STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zum Beschluss der Kommission 2011/141/EU zur Änderung der Entscheidung der Kommission 2007/76/EG über das System zur Zusammenarbeit im Verbraucherschutz („CPCS") und zur Empfehlung der Kommission 2011/136/EU hinsichtlich der Leitlinien für die Anwendung der Datenschutzbestimmungen im CPCS

(2011/C 217/06)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [1],

gestützt auf das dem Europäischen Datenschutzbeauftragten übermittelte Ersuchen um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr [2] —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1. Am 1. März 2011 nahm die Europäische Kommission den Beschluss der Kommission zur Änderung der Entscheidung 2007/76/EG über das CPCS („zweite CPC-Änderung") an [3]. Gleichzeitig nahm die Kommission eine Empfehlung der Kommission zu Leitlinien für die Anwendung der Datenschutzbestimmungen im CPCS („CPC-Datenschutzleitlinien") an [4]. Beide Dokumente wurden dem EDPS gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 zur Konsultation übermittelt.

2. Das CPCS ist ein Informationstechnologiesystem, das von der Kommission gemäß der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz („CPC-Verordnung") entworfen wurde und betrieben wird. Das CPCS erleichtert die Zusammenarbeit im Verbraucherschutz zwischen den „zuständigen Behörden" in den EU-Mitgliedstaaten und der Kommission im Hinblick auf Verstöße gegen eine vordefinierte Reihe von EU-Richtlinien und Verordnungen. Um in den Geltungsbereich der CPC-Verordnung zu fallen, müssen die Verstöße grenzüberschreitenden Charakter besitzen und die „Kollektivinteressen der Verbraucher" schädigen.

3. Im Rahmen ihrer Zusammenarbeit tauschen CPCS-Nutzer Informationen einschließlich personenbezogener Daten aus. Diese personenbezogenen Daten können sich auf Direktoren oder Mitarbeiter eines Verkäufers oder Dienstleistungserbringers beziehen, die eines Verstoßes verdächtigt werden, auf den Verkäufer oder den Dienstleistungserbringer selbst (falls es sich um eine Einzelperson handelt), sowie auf Dritte, wie Verbraucher oder Beschwerdeführer.

4. Das System wurde als sicheres Kommunikationsmittel zwischen den zuständigen Behörden sowie als Datenbank entworfen. Das CPCS wird von den zuständigen Behörden für Informationsersuchen im Rahmen der Ermittlung eines Falls [5] oder für Durchsetzungsersuchen [6] verwendet („Amtshilfeersuchen"). Zudem können zuständige Behörden eine Warnmeldung übermitteln, mit der andere zuständige Behörden und die Kommission über einen Verstoß oder einen mutmaßlichen Verstoß [7] informiert werden. Das

[1] ABI. L 281 vom 23.11.1995, S. 31.
[2] ABI. 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 (2011/141/EU) (ABI. L 59 vom 4.3.2011, S. 63).
[4] Empfehlung der Kommission vom 1. März 2011: Leitlinien für die Anwendung der Datenschutzbestimmungen im System zur Zusammenarbeit im Verbraucherschutz (CPCS) (2011/136/EU) (ABI. L 57 vom 2.3.2011, S. 44).
[5] Siehe Artikel 6 der CPC-Verordnung über „Informationsaustausch auf Ersuchen".
[6] Siehe Artikel 8 der CPC-Verordnung über „Durchsetzungsersuchen".
[7] Siehe Artikel 7 der CPC-Verordnung über „Informationsaustausch ohne Ersuchen".

CPCS beinhaltet ebenfalls weitere Funktionen, einschließlich eines Meldesystems ([8]) und eines Forums für den Austausch von Daten, die nicht mit einem bestimmten Fall verbunden sind.

5. In der vorliegenden Stellungnahme behandelt der EDSB eine Reihe von Datenschutzfragen im Hinblick auf den Rechtsrahmen für das CPCS und konzentriert sich hierbei in erster Linie auf die vor kurzem angenommene zweite CPC-Änderung. Zudem zieht der EDBS Bilanz aus dem bisher erreichten Fortschritt und zeigt einige noch verbliebene Bedenken sowie Erwägungen für die Zukunft auf. Ferner nimmt er Stellung zu verschiedenen Bestimmungen der CPC-Datenschutzleitlinien.

6. Parallel zu der vorliegenden Stellungnahme (die gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001) angenommen wird) erstellt der EDBS in seiner Aufsichtsfunktion ebenfalls eine Stellungnahme zur Vorabkontrolle (gemäß Artikel 27 derselben Verordnung) („Stellungnahme zur Vorabkontrolle"). Die Stellungnahme zur Vorabkontrolle enthält eine detailliertere Beschreibung des CPCS sowie der Verarbeitung personenbezogener Daten mithilfe des Systems. In seiner Stellungnahme zur Vorabkontrolle konzentriert sich der EDBS auf die Empfehlung spezifischer Maßnahmen, die auf der praktischen, technischen und organisatorischen Ebene zu ergreifen sind, um die Einhaltung des Datenschutzes innerhalb des CPCS zu verbessern. Unter Berücksichtigung dessen, dass die CPC-Datenschutzleitlinien mit diesen spezifischen Maßnahmen ebenfalls eng verbunden sind, wird in der Stellungnahme zur Vorabkontrolle ebenfalls zu verschiedenen Bestimmungen der Leitlinien Stellung bezogen.

II. DER RECHTSRAHMEN FÜR DAS CPCS

7. Der EDBS begrüßt, dass das CPCS auf einer soliden Rechtsgrundlage basiert, insbesondere auf einer vom Rat und dem Parlament angenommenen Verordnung. Zudem äußert der EDBS seine Zufriedenheit darüber, dass die Rechtsgrundlage mit der Zeit ergänzt wurde, um weitere Einzelheiten zu regeln und Bedenken im Hinblick auf den Datenschutz auszuräumen. Insbesondere begrüßt der EDBS, dass die Entscheidung der Kommission 2007/76/EG vom 22. Dezember 2006 zur Durchführung der CPC-Verordnung („CPC-Durchführungsbeschluss") angenommen wurde und nachfolgend am 17. März 2008 sowie vor kurzem, am 1. März 2011, mittels der zweiten CPC-Änderung geändert wurde. Er begrüßt ebenfalls, dass die Kommission die CPC-Datenschutzleitlinien angenommen hat, in denen insbesondere auf Datenschutzprobleme eingegangen wird.

