Stellungnahme zur Meldung der Europäischen Kommission vom 9. Januar 2009 für eine Vorabkontrolle über das System zur Zusammenarbeit im Verbraucherschutz („CPCS“)

Brüssel, den 4. Mai 2011 (Fall 2009-0019)

Inhaltsverzeichnis

Postanschrift: Rue Wiertz 60 - 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 63
E-Mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 - Fax : +32 (0)2 283 19 50

1. Einleitung

1.1. Geltungsbereich der Stellungnahme

In der vorliegenden Stellungnahme prüft der Europäische Datenschutzbeauftragte („**EDSB**“) die Frage, ob das System zur Zusammenarbeit im Verbraucherschutz („**CPCS**“) den Datenschutzvorschriften entspricht und formuliert Empfehlungen für weitere Verbesserungen, die insbesondere die Kommission an ihren technischen und organisatorischen Maßnahmen vorzunehmen hat.

Das CPCS ist ein von der Kommission gemäß der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz („**CPC-Verordnung**“) entworfenes und betriebenes IT-System. Das CPCS fördert die Zusammenarbeit im Verbraucherschutz zwischen „**zuständigen Behörden**” in EU-Mitgliedstaaten und der Kommission. Die Zusammenarbeit ist auf Verstöße gegen vorab festgelegte Richtlinien und Verordnungen der EU beschränkt. Außerdem müssen die Verstöße, die in den Anwendungsbereich der CPC-Verordnung fallen, grenzüberschreitender Art sein und den „**Kollektivinteressen der Verbraucher**“ schaden oder schaden können.

Im Rahmen ihrer Zusammenarbeit tauschen die zuständigen Behörden Informationen einschließlich personenbezogener Daten aus (vgl. Punkt 1.3).[1] Das System ist als sicheres Kommunikationsinstrument konzipiert, mit dem die zuständigen Behörden Informationen austauschen können. Darüber hinaus zeichnet das CPCS auch Informationen auf und speichert sie, häufig für recht lange Zeiträume (vgl. Punkt 3.3). Es ist daher als Datenbank zu betrachten.

Die Empfehlungen in dieser Stellungnahme sind an die Kommission gerichtet, die eine zentrale Rolle bei Konzeption und Betrieb des CPCS spielt und der Aufsicht durch den EDSB unterliegt. Viele der in dieser Stellungnahme formulierten Empfehlungen – einschließlich der Empfehlungen, die sich mit Schulung, Datenschutzleitlinien, Information der betroffenen Personen und in die Systemarchitektur integrierten Lösungen des „eingebauten Datenschutzes“ befassen – können auch anderen Nutzern des Systems wie den zuständigen Behörden in den Mitgliedstaaten die Einhaltung der Datenschutzvorschriften erleichtern. Die mit Blick auf die Kommission ausgesprochenen Empfehlungen sollten also dazu beitragen, im CPCS allgemein ein hohes Niveau des Datenschutzes zu gewährleisten.

Parallel zur Annahme dieser Stellungnahme im Rahmen der Vorabkontrolle (gemäß Artikel 27 der Verordnung (EG) Nr. 45/2001 („**Verordnung“**))[2] verfasst der EDSB eine weitere Stellungnahme (gemäß Artikel 28 Absatz 2 der Verordnung), in der er sich mit dem rechtlichen Rahmen des CPCS befasst und vor allem auf die Änderung des Beschlusses 2007/76/EG der Kommission[3] vom 1. März 2011 eingeht. In dieser Stellungnahme nimmt der

[1] Darüber hinaus erhebt und verarbeitet die Kommission personenbezogene Daten von CPCS-Nutzern (Sachbearbeitern), sofern sie für den Betrieb des Systems erforderlich sind (beispielsweise bei der Vergabe von Benutzernamen und Passwörtern). Diese Verarbeitung unterliegt keiner Vorabkontrolle (vgl. Punkt 2.2) und wird daher in dieser Stellungnahme nicht weiter diskutiert.

[2] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001, S. 1.

[3] Beschluss der Kommission vom 1. März 2011 zur Änderung der Entscheidung 2007/76/EG zur Durchführung der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden bezüglich der Amtshilfe.

EDSB eine Bestandsaufnahme der bisherigen Fortschritte vor, greift erneut verbleibende Bedenken auf und stellt Überlegungen für die Zukunft an. Die beiden Texte sollten gemeinsam betrachtet werden.

1.2. Beschreibung der Verarbeitung

Zur Erleichterung der Zusammenarbeit sind im CPCS folgende Informationsströme vorgesehen:

- **Informationsaustausch auf Ersuchen** (Artikel 6 der CPC-Verordnung). Auf Antrag der ersuchenden Behörde übermittelt die ersuchte Behörde unverzüglich alle einschlägigen Informationen, die erforderlich sind, um festzustellen, ob ein Verstoß vorliegt oder ob ein begründeter Verdacht vorliegt, dass ein solcher erfolgen könnte.
- **Informationsaustausch ohne Ersuchen** (Artikel 7). Jede Behörde kann einen Alarm („**Warnmeldung**“) an ihre Netzpartner in anderen Mitgliedstaaten und an die Kommission senden, um sie darüber zu informieren, dass ein Verstoß gegen Verbraucherschutzvorschriften vorliegt oder ein begründeter Verdacht auf einen solchen Verstoß besteht. Die die Warnmeldung versendende Behörde kann entscheiden, an welche anderen Mitgliedstaaten sie die Nachricht sendet. Das bedeutet, dass nicht alle Warnmeldungen zwangsläufig an alle Mitgliedstaaten gehen.
- **Durchsetzungsersuchen** (Artikel 8). Auf Antrag einer ersuchenden Behörde trifft die ersuchte Behörde alle erforderlichen Durchsetzungsmaßnahmen, um unverzüglich eine Einstellung oder ein Verbot des Verstoßes zu bewirken.[4]
- „**Information / Unterrichtung**“ (Artikel 7 Absatz 2 und Artikel 8 Absatz 6). Wenn eine zuständige Behörde nach einer Warnmeldung Durchsetzungsmaßnahmen trifft oder entsprechende Amtshilfeersuchen bei ihr eingehen, so informiert die zuständige Behörde die betroffenen zuständigen Behörden der anderen Mitgliedstaaten und die Kommission (Artikel 7 Absatz 2). Eine Behörde hat ferner ihren Netzpartnern in allen Mitgliedstaaten sowie der Kommission alle Durchsetzungsmaßnahmen mitzuteilen, die sie auf ein Durchsetzungsersuchen hin ergriffen hat und welche Wirkung diese Maßnahmen hatten (auch, ob der Verstoß beendet ist) (Artikel 8 Absatz 6).
- **Koordinierung der Marktüberwachungs- und Durchsetzungstätigkeit** (Artikel 9). Wenn ein Verstoß die Interessen von Verbrauchern in mehr als zwei Mitgliedstaaten schädigt, koordinieren die betreffenden zuständigen Behörden ihre Durchsetzungsmaßnahmen und Amtshilfeersuchen. Sie können insbesondere gleichzeitig Ermittlungs- und Durchsetzungsmaßnahmen durchführen.

Abgesehen von diesen Informationsaustauschmöglichkeiten können nicht fallspezifische Informationen über ein sogenanntes „**Forum-Modul**“ ausgetauscht werden. Dieses Forum ist nicht auf den Austausch personenbezogener Daten ausgelegt (auch wenn nicht ausgeschlossen werden kann, dass ein solcher vorkommt; um die Gefahr der unabsichtlichen Offenlegung personenbezogener Daten im Forum möglichst klein zu halten, vgl. die Empfehlungen unter Punkt 3.2).

1.3. Verarbeitete personenbezogene Daten

Beim Informationsaustausch im CPCS haben die Nutzer mehrere strukturierte Datenfelder auszufüllen. Einige von ihnen können, andere hingegen müssen ausgefüllt werden. In diesen

---

[4] In der vorliegenden Stellungnahme werden „Informationsaustausch auf Ersuchen“ und „Durchsetzungsersuchen“ gelegentlich unter dem Begriff „**Amtshilfeersuchen**“ zusammengefasst.

Datenfeldern sind die Art des begangenen oder vermuteten Verstoßes, der für den Verstoß verantwortliche Verkäufer oder Dienstleistungserbringer (einschließlich Kontaktangaben, IP-Adresse, Muttergesellschaft und Unternehmensleiter), die mögliche Schädigung des Verbrauchers sowie andere für den Fall relevante Angaben einzutragen.

Eines der Datenfelder ist für den/die Namen des/der Unternehmensleiter/-s vorgesehen und gibt die Möglichkeit, eine Verbindung zu bestimmten Personen (den dort genannten Unternehmensleitern) herzustellen, und beinhaltet somit die Verarbeitung personenbezogener Daten.

