referred to as the 'Data Protection Regulation').

(5) Article 8 of the Charter of Fundamental Rights of the European Union recognises the right to data protection. The CPCS should ensure that the different obligations and responsibilities shared between the Commission and Member States as regards data protection rules are clear and data subjects are provided with information and easily available mechanisms to assert their rights.

(6) It is appropriate to establish guidelines for the implementation of data protection rules in the CPCS (hereinafter referred to as the 'guidelines') in order to ensure that data protection rules are respected when data is processed through the CPCS.

(7) Enforcement officials should be encouraged to contact their national Data Protection Supervisory Authorities for guidance and assistance on the best way to implement the guidelines in accordance with national law and if necessary to ensure that notification and prior checking procedures relating to the processing operations under the CPCS are carried out at national level.

(8) Participation in the training sessions organised by the Commission to assist with the implementation of the guidelines should be strongly encouraged.

(9) Feedback to the Commission on the implementation of the guidelines should be provided no later than 2 years following the adoption of this Recommendation. The Commission should then make a further assessment of the level of data protection in the CPCS and should evaluate whether additional instruments, including regulatory measures, are required.

([1]) OJ L 364, 9.12.2004, p. 1.
([2]) OJ L 281, 23.11.1995, p. 31.
([3]) OJ L 8, 12.1.2001, p. 1.

(10) Necessary steps should be taken to facilitate the implementation of the guidelines by actors and users of the CPCS. National data protection authorities and the European Data Protection Supervisor should closely monitor developments and the implementation of data protection safeguards with respect to the CPCS.

(11) The guidelines complement Commission Decision 2007/76/EC [1] and take into account the opinion of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 [2] of the Data Protection Directive and the opinion of the European Data Protection Supervisor [3] established by Article 41 of the Data Protection Regulation (hereinafter referred to as the 'EDPS').

HAS ADOPTED THIS RECOMMENDATION:

Member States should follow the guidelines laid down in the Annex.

Done at Brussels, 1 March 2011.

For the Commission
John DALLI
Member of the Commission

[1] OJ L 32, 6.2.2007, p. 192.
[2] Opinion 6/2007/EC on data protection issues related to the Consumer Protection Cooperation System (CPCS) 01910/2007/EN — WP 130 — adopted on 21 September 2007.
[3] EDPS Opinion Ref. 2010-0692.

ANNEX

Guidelines for the implementation of data protection rules in the Consumer Protection Cooperation System (CPCS)

1. INTRODUCTION

Cooperation between national consumer protection authorities is vital for the proper functioning of the internal market since a lack of effective enforcement in cross-border cases undermines the confidence of consumers in taking up cross-border offers and hence their faith in the internal market and also gives rise to a distortion of competition.

The CPCS is an IT-tool established by the CPC Regulation and provides a structured mechanism for the exchange of information between national consumer protection authorities that form part of the CPC Network. It allows a public authority to call on other public authorities of the CPC Network for assistance in investigating and tackling possible infringements of EU consumer protection legislation and in taking enforcement action to stop illegal commercial practices of sellers and suppliers targeting consumers living in other EU countries. Requests for information and all communication between competent public authorities concerning the application of the CPC Regulation are carried out through the CPCS.

The objective of the CPC Regulation is to enhance the enforcement of consumer protection laws across the internal market by setting up an EU-wide Network of national enforcement authorities and to establish the conditions under which Member States are to cooperate with each other. The CPC Regulation established that such exchanges of information and mutual assistance requests between national enforcement authorities was to be carried out through a designated database. The CPCS was therefore designed to facilitate this administrative cooperation and exchange of information with a view to enforcing EU consumer protection laws.

The scope of cooperation is limited to intra-Community infringements of the legal acts listed in the Annex to the CPC Regulation that protects the collective economic interests of consumers.

2. SCOPE AND OBJECTIVE OF THESE GUIDELINES

These guidelines aim at addressing the central concern of ensuring a balance between efficient and effective enforcement cooperation amongst Member States competent authorities whilst respecting fundamental rights to privacy and the protection of personal data.

Personal data is defined in the Data Protection Directive [1] as any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Since national enforcement officials (case handlers) who are the CPCS users may not always be data protection experts and may not always be sufficiently aware of the data protection requirements imposed by their own national data protection legislation, it is advisable to provide CPCS users with guidelines in which the functioning of the CPCS is explained from a practical data protection perspective as well as detailing the safeguards that are built into the system and the possible risks associated with its use.