8. Obwohl der EDSB bedauert, dass er nicht zu dem Zeitpunkt konsultiert wurde, als die CPC-Verordnung und des CPC-Durchführungsbeschlusses ursprünglich angenommen wurde, begrüßt er, dass er von der Kommission anlässlich der Annahme der beiden Änderungen des CPC-Durchführungsbeschlusses sowie der CPC-Datenschutzleitlinien konsultiert wurde. Der EDBS begrüßt außerdem, dass die Kommission zuvor ebenfalls die Artikel-29-Datenschutzgruppe („WP 29") konsultierte, die am 21. September 2007 ihre Stellungnahme Nr. 6/2007 (WP 139) abgegeben hat. Schließlich begrüßt der EDBS den Umstand, dass in den Erwägungsgründen der CPC-Datenschutzleitlinien Bezug auf diese Konsultationen genommen wird.

9. Der EDSB stellt fest, dass i) die Empfehlungen des EDSB, die in einem vorhergehenden, informellen Austausch erteilt worden waren, ebenso wie die Empfehlungen der WP 29 in der Stellungnahme Nr. 6/2007 von der Kommission sorgfältig berücksichtigt wurden und dass ii) zahlreiche dieser Empfehlungen bei der Weiterentwicklung des Rechtsrahmens für das CPCS und/oder auf der praktischen, technischen und organisatorischen Ebene befolgt wurden. Die Anmerkungen des EDSB in der vorliegenden Stellungnahme sowie in seiner Stellungnahme zur Vorabkontrolle sollten vor diesem positiven Hintergrund gesehen werden.

III. DATENSCHUTZPROBLEME IM ZUSAMMENHANG MIT DER ZWEITEN CPC-ÄNDERUNG

3.1 Aufbewahrung personenbezogener Daten im CPCS

3.1.1 *Einleitung*

10. Als Vorbemerkung weist der EDSB darauf hin, dass die Frage des Abschlusses von Fällen und der Aufbewahrungsfrist in der CPC-Verordnung nicht angemessen und umfassend behandelt wurde ([9]).

11. Tatsächlich sind in der CPC-Verordnung nur zwei spezifische Vorschriften bezüglich der Löschung, jedoch keine Vorschrift bezüglich des Abschlusses von Fällen festgelegt ([10]). Erstens wird gefordert, dass wenn eine Warnmeldung „sich als unbegründet erweist", diese von der zuständigen Behörde zurückgezogen und die Information durch die Kommission unverzüglich aus der Datenbank entfernt werden sollte. Zweitens wird gefordert, dass wenn eine zuständige Behörde gemäß Artikel 8 Absatz 6 der CPC-Verordnung mitteilt, dass ein Verstoß eingestellt wurde, die gespeicherten Daten fünf Jahre nach der Benachrichtigung gelöscht werden sollten.

12. Die CPC-Verordnung legt für die fünfjahrige Aufbewahrungsfrist keinen Zweck fest. Ebenso wenig finden sich zusätzliche Erläuterungen dazu, wie und wann zu beurteilen ist, ob eine Warnmeldung „unbegründet" ist. Ferner enthält die CPC-Verordnung keine Angaben darüber, wie lange die Informationen in Fällen, die nicht von den soeben erwähnten spezifischen Vorschriften abgedeckt sind, in der

([8]) Siehe Artikel 7 Absatz 2 und Artikel 8 Absatz 6 der CPC-Verordnung.

([9]) Siehe ebenfalls Stellungnahme Nr. 6/2007 der Artikel-29-Datenschutzgruppe (auf die in Teil II weiter oben Bezug genommen wird).

([10]) Siehe Artikel 10 Absatz 2 der CPC-Verordnung.

Datenbank verbleiben sollten (d. h. die Verordnung legt nicht fest, wie lange Amtshilfeersuchen in der Datenbank gespeichert werden, wenn diese nicht zu erfolgreichen Durchsetzungmaßnahmen geführt haben, durch die der Verstoß eingestellt worden wäre).

13. Der EDSB begrüßt, dass mit dem CPC-Durchführungsbeschluss in der geänderten Fassung und den CPC-Datenschutzleitlinien versucht wird, zusätzliche Klarstellungen bereitzustellen. Nichtsdestotrotz hegt der EDSB immer noch Bedenken hinsichtlich verschiedener Aspekte der Vorschriften für den Abschluss von Fällen und die Datenaufbewahrung im CPCS, wie weiter unten in den Abschnitten 3.1.2 bis 3.1.4 erörtert wird.

14. Der EDPS empfiehlt, dass diese Bedenken bei der nächsten Überarbeitung des Rechtsrahmens für das CPCS mittels einer weiteren Änderung des CPC-Durchführungsbeschlusses oder vorzugsweise mittels einer Änderung der CPC-Verordnung selbst behandelt werden.

15. Bis eine solche gesetzgeberische Maßnahme möglich wird, empfiehlt der EDSB, dass die Bedenken hinsichtlich der Aufbewahrungszeiträume auf der praktischen, technischen und organisatorischen Ebene behandelt werden und zudem in dem Dokument „Consumer Protection Cooperation Network: Operating Guidelines“ (Netzwerk für die Zusammenarbeit im Verbraucherschutz: operative Leitlinien), auf das im Abschnitt 3.1.2 weiter unten Bezug genommen wird, klar dargelegt werden.

3.1.2 *Rechtzeitiger Abschluss der Fälle*

16. In der zweiten CPC-Änderung wird versäumt, eine Frist festzulegen, innerhalb der ein Fall im Rahmen eines Amtshilfeersuchens (Informationsersuchen oder Durchsetzungsersuchen) abgeschlossen werden muss.