Zum Zeitpunkt der Abfassung dieser Stellungnahme steht das Feld für den Namen des Unternehmensleiters in der CPCS-Architektur technisch zwar zur Verfügung, wird aber noch nicht genutzt. Stattdessen wurde eine vorläufige Lösung gefunden, um den datenschutzrechtlichen Bedenken Rechnung zu tragen, die die Artikel 29-Datenschutzgruppe in ihrer unter Punkt 2.3 zitierten Stellungnahme geäußert hat. Dieser Lösung zufolge werden die Namen der Unternehmensleiter nach ihrem Hochladen in das CPCS derzeit in vertraulichen Anlagen gespeichert und nicht in das zu diesem Zweck vorgesehene Datenfeld eingetragen.

Das bedeutet in der Praxis, dass 1) standardmäßig die „zentralen Verbindungsstellen“[5] keinen Zugriff auf diese Informationen haben, 2) die Kommission keinen Zugriff auf diese Informationen hat und 3) diese Informationen nicht in der Datenbank abgefragt werden können, da sie nicht in einem strukturierten Datenfeld erfasst sind.

Das Verfahren der Nutzung von Anlagen anstelle strukturierter Datenfelder wird auf Seite 15 des Dokuments mit dem Titel „Operativer Leitfaden des Netzes für die Zusammenarbeit im Verbraucherschutz“ geschildert, das der CPC-Ausschuss am 8. Juni 2010 gebilligt hat („**CPCN-Leitfaden“**).[6] Die Kommission wartet derzeit das Vorliegen dieser Stellungnahme und damit weitere Hinweise des EDSB ab, bevor sie die Datenfelder für die Namen der Unternehmensleiter verwendet.

Je nach den Gegebenheiten des Einzelfalls können auch andere im CPCS verarbeitete Daten als personenbezogene Daten gelten und erfordern damit datenschutzrechtliche Maßnahmen.

Dazu gehören unter anderem folgende Daten:

- Der den Verstoß begehende Verkäufer oder Dienstleistungserbringer kann – in manchen Fällen - eine natürliche Person sein. In diesem Fall gelten alle im CPCS verarbeiteten ihr Unternehmen betreffenden Daten (z. B. die Tatsache, dass er eines Verstoßes verdächtigt wird) als ihre personenbezogenen Daten, die durch die Verordnung und gegebenenfalls auch durch die Richtlinie 95/46/EG („**Richtlinie**“) geschützt sind.

- Die Verbindung zwischen dem Namen eines Unternehmens und einer Person kann mitunter sehr deutlich sein und leicht wieder hergestellt werden (so kann beispielsweise der Firmenname eines kleinen Unternehmens den Nachnamen des Inhabers beinhalten und kann die Anschrift des Unternehmens die Privatadresse des

[5] Wie nachstehend unter Punkt 1.4 ausgeführt, sind „zentrale Verbindungsstellen“ Behörden, die in den einzelnen Mitgliedstaaten mit der Koordinierung der Anwendung der CPC-Verordnung betraut wurden.
[6] Zu Zugangsrechten, Kennzeichnungen als „vertraulich“ und Suchmöglichkeiten vgl. Punkt 1.5.

Inhabers sein). Auch in diesem Fall sind die im CPCS verarbeiteten Unternehmensdaten für die Person von Bedeutung.[7]

Das CPCS enthält ferner zwei nicht strukturierte Felder für den Informationsaustausch:

- ein Feld für „**Kurzfassungen**“, das mit Freitext auszufüllen ist[8], und
- eine Möglichkeit zum Anhängen von Unterlagen.

Diese Felder können personenbezogene Daten enthalten, wie die Daten von Beschäftigten, Beschwerdeführern oder Verbrauchern.

Schließlich kann nicht ausgeschlossen werden, dass die über das Forum-Modul ausgetauschten Informationen personenbezogene Daten enthalten. In den CPC-Datenschutzleitlinien (vgl. Punkt 3.1) wird daher Durchsetzungsbeamten klar empfohlen, in den Kurzfassungen und im Diskussionsforum keine personenbezogenen Daten zu nennen.

1.4. Für die Verarbeitung Verantwortliche: Aufgaben und Verantwortlichkeiten

Am CPCS wirken verschiedene Akteure mit, die auf unterschiedliche Weise an der Verarbeitung personenbezogener Daten beteiligt sind. Es gibt im CPCS drei „Arten“ von für die Verarbeitung Verantwortlichen, die jeweils ihre besonderen Aufgaben und Verantwortlichkeiten haben.

- Erstens ist jede **zuständige Behörde** für ihre Nutzung des CPCS verantwortlich (z. B. für die Erheblichkeit und sachliche Richtigkeit der von ihr ins System hochgeladenen Informationen). In ihrer Eigenschaft als Nutzer tritt sie also nach einzelstaatlichem Datenschutzrecht im CPCS als für die Verarbeitung Verantwortlicher auf.
- Zweitens sieht die CPCS-Architektur die sogenannten „**zentralen Verbindungsstellen**“ vor. Dabei handelt es sich um die Behörden, die in den einzelnen Mitgliedstaaten mit der Koordinierung der Anwendung der CPC-Verordnung betraut wurden.[9] Zu ihren Aufgaben gehört es, Amtshilfeersuchen an die richtige zuständige Behörde weiterzuleiten. Die zentralen Verbindungsstellen können im Hinblick auf ihre eigenen Tätigkeiten ebenfalls als für die Verarbeitung Verantwortliche auftreten.
- Schließlich hat auch die **Kommission** eine besondere Aufgabe und besondere Verantwortlichkeiten als für die Verarbeitung Verantwortlicher. So spielt die Kommission insbesondere eine Hauptrolle bei der Festlegung der Funktionalitäten des Systems, sie betreibt das System, gewährleistet die Sicherheit der ausgetauschten Daten, verwaltet die CPCS-Nutzer und geht Zwischenfällen in den Bereichen Technik und Sicherheit nach. Sie kann ferner als einziger Beteiligter bestimmte Aktionen durchführen (wie die Löschung von Fällen). Außerdem hat die Kommission als Empfängerin von Alarmmeldungen und Mitteilungen Zugriff auf bestimmte im System ausgetauschte Daten.

[7] In einigen Mitgliedstaaten gelten auch Daten von juristischen Personen als dem Datenschutzrecht unterliegende personenbezogene Daten und werden entsprechend behandelt. In diesen Ländern haben die im CPCS Informationen austauschenden zuständigen Behörden zumindest in gewissem Ausmaß den Schutz personenbezogener Daten von Unternehmen zu gewährleisten (z. B. bezüglich der Datenqualität oder der Informationspflicht oder der Zugangsrechte).

[8] Die Kurzfassungen sollten keine personenbezogenen Daten enthalten (vgl. Punkt 3.2).

[9] Die Koordinierungsaufgaben sind in Artikel 3 Buchstabe d, Artikel 9 Absatz 2, Artikel 12 Absatz 2 und Absatz 5 der CPC-Verordnung definiert.

Der EDSB begrüßt die Tatsache, dass

- die CPC-Verordnung in ihrem Artikel 10 eindeutig besagt, dass alle oben genannten Parteien ihre eigenen Pflichten als für die Verarbeitung Verantwortliche haben, und
- dass die CPC-Datenschutzleitlinien (in Abschnitt 3) nähere Einzelheiten zu den Aufgaben und Verantwortlichkeiten aufführen.

1.5. Zugang zu Informationen im CPCS

Zuständige Behörden, zentrale Verbindungsstellen und Kommission haben Zugang zu unterschiedlichen Kategorien von Daten, die innerhalb des CPCS ausgetauscht werden:

- Die zuständigen Behörden haben Zugang zu ausdrücklich an sie gerichteten Informations- und Durchsetzungsersuchen, ferner zu Warnmeldungen (sofern sie vom Absender als Empfänger ausgewählt wurden) und zu Mitteilungen, die in ihren Zuständigkeitsbereich fallen.
- Zentrale Verbindungsstellen können nur die Informationen zu einem Fall einsehen, mittels derer sie die zuständige Behörde ermitteln können, an die ein Ersuchen zu übermitteln ist. Sie können nur auf Anlagen zu Amtshilfeersuchen zugreifen, die nicht „**als vertraulich gekennzeichnet**“ wurden.[10] Zu Warnmeldungen und Mitteilungen haben sie gar keinen Zugang.
- Die Kommissionsnutzer des CPCS haben Zugang zu Warnmeldungen[11] und Mitteilungen, allerdings nur im Modus „schreibgeschützt“. Auf Amtshilfeersuchen kann die Kommission nicht zugreifen.

Da die Kommission außerdem für die Pflege und den laufenden Betrieb des Systems zuständig ist, haben ihre Techniker Lese- und Schreibzugriff auf alle Daten im CPCS einschließlich personenbezogener Daten.