The objective of the guidelines is to cover the most significant data protection issues in connection with the CPCS and provide a user-friendly explanation that all CPCS users can refer to. It does not, however, provide an exhaustive analysis of the data protection implications of the CPCS.

It is strongly recommended that data protection authorities in the Member States be consulted to ensure that the guidelines are complemented with specific obligations laid down in national data protection laws. CPCS users can also obtain further assistance and guidance from these national data protection authorities to ensure that data protection requirements are met. A list of these authorities with the contact details and websites can be found at:

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/#eu

It should be clear that the processing of personal data should be carried out in accordance with the specific principles and conditions laid down in the Data Protection Directive. Case handlers are entitled in the context of Regulation to exchange data, including personal data, through the CPCS, if the purpose of the processing is to stop the infringement of EU consumer laws as listed in the CPC Regulation Annex. Before processing such data however, a careful assessment is necessary to ensure that data protection principles are safeguarded and processing is strictly necessary to achieve the aims of the CPC Regulation.

[1] Article 2(a).

With this in mind, case handlers having access to the CPCS will need to carry out a case by case assessment before any processing of personal data can be carried out [1]. The purpose of these guidelines is to assist case handlers with this assessment by providing some guiding data protection principles that need to be considered.

The aim is also to clarify some of the complexities of the CPCS architecture with regard to joint processing operations and joint controllership by setting out what is the role of the Commission and the role of Member States competent authorities as 'joint-controllers' of the CPCS data exchanges.

3. THE CPCS — AN IT-TOOL FOR ENFORCEMENT COOPERATION

The CPCS is an IT-tool designed and maintained by the Commission in cooperation with the Member States. The purpose of the CPCS is to assist Member States with the practical implementation of EU consumer protection legislation. It is used by the CPC Network which consists of public authorities designated by the Member States and EEA countries to cooperate and exchange information with each other in the enforcement of consumer protection laws as provided in the CPC Regulation.

Article 10 of the CPC Regulation states that:

'The Commission shall maintain an electronic database in which it shall store and process the information it receives under Articles 7, 8 and 9. The database shall be made available for consultation only by the competent authorities…'

Article 12(3) of the CPC Regulation adds:

'Requests for assistance and all communication of information shall be made in writing using a standard form and communicated electronically via the database established in Article 10.'

The CPCS facilitates cooperation and exchanges of information limited to intra-Community infringements of the Directives and Regulations listed in the CPC Regulation Annex which deals with a variety of topics including unfair commercial practices, distance selling, consumer credit, package travel, unfair contract terms, time-share, e-commerce and others. The CPCS cannot be used for information exchanges in legislative areas not specifically listed in this Annex.

Examples:

I. A trader established in Belgium is using unfair terms in his dealings with consumers resident in France in breach of the Unfair Contract Terms Directive. The consumer authority in France may use the CPCS to make a request to the consumer authority in Belgium to take all necessary enforcement measures available in Belgium against the trader to bring about the cessation of the intra-Community infringement without delay.

II. The consumer authority in Denmark receives complaints that a particular website is using fraudulent and deceptive commercial practices to the detriment of consumers. The website is hosted in Sweden. The Danish consumer authority needs information in connection with the website. It may therefore use the CPCS to make a request for information to the Swedish consumer authority which has an obligation to supply the information.

Information is uploaded by Member States, stored in the CPCS, accessed by the Member States to whom the information was addressed and deleted by the Commission [2]. The CPCS is used as a repository for information and as a means to exchange information through an efficient and secure communication system.

From a data protection perspective, the establishment of such a database always creates certain risks to the fundamental right of personal data protection: sharing more data than is strictly necessary for the purposes of efficient cooperation; retaining data that should have been deleted and holding data that is no longer accurate or is incorrect; and failing to ensure that the rights of data subjects and obligations of data controllers are respected. It is therefore necessary to address such risks by ensuring that the users of the CPCS are well informed and trained in data protection rules and capable of ensuring compliance with applicable data protection legislation.

4. DATA PROTECTION LEGAL AND SUPERVISORY FRAMEWORK

The European Union has an established legal framework on data protection since 1995: the Data Protection Directive [3] which governs the processing of personal data by Member States and by the Data Protection Regulation [4] which governs the processing of personal data by the European Union institutions and bodies. The application of the data protection law currently depends on who the CPCS actor or user is.