17. In seiner Stellungnahme zur Vorabkontrolle vermerkt der EDSB eine Reihe pragmatischer Maßnahmen, die zum aktuellen Zeitpunkt von der Kommission durchgeführt werden, um zu gewährleisten, dass ruhende Fälle rechtzeitig abgeschlossen werden.

18. In der vorliegenden Stellungnahme empfiehlt der EDSB, dass maximale Fristen für Informationsersuchen und Durchsetzungsersuchen festgelegt werden sollten. Diese sollten bei der nächsten Überarbeitung der Rechtsgrundlage bestimmt werden. Die Fristen sollten mit der Art des Falls sowie mit der entsprechenden Aktivität verknüpft werden. Gleichzeitig sollten die Vorschriften den zuständigen Behörden ebenfalls die Flexibilität gestatten, die Fälle bei Vorliegen von berechtigten Gründen zu verlängern, um zu gewährleisten, dass Fälle nicht vorzeitig geschlossen werden, auch dann nicht, wenn ein komplexer Fall für einen Abschluss mehr Zeit als durchschnittlich benötigt.

19. Um dies zu ermöglichen, empfiehlt der EDSB, das Dokument „Consumer Protection Cooperation Network: Operating Guidelines“ (Netzwerk für die Zusammenarbeit im Verbraucherschutz: operative Leitlinien), das vom CPC-Ausschuss am 6. Dezember 2010 bestätigt wurde, als Ausgangspunkt zu verwenden. In den operativen Leitlinien werden unter Punkt 2.7 unter dem Titel „Phasen und Fristen für CPC-Fälle“ typische Fallverläufe erörtert und es wird dargelegt, dass Informationsersuchen im Durchschnitt innerhalb einer Frist von ein bis drei Monaten bearbeitet werden sollten. Die Bearbeitung von Durchsetzungsersuchen sollte gemäß der operativen Leitlinien innerhalb einer durchschnittlichen Frist von sechs bis neun Monaten möglich sein (außer in Fällen von gerichtlichen Verfügungen oder in Fällen von Rechtsmitteln gegen eine Verwaltungsentscheidung, für die ein Jahr und länger eher realistisch ist).

3.1.3 *Warnmeldungen*

20. Mit der zweiten CPC-Änderung wurde ein neuer Absatz in Punkt 2.2.2 des Anhangs des CPC-Durchführungsbeschlusses eingefügt, in dem gefordert wird, dass „begründete“ Warnmeldungen fünf Jahre nach deren Erstellung aus der Datenbank entfernt werden sollten (im Hinblick auf „unbegründete“ Warnmeldungen fordern die aktuellen Bestimmungen bereits eine Löschung, sobald „sich eine Warnmeldung als unbegründet erweist“).

21. Um diese neue Bestimmung in einen Zusammenhang zu stellen, betont der EDSB, dass eines seiner Hauptanliegen in der Gewährleistung besteht, personenbezogene Daten nicht länger als erforderlich in der CPCS-Datenbank aufzubewahren. Hier handelt es sich um eine sensible Frage insbesondere im Hinblick auf Warnmeldungen (für die eine größere Zahl an Empfängern besteht, als für den bilateralen Austausch), und zwar insbesondere im Hinblick auf Warnmeldungen im Zusammenhang mit mutmaßlichen Verstößen. In der Praxis könnte das Fehlen von klaren Fristen für die Aufrechterhaltung von Warnmeldungen bedeuten, dass bestimmte Warnmeldungen für einen unangemessen langen Zeitraum aufrechterhalten werden (so lange nicht nachgewiesen wird, dass sie eindeutig unbegründet sind). Solche auf einem unbestätigten Verdacht basierenden Handlungen würden für das Grundrecht des Datenschutzes sowie für andere Grundrechte, wie die Unschuldsvermutung, erhebliche Risiken darstellen.

22. Vor diesem Hintergrund begrüßt der EDSB, dass eine Aufbewahrungsfrist für Warnmeldungen festgelegt wurde. Der EDSB ist allerdings der Ansicht, dass die Kommission keine ausreichende Begründung zum Nachweis dessen bereitgestellt hat, dass eine Aufbewahrungsfrist von fünf Jahren angemessen ist. Der EDSB empfiehlt, dass die Kommission eine Verhältnismäßigkeitsbewertung durchführt und die Länge der Aufbewahrungszeiträume für Warnmeldungen neu bewertet. Grundsätzlich sollten alle Warnmeldungen sehr viel früher aus der Datenbank gelöscht werden, es sei denn, eine Warnmeldung über einen Verstoß oder einen mutmaßlichen Verstoß hatte ein Amtshilfeersuchen zur Folge und die grenzübergreifende Ermittlung oder Durchsetzungsmaßnahme ist noch nicht abgeschlossen. Die Aufbewahrungsfrist sollte lange genug sein, um den einzelnen Behörden, die die Nachricht erhalten, die Entscheidung zu ermöglichen, ob weitere Ermittlungsschritte oder Durchsetzungsmaßnahmen eingeleitet werden oder ob ein Amtshilfeersuchen über das CPCS übermittelt werden soll. Allerdings sollte die Aufbewahrungsfrist ausreichend kurz sein, um das Risiko, dass Warnmeldungen für die Erstellung von schwarzen Listen oder Data Mining missbraucht werden, zu minimieren.

23. Vor diesem Hintergrund empfiehlt der EDSB, dass die Kommission den Rechtsrahmen überprüfen sollte, um sicherzustellen, dass Warnmeldungen spätestens sechs Monate nach dem Hochladen gelöscht werden, es sei denn, dass eine andere, angemessenere Aufbewahrungsfrist gerechtfertigt werden kann.

24. Hierdurch sollte insbesondere gewährleistet werden, dass in Fällen, in denen sich ein Verdacht nicht bestätigt hat (oder nicht einmal weiter ermittelt wurde), unschuldige, mit dem Verdacht verbundene Einzelpersonen nicht während eines unangemessen langen Zeitraums auf einer „schwarzen Liste" geführt und „für verdächtig" gehalten werden, was nicht in Übereinstimmung mit Artikel 6 Buchstabe e der Richtlinie 95/46/EG stünde.