Zu den Suchmöglichkeiten erläuterte die Kommission dem EDSB, alle strukturierten Datenfelder seien durchsuchbar. Unstrukturierte Datenfelder wie Anlagen und Freitextfelder für Kurzfassungen sind nicht durchsuchbar. Jeder CPCS-Nutzer kann nur Datenbestände durchsuchen, auf die er Zugriff hat (so kann beispielsweise der Inhalt eines Amtshilfeersuchens nur von den beiden Behörden gesucht werden, die die Information ausgetauscht haben; der Inhalt einer Warnmeldung kann nur von der zuständigen Behörde gesucht werden, die den Alarm hochgeladen hat, sowie von den Behörden, die den Alarm erhalten haben).

Der EDSB begrüßt die Tatsache, dass

- den jeweiligen zuständigen Behörden Zuständigkeitsbereiche zugeordnet wurden: Informationen werden nur an Behörden weitergegeben, die für einen bestimmten Rechtsbereich zuständig sind (also für eine oder mehrere Maßnahmen im Bereich des Verbraucherschutzes);
- zentrale Verbindungsstellen Ersuchen an die betreffenden Behörden weiterleiten und damit die Gefahr von Fehlern bei der Benennung der Empfänger gesenkt wird;

[10] Standardmäßig werden alle Anlagen als vertraulich gekennzeichnet. Die die Anlage hochladende zuständige Behörde hat das Merkmal „Vertraulichkeit“ abzuklicken, wenn sie der zentralen Verbindungsstelle den Inhalt der Anlage zugänglich machen möchte.

[11] Ausnahmen hiervon sind Anlagen zu Warnmeldungen, zu denen die Kommissionsnutzer des CPCS keinen Zugang haben.

- Anlagen zu Amtshilfeersuchen und Warnmeldungen standardmäßig als vertraulich gekennzeichnet werden;
- der Zugriff der Kommission auf die nach der CPC-Verordnung erforderlichen Elemente beschränkt ist. So hat die Kommission insbesondere keinen Zugang zu Informationen, die im Rahmen von Amtshilfeersuchen zwischen Mitgliedstaaten ausgetauscht werden;
- zentrale Verbindungsstellen nur die Informationen zu einem Fall einsehen können, mittels derer sie die zuständige Behörde ermitteln können, an die ein Ersuchen zu übermitteln ist, und
- Suchmöglichkeiten an Zugangsrechte geknüpft sind.

Im Hinblick auf das strukturierte Datenfeld für den Namen des Unternehmensleiters erhebt der EDSB keinen Einwand gegen die Nutzung eines solchen Datenfelds (anstelle der Angabe des Namens des Unternehmensleiters in vertraulichen Anlagen, wie sie derzeit erfolgt).

Falls jedoch die Kommission dem EDSB gegenüber nicht ausreichend begründen kann, dass der Zugang zu diesem Datenfeld für die Kommission zur Wahrnehmung ihrer Überwachungsaufgaben gemäß der CPC-Verordnung erforderlich ist, empfiehlt der EDSB, mit technischen Vorkehrungen im System einen solchen Zugang auszuschließen.

Um ferner sicherzustellen, dass personenbezogene Daten eines Verkäufers oder Dienstleistungserbringers, der eines Verstoßes verdächtigt wird, nicht ungebührlich lange in der Datenbank in einer auffindbaren Form gespeichert werden, sollten auch die Empfehlungen zur Datenaufbewahrung (vgl. Punkt 3.3.2) umgesetzt werden. Bei Verdacht auf einen Verstoß sollten aus einer Warnmeldung stammende Daten zu den Unternehmensleitern auf keinen Fall nach Ablauf des unter Punkt 3.3.2 empfohlenen (vermutlich sechsmonatigen) Zeitraums auffindbar sein. Gegebenenfalls sollten weitere Beschränkungen der Suchmöglichkeiten erwogen werden.

2. Zuständigkeit des EDSB

2.1. Anwendbarkeit der Verordnung (EG) Nr. 45/2001

Sofern die Tätigkeiten der Kommission betroffen sind, fällt die gemeldete Verarbeitung in den Anwendungsbereich der Verordnung und unterliegt der Aufsicht durch den EDSB (vgl. Artikel 1 und 3 der Verordnung).[12]

2.2. Begründung der Vorabkontrolle

Der Informationsaustausch im CPCS umfasst auch personenbezogene Daten zu Verstößen oder Verdachtsfällen auf Verstöße gegen Verbraucherschutzvorschriften. Es kann dabei sowohl um Ordnungswidrigkeiten als auch um Straftatbestände gehen. Das CPCS unterliegt daher Artikel 27 Absatz 2 Buchstabe a der Verordnung, der eine Vorabkontrolle durch den EDSB unter anderem bei „Verarbeitungen von Daten, die Verdächtigungen, Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen“, fordert.

[12] Das auf die zuständigen Behörden und die zentralen Verbindungsstellen anwendbare Recht ist das auf die Richtlinie zurückgehende jeweilige einzelstaatliche Datenschutzrecht; die Tätigkeit der Behörden und Stellen wird durch die jeweilige einzelstaatliche Datenschutzbehörde überwacht.

2.3. Verfahren

Am 9. Januar 2009 meldete die Kommission dem EDSB das CPCS für eine „nachträgliche" Vorabkontrolle.[13] Der EDSB nahm die Stellungnahme am 4. Mai 2011 nach Erhalt der von der Kommission angeforderten Informationen an.[14]

Der EDSB stellt fest, dass das CPCS schon vor der Meldung an den EDSB verwendet wurde und dass daher die Empfehlungen des EDSB im Nachhinein umzusetzen sind. Der EDSB weist die Kommission darauf hin, dass künftig die Stellungnahme des EDSB vor dem Anlaufen jeglicher Verarbeitung personenbezogener Daten anzufordern und abzugeben ist.

3. Rechtliche Würdigung und Empfehlungen

3.1. Rechtsgrundlage und Rechtmäßigkeit der Verarbeitung

Nach der Annahme der CPC-Verordnung (vgl. Punkt 1.1) baute die Kommission die Rechtsgrundlage des CPCS durch eine Durchführungsentscheidung und eine Empfehlung weiter aus.

- Entscheidung der Kommission 2007/76/EG vom 22. Dezember 2006 zur Durchführung der CPC-Verordnung in der am 17. März 2008 und am 1. März 2011 geänderten Fassung („**CPC-Durchführungsentscheidung**")[15]; und
- Empfehlung der Kommission vom 1. März 2011 „Leitlinien für die Anwendung der Datenschutzbestimmungen im System zur Zusammenarbeit im Verbraucherschutz (CPCS)" („**CPC-Datenschutzleitlinien"**)[16].

Wie schon in der Stellungnahme zu den neuen Maßnahmen der Kommission zur Anwendung der CPC-Verordnung ausgeführt, begrüßt der EDSB die Tatsache, dass sich die Verarbeitung auf eine solide Grundlage stützt, deren Kernelement eine von Rat und Parlament angenommene Verordnung ist. Darüber hinaus stellt der EDSB mit Zufriedenheit fest, dass das ursprüngliche Rechtsinstrument im Verlauf der Zeit ergänzt worden ist und nun weitere Einzelheiten geregelt sind und auf Datenschutzanliegen eingegangen wird.

3.2. Datenqualität

Artikel 13 Absatz 1 der CPC-Verordnung besagt: „*Die übermittelten Informationen dürfen nur zu dem Zweck verwendet werden, die Einhaltung der Gesetze zum Schutz der Verbraucherinteressen zu gewährleisten*". Artikel 13 Absatz 2 fügt hinzu: „*Die zuständigen*

[13] Das CPCS war bereits Gegenstand einer Überprüfung durch die Artikel 29-Datenschutzgruppe, die am 21. September 2007 hierzu ihre Stellungnahme 6/2007 abgab (WP 139). Die in der vorliegenden Stellungnahme vertretene Meinung stützt sich auf die Stellungnahme 6/2007.

[14] Gemäß Artikel 27 Absatz 4 der Verordnung ist die Stellungnahme innerhalb von zwei Monaten abzugeben, wobei alle Aussetzungsfristen zu berücksichtigen sind, innerhalb derer vom EDSB angeforderte Zusatzinformationen eingehen. Der EDSB erbat weitere Informationen von der Kommission am 14. Januar 2009 und am 24. Januar 2011. Diese wurden am 22. Dezember 2010 bzw. 2. März 2011 vorgelegt. Den Entwurf seiner Stellungnahme übermittelte der EDSB zur Kommentierung am 18. März 2011. Gleichzeitig verlängerte er aufgrund der Komplexität des Themas die Frist für die Abgabe seiner Stellungnahme um zwei Wochen. Die Kommission legte ihre abschließenden Kommentare am 14. April 2011 vor. Termin für die Abgabe der Stellungnahme des EDSB war damit der 4. Mai 2011.

[15] Entscheidung der Kommission 2007/76/EG zur Durchführung der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden bezüglich der Amtshilfe.

[16] Empfehlung der Kommission vom 1. März 2011 „Leitlinien für die Anwendung der Datenschutzbestimmungen im System zur Zusammenarbeit im Verbraucherschutz (CPCS" (2011/136/EU).