[1] It should be noted that data protection principles apply to both data stored electronically and data stored in hardcopy.
[2] For specific rules on deletion see: Decision 2007/76/EC and 'The Consumer Protection Cooperation Network: Operating Guidelines'.
[3] Directive 95/46/EC.
[4] Regulation (EC) No 45/2001.

Processing acts undertaken by the Commission are governed by Data Protection Regulation and processing acts undertaken by case handlers in the competent national enforcement authorities are governed by the national laws transposing the Data Protection Directive.

Being the two main actors with specific roles to play in the CPCS, both the Commission and the designated competent authorities, as co-controllers, have an obligation to notify and submit their respective processing operations for prior checking by the relevant supervisory authorities and ensure compliance with data protection rules. That said national laws transposing the Data Protection Directive may provide exemptions from both the notification and prior checking requirements.

The harmonisation of data protection laws was intended to ensure both a high level of data protection and safeguard the fundamental rights of individuals whilst allowing the free flow of personal data between Member States. Given that national implementation measures may give rise to differing rules, in order to ensure compliance with data protection rules, CPCS users are strongly advised to discuss these guidelines with their national data protection authorities since rules may vary, for example, on the information to be provided to individuals or the duty to notify certain data processing operations to data protection authorities.

A significant feature of the EU data protection legal framework is its supervision by independent data protection authorities. Citizens have the right to lodge complaints before these authorities and promptly resolve their data protection concerns outside the courts. The processing of personal data at national level is supervised by the national data protection authorities and the processing of personal data by the European institutions is supervised by the European Data Protection Supervisor (EDPS) ([1]). Consequently, the Commission is subject to the supervision of the EDPS and other users of the CPCS to the supervision of national data protection authorities.

5. WHO IS WHO IN THE CPCS? — THE ISSUE OF JOINT CONTROLLERSHIP

The CPCS is a clear example of joint processing operations and joint controllership. Whilst only the competent authorities in the Member States collect, record, disclose and exchange personal data, the storage and deletion of these data on its servers is the responsibility of the Commission. The Commission does not have access to these personal data but is considered as the system manager and operator of the system.

Consequently, the allocation of different tasks and responsibilities between the Commission and the Member States can be summarised as follows:

— Each competent authority is a data controller with respect to its own data processing activities.

— The Commission is not a user but the operator of the system, responsible primarily for the maintenance and security of the system architecture. However, the Commission also has access to the alerts, feedback information and other case related information ([2]). 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. The Commission does not however have access to the information contained in mutual assistance and enforcement requests as these are only addressed to the Member States competent authorities dealing with the specific case in question. That said the CPC Regulation does provide the possibility for the Commission to assist competent authorities in case of certain disputes ([3]) and to be invited to participate in a coordinated investigation involving more than two Member States ([4]).

— The CPCS actors share responsibility with respect to the legitimacy of the processing, information provision and rights of access, objection and rectification.

— Both the Commission and the competent authorities in their roles as controllers are individually responsible for ensuring that the rules relating to their data processing operations are compatible with data protection rules.

6. ACTORS AND USERS IN THE CPCS

Different access profiles exist within the CPCS: access to the database is restricted and allocated to a named competent authority official only (authenticated user) which is not transferable. Requests for access to the CPCS can only be granted to the officials notified to the Commission by Member States competent authorities. A login/password is requested to enter the system which can be obtained by the single liaison office.

Only users in the requested and applicant competent authorities have full access to the complete information exchanged for a given case which includes all attachments in the CPCS case file. Single liaison offices 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 cannot read confidential documents attached to a request or an alert.

([1]) http://www.edps.europa.eu/EDPSWEB/edps/EDPS
([2]) Articles 8, 9, and 15 of CPC Regulation (EC) No 2006/2004.
([3]) Article 8(5) of CPC Regulation (EC) No 2006/2004.
([4]) Article 9 of CPC Regulation (EC) No 2006/2004.

In enforcement cases, general information is shared between users in all the competent authorities notified as being responsible for the legal acts infringed. This is done through the notifications. These notifications should give a broad description of a case and should avoid including personal data. Exceptions may exist such as the name of seller or supplier (if a natural person).

The Commission has no access to information and enforcement requests or confidential documents but does receive notifications and alerts.

7. DATA PROTECTION PRINCIPLES APPLICABLE TO EXCHANGES OF INFORMATION

Processing of personal data by the CPCS users in the Member States may only take place under conditions and in accordance with the principles that the Data Protection Directive establishes. The data controller is responsible for ensuring that the data protection principles are complied with when processing personal data in the CPCS.