25. Diese Einschränkung ist ebenso notwendig, um den Grundsatz der Datenqualität (siehe Artikel 6 Buchstabe d der Richtlinie 95/46/EG) und andere wichtige Rechtsgrundsätze zu gewährleisten. Dies könnte nicht nur zu einem angemesseneren Schutzniveau für den Einzelnen führen, sondern gleichzeitig den Durchsetzungsbeamten ermöglichen, sich wirksamer auf die relevanten Fälle zu konzentrieren.

3.1.4 *Aufbewahrungsfrist für abgeschlossene Amtshilfeersuchen*

26. Mit der zweiten CPC-Änderung wurde ein neuer Absatz zu Punkt 2.15 des Anhangs des CPC-Durchführungsbeschlusses hinzugefügt, in dem Folgendes gefordert wird: „Alle sonstigen Informationen, die in Verbindung mit Amtshilfeersuchen gemäß Artikel 6 der Verordnung (EG) Nr. 2006/2004 stehen, werden fünf Jahre nach Abschluss des Falls aus der Datenbank gelöscht."

27. Mit dem bestehenden Text zusammen gelesen wird im geänderten Punkt 2.15 gefordert, dass nach dem Abschluss des Falls die Aufbewahrungsfrist für sämtliche ausgetauschten Informationen gemäß Artikel 6 fünf Jahre beträgt, mit Ausnahme der folgenden Fälle:

— wenn unrichtige Daten gelöscht werden,

— wenn die ausgetauschten Informationen keine Warnmeldung und kein Durchsetzungsersuchen gemäß Artikel 8 nach sich ziehen oder

— wenn feststeht, dass kein Verstoß im Sinne der CPC-Verordnung vorliegt.

28. Tatsächlich scheint, wie in der Stellungnahme zur Vorabkontrolle ausgeführt wird, die „Standardaufbewahrungszeit" nach Abschluss eines Falls (in Abhängigkeit von bestimmten Ausnahmen) sowohl für Informationsersuchen als auch für Durchsetzungsersuchen fünf Jahre zu betragen.

29. Der Text des CPC-Durchführungsbeschlusses in der durch die zweite CPC-Änderung geänderten Fassung scheint nicht vollständig mit der CPC-Verordnung übereinzustimmen. Insbesondere Artikel 10 Absatz 2 der CPC-Verordnung unterscheidet zwischen einem Informationsaustausch, der zu einer erfolgreichen Durchsetzung führt (d. h. Fälle, in denen die Verstöße aufgrund der ergriffenen Durchsetzungsmaßnahmen eingestellt wurden) einerseits und Informationen, die nicht zu einer erfolgreichen Durchsetzung führen, andererseits. Im ersten Fall ist nach Abschluss des Falls eine Aufbewahrungsfrist von fünf Jahren vorgesehen. Für den letzteren Fall wurden keine spezifischen Bestimmungen festgelegt (außer, dass unbegründete Warnmeldungen zurückgezogen und gelöscht werden sollten).

30. Mit anderen Worten fordert die CPC-Verordnung eine Aufbewahrungsfrist von fünf Jahren nach Abschluss eines Falls nur unter der Voraussetzung, dass Durchsetzungsmaßnahmen ergriffen wurden und dass diese hinsichtlich der Einstellung von Verstößen erfolgreich waren.

31. Obwohl der EDSB hinsichtlich des Zwecks und der Verhältnismäßigkeit der Aufbewahrung von Daten während einer Frist von fünf Jahren nach Abschluss des Falles Zweifel hegt (siehe Anmerkungen im vorliegenden Abschnitt 3.1.4 weiter unten), folgt die Unterscheidung zwischen Fällen, die zu einer erfolgreichen Durchsetzung führten und Fällen, bei denen dies nicht der Fall war, vom Standpunkt des Datenschutzes aus einer gewissen Logik. Insbesondere birgt die Aufbewahrung von Daten im Zusammenhang mit einem bloßen Verdacht über einen langen Zeitraum eine höhere Wahrscheinlichkeit der Unrichtigkeit und zudem das Risiko, dass andere wichtige Rechtsgrundsätze verletzt werden. Daher kann allgemein festgestellt werden, dass die Aufbewahrung solcher Daten während eines langen Zeitraums mit einer höheren Wahrscheinlichkeit zu Datenschutzproblemen führt, als die Aufbewahrung von Daten im Zusammenhang mit tatsächlichem Fehlverhalten, das angemessen nachgewiesen wurde und zu Durchsetzungsmaßnahmen führte.

32. Im Gegensatz zu der CPC-Verordnung scheint der CPC-Durchführungsbeschluss in seiner geänderten Fassung zumindest in bestimmten Fällen zu ermöglichen, die Aufbewahrungsfrist von fünf Jahren ebenfalls auf Informationen anzuwenden, die nicht zu erfolgreichen Durchsetzungsmaßnahmen geführt haben.

33. Gemäß dem CPC-Durchführungsbeschluss scheint beispielsweise ein Informationsersuchen, das zwar zu einer Warnmeldung, jedoch nicht zu einer Durchsetzungsmaßnahme führte, nach „Abschluss des Falls" über einen Zeitraum von fünf Jahren im System zu verbleiben.

34. Die CPC-Verordnung und der CPC-Durchführungsbeschluss scheinen somit jeweils einen etwas anderen Ansatz zu verfolgen. Der CPC-Durchführungsbeschluss, der in einem bestimmten Umfang die Bestimmungen der CPC-Verordnung widerspiegelt, führt zugleich wichtige zusätzliche Vorschriften für die Datenaufbewahrung ein. Während eine Klarstellung der Vorschriften als solche begrüßt wird, stellt der EDSB die Rechtmäßigkeit der Festlegung längerer Aufbewahrungsfristen, die nicht bereits in der CPC-Verordnung gefordert wurden, in Frage. Dies würde dem Grundrecht auf Datenschutz weitere Einschränkungen auferlegen, und zwar durch die Umsetzung einer Gesetzgebung, die im Gegensatz zu der CPC-Verordnung und den anwendbaren Datenschutzvorschriften steht.