Behörden dürfen alle ihnen übermittelten Informationen, Unterlagen, Erkenntnisse, Erklärungen, beglaubigten Kopien und Ermittlungsergebnisse in gleicher Weise als Beweismittel verwenden wie entsprechende im eigenen Land beschaffte Unterlagen".

In Anbetracht des weit gefassten Anwendungsbereichs dieser Bestimmungen kommt es darauf an, dass der Datenaustausch innerhalb des CPCS in der Praxis den in Artikel 4 Absatz 1 Buchstaben a, b, c und d der Verordnung festgelegten Standards für die Datenqualität entspricht. Von besonderer Bedeutung ist es, dass alle ausgetauschten personenbezogenen Daten den Zwecken entsprechen, für die sie erhoben werden, dafür erheblich sind, verhältnismäßig und sachlich richtig sind, nach Treu und Glauben und rechtmäßig verarbeitet werden und nicht für mit den Vorschriften nicht zu vereinbarenden Zwecken verarbeitet werden.

Jeder Fall ist jedoch anders gelagert. Die Einhaltung der Grundsätze der Datenqualität ist daher jeweils im konkreten Fall zu überprüfen, sobald Daten von CPCS-Nutzern hochgeladen, abgefragt oder anderweitig verarbeitet werden. In Anbetracht der Tatsache, dass eine fallweise Beurteilung sehr schwierig ist und dass die meisten CPCS-Nutzer keine Datenschutzexperten sind, kommt folgenden Aspekten eine zentrale Bedeutung zu:

- Die CPCS-Systemarchitektur ist so zu aufzubauen und zu konfigurieren, dass die Einhaltung der Datenschutzgesetze so weit wie irgend möglich erleichtert wird.
- Die Nutzer des Systems sollten angemessen geschult und angeleitet werden und befugt sein, den Datenschutz betreffende Entscheidungen zu treffen.

Der EDSB begrüßt die Tatsache, dass die CPC-Durchführungsentscheidung für jeden Informationsaustausch eine Reihe obligatorischer und fakultativer Felder vorsieht und dass diese in einem angemessenen Verhältnis zum Zweck des Informationsaustauschs stehen.[17]

Der EDSB begrüßt ferner die Empfehlung in den CPC-Datenschutzleitlinien, mit der die personenbezogenen Daten in einem Informationsaustausch begrenzt werden; insbesondere begrüßt er, dass

- Durchsetzungsbeamte die Frage zu prüfen haben, ob die Angabe des Namens des Unternehmensleiter wirklich erforderlich ist;
- sie keine personenbezogenen Daten in das Freitextfeld für „Kurzfassungen" aufnehmen dürfen;
- sie zu beurteilen haben, ob personenbezogene Daten in die angehängten Unterlagen aufzunehmen sind; ist eine solche Aufnahme nicht unbedingt erforderlich, sind die personenbezogenen Daten zu schwärzen oder zu löschen;[18] und dass
- im Diskussionsforum keine fallspezifischen Daten ausgetauscht und keine personenbezogenen Daten genannt werden dürfen.

3.2.1. Löschung unrichtiger Daten

Nach der CPC-Durchführungsentscheidung[19] können die zuständigen Behörden von der Kommission die Löschung unrichtiger Daten verlangen, die auf anderem Wege nicht berichtigt werden können.

[17] Zum Feld „Unternehmensleiter" vgl. unsere Empfehlung unter Punkt 1.5.

[18] Stellt sich nachträglich heraus, dass diese Information für Ermittlungs- oder Durchsetzungszwecke von zentraler Bedeutung ist (wenn sie beispielsweise als Beweismittel herangezogen werden kann), kann sie in einer Folgemitteilung angefordert werden.

[19] Vgl. Anhang, Punkt 2.1.5, in der geänderten Fassung.

Die Kommission erläuterte dem EDSB, bei dieser Bestimmung handele es sich um eine „Notlösung“ für eine kleine Anzahl von Fällen, in denen keine besseren Möglichkeiten für die Berichtigung oder Löschung von Daten zur Verfügung stehen. Dies gelte gelegentlich für Fälle von „Doppeleintragungen“, wenn eine zuständige Behörde irrtümlicherweise dieselbe Information zweimal hochlädt oder wenn die hochladende zuständige Behörde die Rechtsgrundlage (z. B. eine Richtlinie) nicht richtig angegeben hat. In den meisten anderen Fällen seien die zuständigen Behörden selber in der Lage, die hochgeladenen Daten zu berichtigen. So könnten sie beispielsweise Angaben zu den betroffenen Verkäufern und Dienstleistungserbringern ändern oder Daten in einer Anlage berichtigen oder löschen.

Der EDSB hat keine Einwände gegen die vorstehend beschriebene „Notlösung“. Er unterstreicht jedoch, dass das System und seine Schnittstellen so zu konzipieren sind, dass diese Notlösung in möglichst wenigen Fällen zur Anwendung kommt.

Die Löschung muss ferner stets so erfolgen, dass ein angemessener Prüfpfad als Nachweis des durchgeführten Vorgangs verfügbar ist (vgl. auch Punkt 3.6).

3.2.2. Hin zu einem Datenschutzmodul (eingebauter Datenschutz - Privacy by Design)

Wie bereits ausgeführt, empfiehlt der EDSB im Sinne einer einfacheren Umsetzung dieser Empfehlungen in der Praxis, die CPCS-Systemarchitektur so aufzubauen und zu konfigurieren, dass die Einhaltung der Datenschutzgesetze so weit wie möglich erleichtert wird.

Der EDSB begrüßt, dass die Systemarchitektur bereits bestimmte datenschutzfreundliche Merkmale enthält, mit denen sich die Anforderungen des Datenschutzes leichter erfüllen lassen, wie eine Pop-up-Nachricht, die den gerade eine Anlage hochladenden Sachbearbeiter darüber informiert, dass diese Anlage keine personenbezogenen Daten enthalten darf, es sei denn, dies ist unbedingt erforderlich, oder auch die allgemeine Pop-up-Nachricht, die zuständige Behörden dazu veranlasst, Datenschutzaspekte zu prüfen, bevor ein Amtshilfeersuchen oder eine Warnmeldung offiziell über das CPCS „verschickt“ wird.

Sollte die Erfahrung zeigen, dass Sachbearbeiter weiterer Orientierung bedürfen, könnten Alternativen zu den derzeitigen Pop-up-Nachrichten oder zusätzliche technische Maßnahmen entwickelt und Bestandteil eines eigenständigen „**Datenschutzmoduls**“ innerhalb der CPCS-Systemarchitektur werden. Dazu könnten folgende Garantien „zum Durchklicken“ eingebaut werden:

- Füllt eine zuständige Behörde das Feld „Name des Unternehmensleiter“ aus, könnte das System automatisch eine Warnmeldung generieren, in der gefragt wird, ob diese Information für den betreffenden Fall unbedingt erforderlich ist, und in der ferner eine Begründung für die Angabe gefordert wird;
- vor dem Hochladen einer Kurzfassung könnte eine Warnmeldung erscheinen, in der der Nutzer aufgefordert wird, zu bestätigen, dass die Kurzfassung keine personenbezogenen Daten enthält (außer dem Firmennamen des Verkäufers oder Dienstleistungserbringers, falls es sich um eine natürliche Person handelt);
- bevor eine Kennzeichnung als „vertraulich“ gelöscht wird, könnte eine Warnung auftauchen, die deutlich die Implikationen dieser Entscheidung darstellt und insbesondere angibt, wer nun Zugang zu den hochgeladenen Informationen hat.

Das System sollte ferner in dem aus der CPCS-Anwendung heraus anzuwählenden Menü „Hilfe“ Rat zu Datenschutzfragen wie den vorstehend genannten enthalten.

Bei Bedarf könnte ein Merkmal für Rückmeldungen und Kommunikation zwischen zuständigen Behörden und Kommission zu Fragen der Einhaltung von Datenschutzvorschriften vorgesehen werden. Bei Verwendung dieses Merkmals hätte jeder Empfänger von Informationen die Möglichkeit, über das CPCS die zuständige Behörde, die die Information hochgeladen hat, davon in Kenntnis zu setzen, dass es in Zusammenhang mit diesen hochgeladenen Informationen ein Problem bei der Einhaltung der Datenschutzvorschriften gibt. So können beispielsweise personenbezogene Daten in die Kurzfassungen eingeflossen sein, oder in einer Anlage finden sich für den Fall unerhebliche personenbezogene Daten. Mit einem solchen Merkmal ließe sich der Austausch personenbezogener Daten auf ein Mindestmaß reduzieren und die Berichtigung ungenauer oder veralteter Informationen erleichtern.[20]

Wie unter Punkt 3.5 näher diskutiert, könnte das Datenschutzmodul auch einen Koordinierungsmechanismus für die Bearbeitung und Herbeiführung von Entscheidungen zu Auskunftsersuchen von betroffenen Personen enthalten.