It should also be noted that both confidentiality and data protection rules apply to the CPCS. Confidentiality rules and professional secrecy rules can apply to data in general whereas data protection rules are limited to personal data.

It is important to bear in mind that CPCS users in the Member States are responsible for many other processing operations and may not be data protection experts. Data protection compliance in the CPCS does not need to be unduly complicated or pose an excessive administrative burden. Neither does it have to be a one-size fits all system. These guidelines are recommendations for the treatment of personal data and it should be recalled that not all the data exchanged within the CPCS is personal data.

Before each upload of information into the CPCS, enforcement officials need to consider whether the personal data to be sent is strictly necessary to achieve the purposes of efficient cooperation and give consideration to whom they are sending the personal data. The enforcement official needs to ask himself whether the recipient strictly needs to receive this information for the purposes of the alert or mutual assistance request.

The following list of fundamental data protection principles aims at assisting enforcement officials having access to the CPCS to make a case by case assessment of whether data protection rules related to the processing of personal data are being complied with each time they process personal data within the system. Enforcement officials should also bear in mind that exemptions and restrictions on the application of the data protection principles, listed below, may exist at national level and are advised to consult their national data protection authorities [1].

What are the data protection principles to be observed?

The general principles on data protection to be borne in mind before undertaking the processing of any personal data have been taken from the data protection Directive. Since this Directive has been transposed into national law, case-handlers are reminded to consult their national data protection supervisory authorities regarding the application of the principles listed below and are advised to see whether any exemptions or restrictions exist to the application of these principles.

Principle of Transparency

According to the Data Protection Directive, the data subject has the right to be informed when his personal data is being processed. The controller is required to provide his name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair [2].

Data may be processed only under the following circumstances [3]:

— when the data subject has given his consent,

— when the processing is necessary for the performance of or the entering into a contract,

— when processing is necessary for compliance with a legal obligation,

— when processing is necessary in order to protect the vital interests of the data subject,

[1] Article 11(2) and 13 of Directive 95/46/EC.
[2] Article 10 and 11 of Directive 95/46/EC.
[3] Article 7 of Directive 95/46/EC.

— processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed,

— processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.

Principle of lawfulness and fairness

Personal data cannot be collected or processed in unfair or unlawful ways, nor should it be used for ends not compatible with the purposes laid down in the CPC Regulation. For processing to be lawful, case handlers need to ensure that they have clear reasons justifying the processing need. The processing needs to be conducted for specified, explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes ([1]). This can only be provided for in the CPC Regulation.

For the processing to be fair, the data subjects need to be informed of the purposes for which his/her data is to be processed and of the existence of the right of access, rectification and objection.

Principle of proportionality, accuracy and retention periods

The information needs to be proportionate, adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; personal data needs to be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they were processed. Appropriate safeguards need to be built in for personal data stored for longer periods for historical, statistical or scientific use.

Case handlers need to consider whether the information that they are processing is strictly necessary to the purposes to be achieved.

Principle of purpose limitation

Personal data needs to be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes and brought to the attention of the data subject. Case handlers should only process personal data only when there is a clear purpose for doing so i.e. that legal grounds exist within the CPC Regulation that justifies the transfer.

Rights of access

Data subjects have the right according to the Data Protection Directive ([2]) to be informed that their personal data are being processed; the purposes for the processing; the recipients of the data and that they have specific rights i.e. the right to information and rectification. The data subject has the right to access all data processed on him. The data subject also has the right to request the rectification, deletion or blocking of data that is incomplete, inaccurate or is not being processed in compliance with the data protection rules ([3]).

Sensitive data

Processing of data revealing racial or ethnical origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, offences and criminal convictions is prohibited. However, the Data Protection Directive ([4]) does provide for certain exemptions to this rule where sensitive data may be processed under given conditions ([5]). Since CPCS users may find themselves in a position where they are handling sensitive data ([6]), it is advised to approach sensitive data with caution. CPCS users are recommended to consult their national data protection authority on whether derogations apply to the processing sensitive data.

Exemptions

In the context of the prevention, investigation, detection and prosecution of criminal offences some exemptions are allowed by the Data Protection Directive. Case handlers are advised to consult national law to assess whether such exemptions are possible and to what extent ([7]). Should such exemptions be used, it is recommended that they are clearly indicated in the privacy statements of each competent authority.