35. In Übereinstimmung mit den vorhergehenden Ausführungen empfiehlt der EDSB, dass die Kommission den Rechtsrahmen überprüft und erneut abwägt, ob die Aufbewahrungsfrist von fünf Jahren über die Fälle, bei denen gemäß der CPC-Verordnung eine erfolgreiche Durchsetzung erfolgte, hinausgehend auch auf alle anderen Fälle angewandt werden sollte.

36. Zudem äußert der EDSB seine Zufriedenheit darüber, dass die CPC-Datenschutzleitlinien darauf abzielen, den Zweck der Aufbewahrung nach Abschluss des Falls festzulegen. Hierbei handelt es sich um eine wichtige Frage, deren Behandlung sowohl in der CPC-Verordnung als auch in der zweiten CPC-Änderung versäumt wird. Insbesondere ist in den CPC-Datenschutzleitlinien Folgendes festgelegt: „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“ ([11]).

37. Während diese Klarstellung begrüßt wird, ist der EDSB jedoch aufgrund des Fehlens einer weiteren Begründung für die Notwendigkeit dieser Vorgehensweise nicht von der Angemessenheit und der Zulänglichkeit dieses Zwecks zur Rechtfertigung einer fünfjährigen Aufbewahrungsfrist überzeugt. Daher empfiehlt der EDPS, dass die Kommission:

— klarstellen sollte, welches der Zweck einer fünfjährigen Datenaufbewahrung ist;

— bewerten sollte, ob mit einer kürzeren Aufbewahrungsfrist dieselben Ziele erreicht werden können und

— bewerten sollte, ob alle aktuell vorgesehenen Informationen gespeichert werden müssen oder ob eine Teilmenge der Informationen ausreichen würde (d. h., es sollte untersucht werden, ob die ausschließliche Speicherung von Meldungen gemäß Artikel 8 Absatz 6 ausreichend wäre; es sollte ebenfalls gesondert überprüft werden, ob die Speicherung der Namen von Direktoren oder von Anhängen, die gegebenenfalls personenbezogene Daten enthalten, notwendig ist; es sollte ebenfalls unterschieden werden zwischen Daten, die sich auf mutmaßliche Verstöße bzw. auf „nachgewiesene“ Verstöße beziehen).

3.2 **Der Zugang der Kommission zu Daten im CPCS**

38. Der EDSB äußert seine Zufriedenheit darüber, dass (durch die Einführung eines neuen Punkts 4.3 im Anhang des CPC-Durchführungsbeschlusses) die zweite CPC-Änderung den Zugang der Kommission zu den Daten im CPCS verdeutlicht und dass dieser Zugang eindeutig und spezifisch auf die Informationen beschränkt ist, die gemäß der CPC-Verordnung erforderlich sind. Insbesondere begrüßt der EDSB, dass die Kommission keinen Zugang zu vertraulicher Kommunikation zwischen den zuständigen Behörden in den Mitgliedstaaten, wie beispielsweise zu Amtshilfeersuchen, erhalten hat.

39. Diese Klarstellung und Einschränkung sind besonders wichtig in Anbetracht dessen, dass ein Mangel an Klarheit zu einer Situation hätte führen können, in der die Kommission in der Lage gewesen wäre, auf Informationen einschließlich personenbezogener Daten zuzugreifen, die ausschließlich für die zuständigen Behörden in den Mitgliedstaaten bestimmt sind.

40. In Abschnitt 5 der CPC-Datenschutzleitlinien wird ausgeführt: „Dieses Zugriffsrecht dient der Kommission dazu, die Anwendung der Verordnung über die Zusammenarbeit und die Anwendung der im Anhang der Verordnung aufgeführten Verbraucherschutzvorschriften zu kontrollieren und entsprechende Statistiken zu erstellen.“

41. Dies bedeutet nicht, dass die Kommission zu sämtlichen Informationen, die innerhalb des CPCS zwischen den Mitgliedstaaten ausgetauscht werden, Zugang haben sollte.

42. Tatsächlich betont der EDSB, dass der Zugang zu Datenbanken wie dem CPCS unter die Definition der Verarbeitung personenbezogener Daten fällt. Gemäß Artikel 5 Buchstabe a der Verordnung (EG) Nr. 45/2001, der für die Zugriffsrechte der Kommission im CPCS relevant ist, dürfen Organe lediglich dann personenbezogene Daten verarbeiten, wenn dies für die Wahrnehmung einer Aufgabe im öffentlichen Interesse notwendig ist, und weiterhin vorausgesetzt, dass die Verarbeitung auf den Verträgen oder auf abgeleitetem Recht basiert.

([11]) Siehe Abschnitt 8 der Leitlinien, „Einige zusätzliche Hinweise; Warum beträgt die Aufbewahrungsfrist fünf Jahre?“ Die CPC-Datenschutzleitlinien fügen ebenfalls hinzu: „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.“

43. Der EDSB versteht unter diesen Anforderungen, die sich direkt aus dem in Artikel 8 der Europäischen Menschenrechtskonvention und in Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union verankerten Recht auf Datenschutz ergeben, dass die Kommission lediglich über eine Zugriffsbefugnis auf die Informationssysteme der Mitgliedstaaten verfügen kann, falls dies in spezifischen gesetzlichen Bestimmungen festgelegt ist, die auf einer voll und ganz angemessenen Rechtsgrundlage (in der Regel dem ordentlichen Gesetzgebungsverfahren) basieren. Rechtssicherheit und Transparenz sind die beiden zugrunde liegenden Werte, aus denen hervorgeht, warum eine spezifische und sichere Rechtsgrundlage für den Zugang der Kommission eine besonders wichtige Garantie für die Gewährleistung der Grundrechte der Einzelpersonen im Hinblick auf den Datenschutz darstellt.