3.2.3. Schulung und Aufklärung zum Thema Datenschutz

Wie bereits erwähnt, erfordert ein hohes Datenschutzniveau im CPCS, dass die Nutzer des Systems angemessen darüber belehrt werden, wie der Datenschutz in der Praxis bei der Verarbeitung von Daten im CPCS anzuwenden ist.

Diesbezüglich begrüßt der EDSB, dass sich die Kommission bemüht hat, in den CPC-Datenschutzleitlinien mithilfe von Workshops, Kontakten zu zentralen Verbindungsstellen und auf anderem Wege bei den Sachbearbeitern aufklärend zu wirken, und unter anderem die folgenden Datenschutzprobleme unterstrichen hat:

- Sachbearbeiter sollten möglichst wenige personenbezogene Daten angeben (d. h., sie sollten personenbezogene Daten nur angeben, wenn diese für den Zweck des Informationsaustauschs erheblich sind);
- sie sollten sich der Tatsache bewusst sein, dass das Feld „Unternehmensleiter“ fakultativ ist, und sorgfältig abwägen, ob diese Information wirklich in das CPCS eingegeben werden muss;[21]
- sie sollten sorgfältig darauf achten, an welche Empfänger ihre Meldungen gehen, und personenbezogene Daten nur bei Bedarf weitergeben. Dies gilt für die Kommunikation sowohl mit anderen zuständigen Behörden als auch innerhalb einer bestimmten zuständigen Behörde;
- sie sollten Fälle möglichst zügig zum Abschluss bringen und unmittelbar danach die Löschung dieser Fälle beantragen;
- sie sollten über die Informations- und Zugangsrechte der betroffenen Personen Bescheid wissen und sich mit der Behandlung von Zugangsersuchen auskennen;
- sie sollten die Maßnahmen zur Wahrung der Vertraulichkeit und der Sicherheit befolgen. Diesbezüglich sollte jede zuständige Behörde ferner dafür sorgen, dass nur ordnungsgemäß akkreditierte Beamte Zugang zum CPCS haben und dass die

[20] So lange mit dem derzeitigen Merkmal „Fragen und Antworten“ (Chat) im CPCS die von einem bestimmten Informationsaustausch betroffenen zuständigen Behörden diese Fragen innerhalb der CPCS-Architektur diskutieren, mag ein besonderer Kommunikationskanal noch nicht unbedingt erforderlich sein.

[21] Der EDSB begrüßt die Tatsache, dass die CPCS-Schnittstelle mit einem Sternchen deutlich alle Datenfelder kennzeichnet, die ausgefüllt werden müssen, und dass das Feld „Unternehmensleiter“ nicht zu ihnen gehört.

Behörden, sobald ein Beamter seinen Posten verlässt, die Kommission unverzüglich davon in Kenntnis setzen, damit der diesem Nutzer gewährte Zugang sofort widerrufen werden kann.

Der EDSB begrüßt, dass in den CPC-Datenschutzleitlinien die Bedeutung der Schulung unterstrichen wird.

Damit die in den CPC-Datenschutzleitlinien formulierten Empfehlungen auch tatsächlich in die Praxis umgesetzt werden, sollten sie nach Auffassung des EDSB mit angemessenen Schulungsplänen ergänzt werden. Den CPCS-Nutzern sollten solide Kenntnisse der einschlägigen Datenschutzprobleme vermittelt werden, auf die sie beim Austausch von Daten im CPCS stoßen könnten. Hierbei spielen die Aufklärungsaktivitäten der Kommission eine wichtige Rolle.

3.3. Aufbewahrungsfrist

In Artikel 6 Absatz 1 Buchstabe e der Richtlinie heißt es, dass „*personenbezogene Daten […] nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht […]*“. Artikel 4 Absatz 1 Buchstabe e der Verordnung enthält eine gleichwertige Bestimmung.

3.3.1. Fakten, rechtlicher Rahmen und Bestandsaufnahme

Im Verlauf der Bearbeitung von CPCS-Fällen sind drei Fristen zu beachten:

- Aufbewahrungsfrist bis zum Abschluss des Falls: Diese Frist beginnt mit der Einleitung eines Falls und endet mit dem Abschluss des Falls im System;
- Aufbewahrungsfrist zwischen Abschluss und Löschung: Diese Frist beginnt bei Abschluss eines Falls und endet, wenn die Information im System endgültig gelöscht wird;
- Gesamtaufbewahrungsfrist: Diese Frist ergibt sich aus der Addition der beiden anderen Aufbewahrungsfristen.

Die CPC-Verordnung sieht besondere Regeln nur vor für 1) unbegründete Warnmeldungen (die unverzüglich zu löschen sind) und 2) Fälle, in denen es zu einer erfolgreichen Durchsetzung kam (sie sind fünf Jahre nach Abschluss des Falls zu löschen).

Sie enthält keine weiteren besonderen Vorschriften dazu, wann Fälle zu schließen oder Informationen aus der Datenbank zu löschen sind. Ein solcher Mangel an Klarheit könnte dazu führen, dass einige Fälle niemals abgeschlossen und niemals gelöscht oder länger als nötig in der Datenbank gespeichert bleiben. Die Kommission hat sich daher der Frage angenommen und an verschiedenen Stellen für Klarheit gesorgt.

Klarstellungen in der CPC-Durchführungsentscheidung

(i) Die CPC-Durchführungsentscheidung enthält weitere Vorschriften für unterschiedliche Informationsströme:

- Wird ein **Auskunftsersuchen** „abgeschlossen“, weil die ausgetauschten Informationen keine Folgemaßnahmen (wie ein Durchsetzungsersuchen oder eine Warnmeldung) nach sich gezogen haben oder weil sich herausgestellt hat, dass kein

innergemeinschaftlicher Verstoß vorgelegen hat und die betreffende zuständige Behörde erklärt, dass dies der Fall ist, hat die zuständige Behörde innerhalb von sieben Tagen die Kommission zu unterrichten (die Kommission wiederum muss dann innerhalb von sieben Tagen nach der Unterrichtung alle entsprechenden Daten aus der Datenbank entfernen). In allen anderen Fällen[22] werden Auskunftsersuchen fünf Jahre nach Abschluss des Falls gelöscht;

- ist eine **Warnmeldung** begründet, wird sie fünf Jahre nach ihrer Ausgabe aus der Datenbank entfernt. Erweist sich eine Warnmeldung als unbegründet, hat die zuständige Behörde sie innerhalb von sieben Tagen zurückzuziehen (die Kommission wiederum hat dann alle in der Datenbank gespeicherten Daten innerhalb von sieben Tagen nach der Rücknahme der Warnmeldung zu löschen);

- wird ein **Durchsetzungsersuchen** abgeschlossen (nach der Meldung, dass der Verstoß beendet ist), werden alle mit dem Fall in Zusammenhang stehenden Daten fünf Jahre nach Abschluss des Falls gelöscht;

- enthält ein Auskunftsersuchen, eine Warnmeldung oder ein Durchsetzungsersuchen **unrichtige Daten**, die sich nicht auf andere Weise berichtigen lassen, sind diese innerhalb von 14 Tagen (2 x 7, berechnet wie oben beschrieben) zu löschen.

(ii) Aufklärung in den CPC-Datenschutzleitlinien

Neben den genannten Vorschriften in der CPC-Durchführungsentscheidung weisen auch die CPC-Datenschutzleitlinien nachdrücklich auf die Bedeutung eines zügigen Abschlusses von Fällen hin.

(iii) Benchmarking im CPCN-Leitfaden

Im CPCN-Leitfaden geht es unter Punkt 2.7 unter dem Titel „Schritte und Fristen in einem CPC-Fall“ um typische Abläufe von Fällen und wird empfohlen, Auskunftsersuchen im Durchschnitt innerhalb von einem bis drei Monaten zu behandeln, Durchsetzungsersuchen in sechs bis neun Monaten (abgesehen von Fällen, bei denen ein einzelstaatliches Verfahren einen längeren Zeitraum vorsieht, wenn z. B. gegen eine Verwaltungsentscheidung Einspruch eingelegt werden kann; dann ist ein Jahr oder mehr realistischer).

(iv) Jährliche Bestandsaufnahme

Die Kommission nimmt eine jährliche Bestandsaufnahme vor, um eine zügige Abwicklung der Fälle zu fördern. So erstellt sie vor allem eine Liste von Fällen, in der die Fälle besonders herausgehoben werden, die über einen Zeitraum geöffnet waren, der den durchschnittlichen Bearbeitungszeitraum deutlich übersteigt (Vergleich mit den im CPCN-Leitfaden vorgegebenen Fristen, siehe oben). Diese Fälle werden den zentralen Verbindungsstellen gemeldet, die dann wiederum aufgefordert sind, die betreffenden zuständigen Behörden zu kontaktieren.[23]

(v) Regelmäßige Information über den neuesten Stand zwischen den von einem Amtshilfeersuchen betroffenen zuständigen Behörden

[22] Ausgenommen sind unrichtige Daten, wie nachstehend erläutert.