([1]) Article 6(1)(b) of Directive 95/46/EC.
([2]) Article 10, 11, 12 of Directive 95/46/EC.
([3]) Article 12 of Directive 95/46/EC.
([4]) Article 8(2) of Directive 95/46/EC.
([5]) Article 8 of Directive 95/46/EC.
([6]) Chapter 4 of the Annex to Decision 2007/76/EC.
([7]) Opinion 6/2007/EC on data protection issues related to the Consumer Protection Cooperation System (CPCS) 01910/2007/EN — WP 130 — adopted on 21 September 2007, p. 24-26.

Applying the data protection principles

Applying these data protection principles to the functioning of the CPCS leads to the following recommendations:

(1) The use of the CPCS should be strictly limited to the purposes set out in the CPC Regulation. Article 13(1) of the CPC Regulation states that information communicated may only be used for the purpose of ensuring compliance with the laws that protect consumers' interests. These laws are listed in the Annex to the CPC Regulation.

(2) It is recommended that enforcement officials use the information obtained from a mutual assistance request or alert only for the purposes relating to that specific case, in strict compliance with data protection legal requirements, assessing ex ante the necessity of the processing in the context of investigations carried out in the wider public interest.

(3) When transferring data, enforcement officials make an assessment on a case by case basis of who should be the recipients of the information to be processed.

(4) The CPCS users should carefully select the questions they ask in the mutual assistance request and not ask for more data than in necessary. This is not only an issue of respecting data quality principles but also a matter of reducing the administrative burden.

(5) The Data Protection Directive [1] requires that personal data needs to be accurate and kept up to date. It is recommended that it should be for the competent authority which supplied the information to contribute towards the ensuring the accuracy of the data stored in the CPCS. Pop up messages have been added as a feature in the CPCS to periodically remind case handlers to check whether personal data is accurate and kept up to date.

(6) A practical way to inform data subjects' of their rights is through a comprehensive webpage privacy notice. It is recommended that each competent authority should provide a webpage privacy notice on their websites. Each privacy notice should conform with all the information obligations as established by the Data Protection Directive, include a link to the Commission's privacy notice webpage and should give further details including contact details on the competent authority in question as well as any national restrictions on the right of access or information. All data controllers involved are responsible for ensuring that privacy notices are published.

(7) The data subject may request access, rectification and deletion of their personal data from more than one source. Although each competent authority is responsible, as the data controller, for its own data processing operations, a coordinated response to requests relating to cross-border cases should be pursued. It is recommended that in such cases, competent authorities inform other concerned competent authorities of the receipt of the request.

When a competent authority considers that granting a request may affect the investigation or enforcement procedure being carried out by other competent authorities, the former should request the opinion of the latter before granting the request.

The data subject may also turn to the Commission with its request. The Commission may only grant a request for data to which it has access. On receipt of a request, the Commission should consult the competent authority which supplied the information. If no objections are raised or the competent authority fails to respond within a reasonable period, the Commission may decide whether or not to grant the request on the basis of the Data Protection Regulation. The Commission should also request the opinion of competent authorities whose investigative or enforcement activities may be compromised as a result of granting the request. The Commission should examine whether incorporating additional technical features into the CPCS would facilitate such exchanges.

(8) The CPC Implementing Decision 2007/76/EC provides the establishment of data fields within the CPCS for the names of company directors. Enforcement officials need to make an assessment on whether the inclusion of this type of personal data is necessary to solve the case. A case by case assessment of whether it is necessary to include the name of a company director in the designated data field needs to be made before each upload of information in the CPCS and prior to sending an alert or mutual assistance request to another competent authority.

(9) The CPC Implementing Decision 2007/76/EC requires that the competent authority uploading information or enforcement requests or alerts needs to indicate whether the information is to be treated confidentially. This is to be done on a case by case basis. Similarly, the requested authority, when supplying information, needs to indicate whether the information is to be treated confidentially. The CPCS includes a default value feature where CPCS users need to explicitly grant access to documents by unclicking the confidential flag.

[1] Article 6(1)(d) of Directive 95/46/EC.