44. Weder die allgemeine Überwachungsbefugnis der Kommission als „Hüterin des Vertrags", noch die Verpflichtung der Mitgliedstaaten zur Gewährleistung einer loyalen Zusammenarbeit sind hinreichend präzise, um der Kommission Zugang zu Datenbanken mit personenbezogenen Daten zu gewähren. Eine loyale Zusammenarbeit beinhaltet, dass die Mitgliedstaaten — unter bestimmten Voraussetzungen — der Kommission Informationen bereitstellen sollten, wenn sie darum ersucht werden oder wenn sie im Rahmen einer bestimmten Vorschrift verpflichtet sind, Informationen bereitzustellen. Dies beinhaltet jedoch nicht, dass die Kommission Zugang zu ihren Datenbanken haben sollte.

45. In diesem Zusammenhang betont der EDSB ebenfalls, dass die CPC-Verordnung die Möglichkeit ausschließt, dass die Kommission zu den in Amtshilfeersuchen und Durchsetzungsersuchen enthaltenen Informationen Zugang erhält. Artikel 6 und Artikel 8 der CPC-Verordnung benennen lediglich die ersuchte Behörde und nicht die Kommission als Empfänger dieser Daten.

3.3 **Besondere Datenkategorien im CPCS**

46. Der EDSB begrüßt, dass die zweite CPC-Änderung in Punkt 4.4 des Anhangs zum CPC-Durchführungsbeschluss eine Bestimmung zur Verarbeitung besonderer Datenkategorien im CPCS einführt. Der EDSB begrüßt insbesondere, dass die Bestimmung eine solche Verarbeitung auf Fälle beschränkt, in denen die Erfüllung von Verpflichtungen im Rahmen der CPC-Verordnung auf andere Weise „unmöglich wird" und der zusätzlichen Bedingung unterliegt, dass die Verarbeitung solcher Daten „gemäß der Richtlinie 95/46/EG zulässig" sein sollte.

IV. **EINGEBAUTER DATENSCHUTZ UND RECHENSCHAFTSPFLICHT**

47. Nachdem in Teil III die spezifischen, von der zweiten CPC-Änderung aufgeworfenen Fragen erörtert wurden, lenkt der EDSB in den Teilen IV bis VI die Aufmerksamkeit der Kommission auf eine Reihe anderer Punkte, die im Rahmen der Weiterentwicklung des Rechtsrahmens für das CPCS berücksichtigt werden sollten.

4.1 **Eingebauter Datenschutz**

48. Der EDSB bestärkt die Kommission und andere EU-Organe seit Längerem in der Absicht, technologische und organisatorische Maßnahmen zu ergreifen, mit denen der Datenschutz und die Sicherheit als grundlegende Bestandteile in das Konzept und die Umsetzung ihres Informationssystems integriert werden („eingebauter Datenschutz") ([12]).

49. Obwohl der EDSB begrüßt und anerkennt, dass bestimmte in diese Richtung weisende Maßnahmen ergriffen wurden, empfiehlt er, dass die Kommission eine umfassende Bewertung vornehmen sollte, welche weiteren Garantien für den eingebauten Datenschutz in die Systemarchitektur des CPCS integriert werden könnten. Unter anderem sollte Folgendes berücksichtigt und gegebenenfalls durchgeführt werden:

— Lösungen zum eingebauten Datenschutz, mit denen die Systemnutzer angeleitet werden, „angemessene" Datenschutzentscheidungen zu treffen (siehe Abschnitt 3.2 der Stellungnahme zur Vorabkontrolle);

— Maßnahmen, die einen rechtzeitigen Abschluss und eine rechtzeitige Löschung des Falls ermöglichen (wie oben, Abschnitt 3.3);

— Verfahren, die das Recht auf Information und das Recht auf Auskunft der betroffenen Personen begünstigen (wie oben, Abschnitt 3.5);

— klare Verfahren für alle Modifizierungen, die direkt auf der Ebene der Datenbank ausgeführt werden, Protokollierung der Zugriffe, die Beschreibung der Maßnahme und die Genehmigung auf einer angemessenen Ebene (wie oben, Abschnitt 3.6) und

— eine „verschlüsselte" Speicherung von Informationen in der Datenbank, so dass IT-Betreiber nicht auf diese zugreifen können (zumindest für bestimmte Daten, wie beispielsweise vertrauliche Anhänge) (wie oben, Abschnitt 3.6).

4.2 **Rechenschaftspflicht**

50. Zudem empfiehlt der EDSB in Übereinstimmung mit dem Grundsatz der „Rechenschaftspflicht" ([13]), einen klaren Rahmen für die Rechenschaftspflicht festzulegen, durch den die Einhaltung des Datenschutzes gewährleistet und ein Nachweis hierfür erbracht wird, wie zum Beispiel:

([12]) Siehe Abschnitt 7 der Stellungnahme des EDSB zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — „Gesamtkonzept für den Datenschutz in der Europäischen Union", die am 14. Januar 2011 abgegeben wurde. (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

([13]) Wie oben.

— Bereitstellung und gegebenenfalls Aktualisierung einer Datenschutzpolitik, die auf der höchsten Ebene innerhalb der GD SANCO zu genehmigen ist. Diese Datenschutzpolitk sollte ebenfalls einen Sicherheitsplan umfassen (siehe Abschnitt 3.6 der Stellungnahme zur Vorabkontrolle) ([14]);

— Durchführung regelmäßiger Prüfungen zur Bewertung der fortdauernden Angemessenheit und Übereinstimmung mit der Datenschutzpolitik (einschließlich einer Prüfung des Sicherheitsplans, wie oben, Abschnitt 3.6);

— (zumindest teilweise) Veröffentlichung der Ergebnisse dieser Prüfungen, um den Interessenträgern hinsichtlich der Einhaltung des Datenschutzes Gewissheit zu verschaffen und

— Meldung von Datenschutzverletzungen und anderen sicherheitsrelevanten Ereignissen an den Datenschutzbeauftragten der Kommission und an die entsprechenden betroffenen Personen (und gegebenenfalls an andere Interessenträger und Behörden) ([15]).