[23] Die Kommission plant ferner, in die Datenbank ein Merkmal „Zeitstempel“ aufzunehmen, mit dem bei der jährlichen Bestandsaufnahme bestätigt werden soll, dass die in die Datenbank eingegebenen personenbezogenen Daten noch richtig sind. Der EDSB begrüßt diese Absicht.

Schließlich fordert Punkt 2.1.3 der CPC-Durchführungsentscheidung, dass die ersuchte Behörde die ersuchende Behörde regelmäßig und in angemessenen Abständen, mindestens aber alle drei Monate über die aufgrund des Ersuchens getroffenen Ermittlungs- und Durchführungsmaßnahmen auf dem Laufenden hält.

3.3.2. Bewertung und Empfehlungen des EDSB

Wie bereits dargelegt, hat die Kommission erhebliche Fortschritte bei der Klarstellung der Regeln für die Datenspeicherung im CPCS gemacht. Sie hat auch Maßnahmen ergriffen, damit die Fälle zügig abgeschlossen werden können.

(i) Zügiger Abschluss von Fällen

Zum Abschluss von Fällen und in Anbetracht der relativ geringen Zahl von Informationsaustauschen, die derzeit im CPCS erfolgen (seit 2007 wurden pro Jahr durchschnittlich 300 neue Fälle einschließlich Warnmeldungen eröffnet), merkt der EDSB an, dass die oben geschilderten Maßnahmen als ausreichend betrachtet werden können, um datenschutzrechtliche Bedenken auszuräumen, die auf das Risiko zurückzuführen sind, dass veraltete und/oder nicht verwendete personenbezogene Daten in erheblichem Umfang über längere Zeiträume in der Datenbank gespeichert bleiben.

Für den Fall, dass die oben beschriebenen Maßnahmen nicht ausreichen, um in Zukunft einen zügigen Abschluss von Fällen zu gewährleisten (aufgrund einer steigenden Zahl von Informationsaustauschen über das CPCS oder auf anderem Weg), empfiehlt der EDSB der Kommission, weitere Maßnahmen zu ergreifen. Dazu könnte unter anderem die automatische Löschung von Fällen gehören, die trotz wiederholter Mahnungen inaktiv geblieben sind.

(ii) Warnmeldungen

Bezüglich der Warnmeldungen hegt der EDSB Bedenken, dass Warnmeldungen fünf Jahre lang im System verbleiben, sofern sie nicht von der ausgebenden zuständigen Behörde als „unbegründet“ bezeichnet und zurückgezogen werden.

Wie in der Stellungnahme des EDSB zu den neuen Maßnahmen der Kommission bezüglich der Anwendung der CPC-Verordnung noch näher diskutiert werden wird, und in Anbetracht der Risiken durch die Speicherung von Daten zu unbestätigten Verdachtsfällen über einen langen Zeitraum empfiehlt der EDSB, alle Warnmeldungen nach kürzerer Zeit zu löschen. Dies sollte zumindest in den Fällen geschehen, in denen sie keine Folgemaßnahmen über das CPCS oder auf anderem Weg nach sich ziehen. In seiner Stellungnahme zu den neuen Maßnahmen der Kommission empfiehlt der EDSB, Warnmeldungen spätestens sechs Monate nach ihrem Hochladen zu löschen (es sei denn, es kann eine andere angemessene Aufbewahrungsfrist begründet werden).

(iii) Aufbewahrungsfrist für abgeschlossene Amtshilfeersuchen

Die „Standard“-Aufbewahrungszeit im CPCS nach Abschluss eines Falls (mit bestimmten Ausnahmen) dürfte sowohl bei Auskunftsersuchen als auch bei Durchsetzungsersuchen bei fünf Jahren liegen.

Weder die CPC-Verordnung noch die CPC-Durchführungsentscheidung geben eine Erklärung für den Zweck oder die Notwendigkeit der Datenaufbewahrung über einen so langen

Zeitraum. Eine ansatzweise Erklärung findet sich in den CPC-Datenschutzleitlinien, wo es heißt: „*Während der Aufbewahrungsfrist dürfen befugte Durchsetzungsbeamte, die für eine zuständige Behörde arbeiten, welche ursprünglich mit dem Fall zu tun hatte, die Akte einsehen, um bei wiederholten Verstößen mögliche Zusammenhänge herzustellen; dies trägt zu einer besseren und effizienteren Durchsetzung bei*“.[24]

Diesbezüglich empfiehlt der EDSB der Kommission Folgendes:

- nähere Erläuterungen zum Zweck der fünfjährigen Aufbewahrungsfrist für die Daten,
- Bewertung der Frage, ob nicht auch eine kürzere Aufbewahrungsfrist zielführend ist, und
- Bewertung der Frage, ob alle derzeit vorgesehenen Informationen gespeichert werden müssen oder ob vielleicht auch ein Teil dieser Informationen ausreichen würde (so sollte beispielsweise geprüft werden, ob nicht die Speicherung lediglich von Mitteilungen nach Artikel 8 Absatz 6 genügen würde; es sollte auch der Frage nachgegangen werden, ob die Speicherung der Namen der Unternehmensleiter oder von Anlagen erforderlich ist, die unter Umständen personenbezogene Daten enthalten; ferner sollte zwischen Daten zu „vermuteten“ und zu „nachgewiesenen“ Verstößen differenziert werden).

Weitere Empfehlungen und Überlegungen zur Aufbewahrungsfrist sind in der Stellungnahme des EDSB zu den neuen Maßnahmen der Kommission für die Anwendung der CPC-Verordnung zu finden. Wie bereits erwähnt, ergänzen sich die beiden Kommentierungen und sollten daher gemeinsam betrachtet werden.

3.4. Informationspflicht gegenüber der betroffenen Person

Nach Artikel 10 und 11 der Richtlinie sind die zuständigen Behörden verpflichtet, der betroffenen Person gewisse Auskünfte über die Verarbeitung zu geben, ohne dass sie darum von der betroffenen Person ausdrücklich ersucht werden müssen.[25] Entsprechende Bestimmungen der Verordnung (Artikel 11 und 12) sehen ähnliche Anforderungen an die Kommission bezüglich der durch sie verarbeiteten personenbezogenen Daten vor. Die CPC-Datenschutzleitlinien empfehlen einen „geschichteten“ Ansatz bei der Bereitstellung von Datenschutzhinweisen. Dieser Ansatz sieht folgendermaßen aus:

- Die Kommission sollte auf der CPCS-Seite der Website EUROPA einen ausführlichen Datenschutzhinweis einstellen, in dem mit klaren und einfachen Formulierungen die Arbeitsweise des CPCS sowie die im CPCS angewandten Datenschutzgarantien erklärt werden; zusätzlich, wenn auch nicht ausschließlich, sollte eine nach der Verordnung erforderliche Datenschutzerklärung zu den Verantwortlichkeiten der Kommission eingestellt werden;
- die zuständigen Behörden sollten ebenfalls (selbst oder über ihre zentralen Verbindungsstellen), beispielsweise auf ihren Websites, Datenschutzhinweise bereitstellen, deren Inhalt sich nach den jeweiligen einzelstaatlichen Datenschutzvorschriften richtet. Hier sollte ein Link zur Website der Kommission mit deren Datenschutzhinweis vorhanden sein, aber auch nähere Informationen

[24] In den CPC-Datenschutzleitlinien heißt es ferner: „Die Aufbewahrungsfrist soll die Zusammenarbeit der bei innergemeinschaftlichen Verstößen gegen die Verbraucherschutzvorschriften zuständigen Durchsetzungsbehörden erleichtern sowie beitragen zum reibungslosen Funktionieren des Binnenmarkts, zur Qualität und Kohärenz der Durchsetzung der Verbraucherschutzvorschriften, zum Monitoring des Schutzes der wirtschaftlichen Interessen der Verbraucher sowie zur Steigerung von Qualität und Kohärenz der Durchsetzung.“

[25] Falls nicht einige der in Artikel 13 der Richtlinie aufgeführten Ausnahmen gelten.

einschließlich Kontaktdaten der betreffenden zuständigen Behörde sowie einzelstaatlichen Einschränkungen des Auskunfts- und Informationsrechts zu finden sein.

Die Kommission hat einen Entwurf eines Datenschutzhinweises ausgearbeitet und dem EDSB übermittelt.

Der EDSB begrüßt die einschlägigen Bestimmungen in den CPC-Datenschutzleitlinien sowie die Ausarbeitung eines benutzerfreundlichen und informativen Datenschutzhinweises. Er fordert jedoch weitere Maßnahmen auf, mit denen gewährleistet wird, dass betroffene Personen wirksam über die Verarbeitung ihrer personenbezogenen Daten informiert werden.