8. CPCS AND DATA PROTECTION

Data protection friendly environment

The CPCS has been designed with data protection legislation requirements in mind:

— The CPCS uses s-TESTA which stands for secured Trans European Services for Telematics between Administrations. It offers a managed, reliable and secure pan-European communication platform for European and National administrations. The s-TESTA network is based on a dedicated private infrastructure completely separated from the Internet. Appropriate security measures are included in the system's design to ensure the best possible protection for the Network. The Network is subject of a security accreditation to make it suitable for transmitting information classified at the level 'EU Restricted'.

— A number of technical features have been introduced: secure and personalised passwords to notified competent officials in designated authorities, use of a secure network s-TESTA), pop-up messages that remind case handlers that they need to consider data protection rules when processing personal data, creation of different user profiles that modulate the access to the information depending on the user role (the competent authority, the single liaison office or the Commission), the possibility to limit access to documents by defining them as confidential and the message on the CPCS homepage pointing to the data protection rules.

— Implementing rules ([1]) that cover key aspects to ensure data protection compliance: clear deletion rules (what information; how and when to delete data); principles that specify the types of access to the information (only directly concerned competent authorities have full access and the others only have general information).

— Operational guidelines ([2]) that further clarify what to consider when completing the different data fields and integration of these guidelines ([3]).

— Annual reviews to ensure that competent authorities verify the accuracy of personal data (tagging is planned but has not yet been implemented) and also that cases are closed and/or deleted as foreseen by the rules to ensure that cases are not forgotten. The Commission organises on a regular basis with Member States a systematic review of cases that have been opened for a period substantially longer than the average case-handling period.

— Automatic deletion of mutual assistance cases 5 years after the closing of the case as required by the CPC Regulation.

— The CPCS is an evolving IT-tool which aims to be data protection friendly. Many safeguard features have already been built into the system architecture which has been described above. The Commission intends to continue developing further improvements as required.

Some additional guidance

How long should a case be stored and when should it be closed and deleted?

Only the Commission can delete information from the CPCS ([4]) and it does so normally at the request of a competent authority. When making such a request, the competent authority needs to specify the grounds for the deletion request. The only exception is enforcement requests. These are automatically deleted by the Commission 5 years from the closure of the case by the applicant authority.

Rules with given time limits have been established to ensure the deletion of data that is no longer required; inaccurate; proves to be unfounded and/or has been retained for maximum storage periods.

Why is the data retention period set at 5 years?

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. During the retention period authorised enforcement officials working for a 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.

([1]) Decision 2007/76/EC.
([2]) The Consumer Protection Cooperation Network: Operating Guidelines — endorsed by the CPC Committee on 8 June 2010.
([3]) The content of these guidelines will be integrated into future trainings on the CPCS.
([4]) Article 10 of the CPC Regulation (EC) No 2006/2004 and Chapter 2 of the Annex to the CPC Implementing Decision 2007/76/EC.

What information can be included in the discussion forum?

The discussion forum is annexed to the CPCS and is a tool intended for the exchange of information with respect to issues such as new enforcement powers and best practice. Generally, the discussion forum although not frequently used by enforcement officials should not serve to exchange case-related data and should not refer to personal data.

What type of data can be included in the short summaries and attached documents?

The CPC Implementing Decision 2007/76/EC foresees the data field 'attached documents' in the case of alerts and information and enforcement requests. The short summaries are fields where a description of the infringement should be made. It is recommended that personal data should not be included in the short summaries as the purpose of this data field is to have a general description of the infringement. Personal data in attached documents that is not strictly necessary should be blacked out or removed.

What is meant by 'reasonable suspicion' that an infringement has occurred?

Reasonable suspicion needs to be interpreted in accordance with national law. However, it is recommended that suspected infringements should only be included in the CPCS if there is some evidence to support the case that an infringement has or is likely to have occurred.

What about transfers to third countries?

The CPC Regulation [1] provides that information communicated under the CPC Regulation may also be communicated to an authority of a third country by a Member State having a bilateral assistance agreement provided the consent of the competent authority that originally communicated the information has been obtained and that data protection provisions are met.

It is recommended that in the absence of an international agreement by the European Union for mutual assistance cooperation arrangements [2] with a third country, any bilateral assistance agreement with a given third country should provide for adequate data protection safeguards and be notified to the relevant data protection supervisory authorities so that prior checking may be carried out, unless the Commission has found that the third country ensures an adequate level of protection for personal data transferred from the Union in accordance with Article 25 of the Data Protection Directive.

[1] Article 14(2) of CPC Regulation (EC) No 2006/2004.
[2] Article 18 of CPC Regulation (EC) No 2006/2004.