V. ÜBERMITTLUNG PERSONENBEZOGENER DATEN ÜBER DIE EUROPÄISCHE UNION HINAUS

5.1 Bilaterale Abkommen

51. Artikel 14 Absatz 2 der CPC-Verordnung sieht vor, dass gemäß der CPC-Verordnung übermittelte Informationen im Rahmen eines bilateralen Amtshilfeabkommens mit einem Drittland ebenfalls von einer zuständigen Behörde an die Behörde des Drittlandes übermittelt werden können, sofern i) die Einwilligung der zuständigen Behörde, von der die Informationen ursprünglich stammen, eingeholt wurde und ii) die geltenden EU-Datenschutzvorschriften eingehalten werden.

52. Artikel 25 und 26 der Richtlinie 95/46/EG unterwerfen Übermittlungen an Drittländer bestimmten zusätzlichen Bedingungen. Diese Bedingungen sollen gewährleisten, dass die Daten im Ausland angemessen geschützt werden. Zusätzlich wird eine Reihe von Ausnahmen festgelegt. Die Durchführung und Auslegung dieser Bestimmungen der Richtlinie 95/46/EG können in den verschiedenen Mitgliedstaaten von einander abweichen.

53. Vor dem Hintergrund der vorstehenden Ausführungen kann der EDSB die in der CPC-Verordnung enthaltenen Garantien akzeptieren, nämlich, dass alle Übermittlungen in Drittländer den beiden folgenden Bedingungen unterliegen: i) der Einwilligung der zuständigen Behörde, von der die Informationen ursprünglich stammen, und ii) der Einhaltung der EU-Datenschutzvorschriften.

54. Der EDSB begrüßt ebenfalls, dass die CPC-Datenschutzleitlinien empfehlen, dass — es sei denn, in einem Drittland ist ein angemessenes Schutzniveau gewährleistet — sämtliche bilateralen Amtshilfeabkommen angemessene Sicherheitsbestimmungen im Hinblick auf den Datenschutz enthalten sollten und — falls erforderlich — das Abkommen ebenfalls den entsprechenden Datenschutz-Aufsichtsbehörden gemeldet werden sollte.

55. Ungeachtet dessen sind die in der CPC-Verordnung festgelegten Vereinbarungen nicht ideal. Ihre Anwendung ist komplex: eine zuständige Behörde müsste im Rahmen der Entscheidung, ob Informationen in ein Drittland übermittelt werden sollen, nicht nur das Amtshilfeabkommen des eigenen Landes mit dem Drittland, die Datenschutzgesetze des eigenen Landes und ihre eigene Bewertung der Angemessenheit einer Datenübermittlung in das fragliche Drittland auf der Grundlage der Datenschutzgesetze des eigenen Landes berücksichtigen, sondern müsste ebenfalls beachten, ob die zuständigen Behörden, die zu der Akte beigetragen haben (und dies können mehrere Behörden sein) ihre Zustimmung auf der Grundlage ihrer eigenen Datenschutzgesetze erteilt haben.

56. Vom Standpunkt des Datenschutzes führt diese Komplexität zu Unsicherheiten hinsichtlich der Rechte der betroffenen Personen und insbesondere zu Unsicherheiten hinsichtlich dessen, ob und unter welchen Bedingungen Daten der betroffenen Personen ins Ausland übermittelt werden können. Die betroffenen Personen ziehen ebenfalls nicht im größtmöglichen Maß Nutzen aus einem soliden und harmonisierten europäischen datenschutzrechtlichen Normensystem. Zusätzlich beeinträchtigt diese Komplexität vom Standpunkt der zuständigen Behörden aus möglicherweise ebenfalls die Zusammenarbeit zwischen den zuständigen Behörden und hat einen hohen Verwaltungsaufwand zur Folge.

57. Vor dem Hintergrund der vorhergehenden Ausführungen befürwortet der EDSB den Abschluss von EU-weiten Vereinbarungen, die angemessene Datenschutzgarantien bereitstellen, während gleichzeitig die Anwendung von heterogenen Kriterien und der hieraus resultierende Verwaltungsaufwand für die zuständigen Behörden vermieden wird.

5.2 EU-weite Vereinbarungen

58. Zusätzlich zu den in Artikel 14 hinsichtlich der Amtshilfeabkommen vorgesehenen Möglichkeiten legt Artikel 18 der CPC-Verordnung hinsichtlich internationaler Vereinbarungen fest: „Die Gemeinschaft arbeitet […] mit Drittstaaten und den zuständigen internationalen Organisationen zusammen.“ Und: „Die Einzelheiten der Zusammenarbeit, einschließlich der Festlegung der Einzelheiten für die Amtshilfe, können Gegenstand von Abkommen zwischen der Gemeinschaft und den betreffenden Drittstaaten sein.“

([14]) Die Kommission sollte ebenfalls in Erwägung ziehen, zumindest eine teilweise Folgenabschätzung für den Datenschutz und die Privatsphäre durchzuführen, mit Schwerpunkt auf den Zwecken, der Länge und den Modalitäten der Aufbewahrungsfristen und nach Möglichkeit andere noch offene Fragen diskutieren, die bisher noch nicht umfassend behandelt wurden.

([15]) Siehe Abschnitt 6.3 der weiter oben aufgeführten Stellungnahme des EDSB vom 14. Januar 2011.

59. Aus den in Abschnitt 5.1 weiter oben dargelegten Gründen unterstützt der EDSB die Kommission in ihrer Initiative, EU-weite Abkommen mit angemessenen, auf EU-Ebene harmonisierten Datenschutzgarantien zu verhandeln und abzuschließen, um die bestehenden bilateralen Abkommen zu ersetzen.