Mit Blick auf den Entwurf des Datenschutzhinweises empfiehlt der EDSB Folgendes:

- Punkt 3.1 des Entwurfs (Daten, die von den Netzbehörden verarbeitet werden) sollte in Anbetracht von Punkt 1.3 der vorliegenden Stellungnahme dahin gehend geändert werden, dass die Art der verarbeiteten personenbezogenen Daten ausführlicher beschrieben wird, die sich nicht auf die Namen der Unternehmensleiter und Informationen in beigefügten Unterlagen beschränken;
- Punkt 5.2 (Zuständiger Verantwortlicher für die von der Kommission gespeicherten und verarbeiteten Daten) sollte im Lichte von Punkt 1.4 dieser Stellungnahme dahin gehend geändert werden, dass die Aufgaben und Verantwortlichkeiten der Kommission genauer beschrieben werden, die über die Verarbeitung von Kontaktinformationen für Sachbearbeiter hinausgehen und beispielsweise die Verantwortung der Kommission als Betreiberin des Systems umfassen;
- Punkt 9.2 (Beschwerden), zweiter Kugelpunkt, sollte dahin gehend abgeändert werden, dass nicht mehr angedeutet wird, dass Beschwerden gegen Tätigkeiten der zuständigen Behörden und der zentralen Verbindungsstellen ebenfalls beim EDSB einzureichen sind. Diese Beschwerden sind von den zuständigen Datenschutzbehörden in den Mitgliedstaaten zu bearbeiten;
- es könnten weitere Änderungen am Entwurf erforderlich werden, um auf die an anderer Stelle in dieser Stellungnahme vorgesehenen Garantien einzugehen (z. B. zu den Aufbewahrungsfristen und dem Verfahren zur Umsetzung des Auskunftsrechts der betroffenen Person);
- die Kommission sollte ihren Entwurf eines Datenschutzhinweises überarbeiten und ihn dann in einer hervorgehobenen Position so auf ihre Website stellen, dass betroffene Personen ihn leicht finden können (üblicherweise ganz oben auf der Leitseite).

Zweitens empfiehlt der EDSB der Kommission, so weit wie möglich in ihrer Eigenschaft als Betreiberin des CPCS eine proaktive Rolle bei der Aufklärung der zuständigen Behörden (oder zentralen Verbindungsstellen) über die Bedeutung der Bereitstellung eines Datenschutzhinweises zu spielen, damit diese Hinweise auf einzelstaatlicher Ebene gefördert werden.

Der EDSB begrüßt und unterstützt insbesondere Seminare und ähnliche bisher abgehaltene Veranstaltungen. Es hat sich ferner bewährt, auf der CPCS-Website der Kommission einen Link zu nationalen/lokalen Datenschutzhinweisen unterzubringen (und umgekehrt bei lokalen Hinweisen einen Link zum Hinweis der Kommission vorzusehen). In diesem Zusammenhang unterstreicht der EDSB erneut die wichtige koordinierende Rolle, die die zentralen Verbindungsstellen bei der Bereitstellung des Datenschutzhinweises in den einzelnen Mitgliedstaaten spielen können.

Schließlich weist der EDSB noch darauf hin, dass Informationen über das Internet zwar eine große Bedeutung zukommt, dass diese Informationen jedoch, sofern sie den jeweiligen betroffenen Personen nicht unmittelbar zur Kenntnis gebracht werden, einen unmittelbar den betroffenen Personen gegebenen Hinweis nicht ersetzen können.

So weit wie praktisch möglich sollte die Kommission daher bei den zuständigen Behörden über bewährte Verfahren zur unmittelbaren Bereitstellung des Datenschutzhinweises aufklären. Eine Möglichkeit zur Bereitstellung des Datenschutzhinweises bietet sich beispielsweise in der Ermittlungsphase, in der die ermittelnde Behörde den Vertreter eines verdächtigten Unternehmens über die gegen das Unternehmen laufenden Ermittlungen informiert. Bei dieser Gelegenheit könnte dem Verdächtigen auch mitgeteilt werden, dass personenbezogene Daten über CPCS ausgetauscht werden können, und ein Link zu der Online-Datenschutzerklärung angegeben (oder ein Exemplar der Erklärung übergeben) werden.

3.5. Rechte der betroffenen Person

Nach Artikel 12 der Richtlinie und dem entsprechenden Artikel 13 der Verordnung sind die für die Verarbeitung Verantwortlichen verpflichtet, der betroffenen Person auf deren Antrag Auskunft zu ihren personenbezogenen Daten zu erteilen, unrichtige Daten zu berichtigen und unter bestimmten Umständen Daten zu löschen. Gemäß Artikel 13 der Richtlinie und Artikel 20 der Verordnung sind gewisse Ausnahmen möglich.

3.5.1. Einschränkungen von Auskunftsrechten

Das Bestehen dieses Rechts sowie mögliche Ausnahmen können erhebliche Auswirkungen haben. Wichtig ist, dass nach den allgemeinen Vorschriften die betroffene Person das Recht hat, zu erfahren, ob ihre Geschäftstätigkeit als mutmaßlicher Verstoß gemeldet wurde. Je nach den Gegebenheiten kann die Inanspruchnahme dieses Rechts jedoch mit laufenden Ermittlungen kollidieren.

Gemäß Artikel 13 Absatz 4 der CPC-Verordnung erlassen die Mitgliedstaaten Rechtsvorschriften, die bei einer Ermittlung unter anderem das Auskunftsrecht der betroffenen Person (im Einklang mit der Richtlinie) beschränken können. Auch die Kommission kann (gemäß der Verordnung) gewisse Beschränkungen vornehmen.

Gestützt auf die vorstehenden Ausführungen wendet eine zuständige Behörde bei der Entscheidung über ein Auskunftsersuchen das eigene einzelstaatliche Recht an (das im Einklang mit der Richtlinie stehen sollte). Bedenkt man ferner, dass an jedem Informationsaustausch im CPCS mindestens zwei Parteien teilnehmen, und dass die einzelstaatlichen Rechtsvorschriften und Verfahren beim Datenschutz und beim Verbraucherschutz und seiner Durchsetzung noch nicht vollständig harmonisiert sind, kann es vorkommen, dass eine Behörde der betroffenen Person Auskunft über ihre personenbezogenen Daten geben möchte, die andere die Auskunft jedoch einschränkt.

Um die sich aus einer derartigen Situation ergebenden potenziellen Konflikte und Unstimmigkeiten möglichst gering zu halten, wäre ein koordinierter Ansatz wünschenswert. Die Koordinierung könnte bewirken, dass einerseits die Rechte der betroffenen Personen in vollem Umfang gewahrt werden und andererseits bei Bedarf angemessene Ausnahmen berücksichtigt werden, die im einzelstaatlichen Recht vorgesehen sind, und dass legitime Gründe für die Beschränkung des Auskunftsrechts eingehalten werden. Das ist nicht nur für

den Datenschutz von Bedeutung, sondern sorgt auch dafür, dass die zuständigen Behörden in den Mitgliedstaaten darauf vertrauen können, dass ihre legitimen Gründe für die Einschränkung respektiert werden, wenn von ihnen gelieferte Daten an andere Mitgliedstaaten übermittelt werden.

Im Ermangelung (oder Erwartung) einer weiteren Harmonisierung begrüßt der EDSB die Tatsache, dass die CPC-Datenschutzleitlinien Klarstellungen bieten und einen koordinierten Ansatz ermutigen.

So begrüßt der EDSB insbesondere, dass in den Leitlinien empfohlen wird, dem Antrag einer betroffenen Person erst stattzugeben, wenn die Behörden, deren Ermittlungen durch die Auskunft beeinträchtigt würden, dazu eine Stellungnahme abgeben konnten.

Der EDSB empfiehlt ein abgestuftes Vorgehen. So sollte insbesondere die zuständige Behörde, die über das Auskunftsersuchen entscheidet, weniger eine offizielle Genehmigung der anderen betroffenen Behörden einholen, als vielmehr in ihrem eigenen Entscheidungsprozess (so weit dies nach den eigenen einzelstaatlichen Rechtsvorschriften angemessen ist) berücksichtigen, dass eine Auskunft die von einer anderen zuständigen Behörde in einem anderen Mitgliedstaat durchgeführten Ermittlungen gefährden könnte.

Der EDSB unterstreicht ferner, dass die sorgfältige Prüfung der Auswirkungen auf Ermittlungen in anderen Mitgliedstaaten (das von der Kommission angeführte „Vorsichts"-Prinzip) nicht zu einem „Wettlauf nach unten" beim Datenschutz und zur Anpassung an die Gesetze der Mitgliedstaaten mit den restriktivsten Regelungen des Auskunftsrechts führen darf.

In Anbetracht dieser Ausführungen empfiehlt der EDSB der Kommission Folgendes:

- Annahme eigener Vorschriften für Einschränkungen bei an sie gerichteten Auskunftsersuchen;
- Zusammenarbeit mit Mitgliedstaaten, um in Erfahrung zu bringen, wie die Mitgliedstaaten Einschränkungen handhaben;
- so weit wie möglich Unterstützung eines koordinierten Ansatzes, wie er vorstehend skizziert wurde, und
- Unterstützung der Verbreitung der Ergebnisse dieser Übung bei den zuständigen Behörden und den betroffenen Personen.

3.5.2. Verfahren, mit dem betroffene Personen ihre Rechte ausüben können

Es ist nicht nur zu klären, ob Ausnahmen möglich sind, sondern es muss auch dafür gesorgt werden, dass die betroffenen Personen ihre Rechte leicht und unkompliziert wahrnehmen können.

In Anbetracht der Anzahl der für die Verarbeitung Verantwortlichen (Kommission, zentrale Verbindungsstellen, diverse zuständige Behörden), der Tatsache, dass jeder von ihnen Zugriff auf verschiedene Sätze personenbezogener Daten im CPCS hat und dass eine Vielzahl einzelstaatlicher Datenschutzvorschriften anzuwenden ist, ist eine Zuweisung der Verantwortung dafür, dass eine betroffene Person ihr Auskunftsrecht wahrnehmen kann, besonders schwierig. Dies gilt umso mehr, als sich – wie vorstehend beschrieben – die Auskunftserteilung durch einen CPCS-Nutzer in einem Mitgliedstaat auf die Vertraulichkeit von Ermittlungen in einem anderen Mitgliedstaat auswirken kann. Bei der Erteilung von Auskünften müssen daher unter Umständen mehrere Parteien zusammenarbeiten.

In der Praxis kann eine betroffene Person Auskunft über ihre personenbezogenen Daten sowie deren Berichtigung und Löschung bei jeder der folgenden Stellen verlangen:

- der zuständigen Behörde, die die Daten hochgeladen hat;
- einer anderen zuständigen Behörde, die Zugriff auf die Daten hat;
- der Kommission.

Möglich ist auch, dass eine betroffene Person Auskunft von einem für die Verarbeitung Verantwortlichen fordert, der gar keinen Zugriff auf die geforderten Informationen hat (weil er z. B. eine Warnmeldung nicht erhalten hat oder weil er an einer koordinierten Ermittlung nicht beteiligt war).

Die CPC-Datenschutzleitlinien besagen, dass die Kommission einem Antrag auf Auskunft nur bei Daten stattgeben darf, zu denen die Kommission (also die CPCS-Nutzer bei der Kommission) Zugang hat (in den meisten Fällen ist dies auf Warnmeldungen und Mitteilungen beschränkt; vgl. Punkt 1.4).

Der EDSB begrüßt die Klarstellungen in den Leitlinien. Dennoch sind weitere Klarstellungen erforderlich. So wären insbesondere die praktischen Aspekte der Wahrnehmung des Auskunftsrechts genauer festzulegen, damit dem Ersuchen der betroffenen Person wirksam, einfach, vorhersehbar und zügig nachgekommen werden kann und damit sowohl für die betreffenden für die Verarbeitung Verantwortlichen als auch für die betroffenen Personen ein möglichst geringer Verwaltungsaufwand und keine Schwierigkeiten entstehen.

Das Verfahren sollte ferner in einer den betroffenen Personen leicht zugänglichen Datenschutzerklärung transparent beschrieben werden. So muss klar gesagt werden, an wen die betroffenen Personen ihren Antrag richten, wer über den Antrag entscheidet und welches Recht hierbei anzuwenden ist.

Schließlich sollte aus praktischen Erwägungen die Koordinierung auch dafür sorgen, dass nach Möglichkeit die betroffenen Personen nicht an alle zuständigen Behörden, die das CPCS nutzen und Zugriff auf personenbezogene Daten haben könnten, jeweils einen Antrag zu stellen haben. In Anbetracht der Tatsache, dass derzeit mehr als 300 zuständige Behörden im CPCS registriert sind, könnte dies einen übermäßigen Aufwand bei der Wahrnehmung eines Grundrechts bedeuten.

Im Sinne eines möglichst geringen Verwaltungsaufwands und einer reibungslosen Zusammenarbeit empfiehlt der EDSB die Unterstützung der Zusammenarbeit durch ein IT-Tool, das Bestandteil des unter Punkt 3.2.2 erwähnten Datenschutzmoduls sein könnte. Diese Funktionalität könnte insbesondere eingesetzt werden, um Auskunftsersuchen in Fällen zu bearbeiten und weiterzuleiten, bei denen eine Auskunft über die Daten sich auf die Ermittlungen von zwei oder mehr zuständigen Behörden auswirken könnte. Darüber hinaus kann sie dabei helfen, Ersuchen an andere relevante zuständige Behörden in Fällen weiterzuleiten, in denen die von der betroffenen Person angesprochene zuständige Behörde keinen Zugriff auf alle sie betreffenden Daten im CPCS hat. Eine solche Funktionalität könnte sich als besonders hilfreich erweisen, wenn das CPCS stärker genutzt wird und die Zahl der Auskunftsersuchen steigt.

Der EDSB schließt jedoch andere Koordinierungsmethoden (ohne Einsatz des IT-Tools) nicht aus, solange das entsprechende Verfahren den betroffenen Personen eine praktikable Lösung bei der Wahrnehmung ihrer Rechte bietet. Sollte Bedarf an einer effizienteren Koordinierung

entstehen, könnte die Integration dieser Funktionalität in das CPCS als zweiter Schritt in Erwägung gezogen werden. Um sicherzustellen, dass bei neuem Bedarf auch weitere Entwicklungen vorgenommen werden, empfiehlt der EDSB der Kommission, Statistiken über die Zahl der bei den zuständigen Behörden gestellten Auskunftsersuchen über Daten zu führen, die über das CPCS ausgetauscht werden. Dort wäre auch die Zeit zu erfassen, die bis zur Erledigung eines Antrags vergeht.

3.6. Vertraulichkeit und Sicherheit der Verarbeitung

[...]

4. Schlussfolgerungen

Der EDSB begrüßt, dass sich das CPCS auf eine Rechtsgrundlage wie die CPC-Verordnung stützt und dass dieser Rechtstext im Verlauf der Zeit durch die CPC-Durchführungsentscheidung und die CPC-Datenschutzleitlinien ergänzt worden ist, die nähere Einzelheiten der Verarbeitung sowie besondere Datenschutzgarantien enthalten. Der EDSB erkennt ferner die auf praktischer Ebene erledigten Arbeiten im Hinblick auf Sicherheit und Funktionalitäten des CPCS an.

Insgesamt gibt es nach Auffassung des EDSB keinen Grund zu der Annahme, dass ein Verstoß gegen die Verordnung vorliegt, sofern die in dieser Stellungnahme formulierten Empfehlungen umgesetzt werden:

- zur Datenqualität: 1) Die CPCS-Systemarchitektur sollte weiterhin so konfiguriert werden, dass sie weitestgehend die Einhaltung der Datenschutzvorschriften erleichtert, und 2) die Kommission sollte mit ihren Aktivitäten fortfahren, damit die Nutzer des Systems angemessen geschult und angeleitet werden und die Befugnis erhalten, in Fragen des Datenschutzes Entscheidungen zu treffen;
- zur Aufbewahrungsfrist: 1) sofern keine Ermittlungs- oder Durchsetzungsmaßnahme läuft, sollten Warnmeldungen innerhalb einer angemessenen Frist nach ihrer Ausgabe zurückgezogen und gelöscht werden (der EDSB empfiehlt eine Frist von sechs Monaten, falls es keine stichhaltigen Gründe für eine andere Frist gibt); die Kommission sollte: 2) den Zweck der Aufbewahrungsfrist von fünf Jahren näher erläutern, 3) prüfen, ob die gleichen Ziele nicht auch mit einer kürzeren Aufbewahrungsfrist zu erreichen sind, und 4) der Frage nachgehen, ob wirklich alle der derzeit vorgesehenen Informationen gespeichert werden müssen oder ob auch ein Teil dieser Informationen genügen würde.
- die Kommission sollte ihren Entwurf einer Datenschutzerklärung überarbeiten und an hervorgehobener Position in ihre Website stellen und bei den zuständigen Behörden (oder zentralen Verbindungsstellen) über die Bedeutung der Bereitstellung des Datenschutzhinweises aufklären, um so die Bereitstellung dieses Hinweises auf einzelstaatlicher Ebene zu fördern;
- es sollten weitere Maßnahmen ergriffen werden, um den betroffenen Personen die Wahrnehmung ihres Rechts auf Auskunft über ihre Daten sowie auf Berichtigung und Löschung ihrer Daten zu erleichtern. Zur leichteren Koordinierung sollte ein Datenschutzmodul im CPCS in Erwägung gezogen werden.

- *[...]*.

Brüssel, den 4. Mai 2011

(**unterzeichnet**)

Giovanni Buttarelli
Stellvertretender Europäischer Datenschutzbeauftragter