60. Die Unterstützung des EDSB solcher EU-weiten Abkommen hängt jedoch von der Zusage seitens der Kommission und der EU-Gesetzgeber ab, das höchstmögliche Schutzniveau für den Austausch personenbezogener Daten mit Drittländern zu gewährleisten. Die Auswirkungen internationaler Abkommen über eine Zusammenarbeit mit Drittländern müssen vom Standpunkt des Datenschutzes aus sorgfältig abgewogen werden, für diese gegenseitigen Übermittlungen müssen klare Vorschriften festgelegt und angemessene Datenschutzgarantien bereitgestellt werden, und zwar auf der Grundlage einer Konsultation des EDSB und gegebenenfalls nationaler Datenschutzbehörden.

61. Obwohl in Artikel 18 der CPC-Verordnung die Frage eines direkten Zugriffs auf das CPCS durch Behörden eines Drittlandes nicht direkt behandelt wird, ist dies technisch möglich. Der EDSB möchte nicht von der Integration neuer Funktionen in das CPCS abraten, um den zuständigen Behörden in Drittländern einen streng begrenzten und selektiven Zugang mithilfe eines speziell entworfenen Mechanismus zu ermöglichen (Kommunikationsweg und Schnittstelle). Dies könnte tatsächlich die Wirksamkeit der Zusammenarbeit erhöhen.

62. Nichtsdestotrotz birgt solch ein direkter Zugang bestimmte Risiken und daher müssen seine Auswirkungen auf den Datenschutz und die erforderlichen technischen/organisatorischen Vorkehrungen und Garantien gesondert behandelt werden. Eine solche technische Funktion sollte unter der Anwendung der Grundsätze des „eingebauten Datenschutzes" aufgebaut werden. Die Sicherheit sollte ebenfalls eine klare Priorität darstellen. Schließlich sollte der EDSB und gegebenenfalls nationale Datenschutzbehörden konsultiert werden.

VI. **„VERBRAUCHERRECHTE AUF DATENSCHUTZ" UND DIE ÜBER DAS CPCS VERSTÄRKTE ZUSAMMENARBEIT DER DATENSCHUTZBEHÖRDEN**

63. Vorausgesetzt, dass die Empfehlungen des EDSB (einschließlich der Empfehlungen in seiner Stellungnahme zur Vorabkontrolle) berücksichtigt werden, ist der EDSB zuversichtlich, dass das CPCS ein effizientes und datenschutzfreundliches Instrument für grenzübergreifende Durchsetzungsmaßnahmen gegen Verbraucherrechtsverstöße auf dem internationalen Markt darstellen kann.

64. Mit der Entwicklung des elektronischen Handels und der zunehmenden Verwendung elektronischer Kommunikationsnetzwerke durch Verbraucher verschiedener Produkte und Dienstleistungen werden mehr und mehr Daten von Einzelpersonen verarbeitet, während diese als Verbraucher handeln. Verbraucher können sich folglich zunehmend mit Verstößen gegen ihre Rechte im Hinblick auf den Datenschutz konfrontiert sehen. Folglich besteht für die Datenschutzbehörden ebenfalls Bedarf an einer effizienten Zusammenarbeit, um solche Verstöße zu unterbinden.

65. Zu den am häufigsten auftretenden Fällen einer Verletzung von „Verbraucherrechten auf Datenschutz" gehören unerbetene Werbenachrichten (Spam), Identitätsdiebstahl, illegale Profilerstellung, unrechtmäßige verhaltensorientierte Internetwerbung und Datenmissbrauch (Sicherheitsverletzungen).

66. Angesichts dessen, dass die Zahl der Fälle mit grenzübergreifendem Charakter in der Informationsgesellschaft wahrscheinlich ansteigen wird, fordert der EDSB die Kommission dazu auf, mögliche Gesetzgebungsmaßnahmen in Betracht zu ziehen, um die „Verbraucherrechte auf Datenschutz" zu schützen und die grenzübergreifende Zusammenarbeit zwischen den zuständigen Behörden zu verstärken, und zwar sowohl im Hinblick auf die Datenschutzbehörden, als auch auf die Verbraucherschutzbehörden.

67. Insbesondere und unter Berücksichtigung anderer möglicher Optionen sollte sorgfältig abgewogen werden, ob den Datenschutzbehörden ein maßgeschneiderter Zugang zum CPCS gestattet wird, um die Zusammenarbeit untereinander sowie mit anderen zuständigen Behörden zu ermöglichen, die bereits über einen Zugang zum CPCS verfügen.

68. Der Zugang durch Datenschutzbehörden sollte klar auf diejenigen Elemente beschränkt werden, die zur Ausführung der Aufgaben im Bereich ihrer Zuständigkeit und in Übereinstimmung mit den ermittelten Synergien notwendig sind. Selbstverständlich sollte ebenfalls gewährleistet werden, dass der Rahmen für die Beteiligung von Datenschutzbehörden so entworfen wird, dass ihrer Unabhängigkeit ordnungsgemäß Rechnung getragen wird.

VII. **SCHLUSSFOLGERUNGEN**

69. Der EDPS begrüßt, dass das CPCS auf einer Rechtsgrundlage basiert, die ebenfalls spezifische Datenschutzgarantien gewährleistet. Zur Ausräumung der verbliebenen Bedenken im Hinblick auf den Datenschutz stellt der EDSB fest, dass die weiter unten zusammengefassten Empfehlungen berücksichtigt werden sollten, wenn der Rechtsrahmen für das CPCS demnächst überarbeitet wird.

70. In der Zwischenzeit können zusätzliche Maßnahmen, die (gemäß der Empfehlungen in der Stellungnahme zur Vorabkontrolle) auf der praktischen, technischen und organisatorischen Ebene durchgeführt werden, eine einstweilige teilweise Lösung bezüglich dieser Bedenken bieten. In Erwartung von Gesetzesänderungen können bestimmte Änderungen ebenfalls anhand der operativen Leitlinien für das CPCS eingeführt werden.

71. Hinsichtlich der Aufbewahrungsfrist empfiehlt der EDSB Folgendes: i) Amtshilfeersuchen sollten innerhalb von spezifisch festgelegten Fristen abgeschlossen werden; ii) falls keine Ermittlungen oder Durchsetzungsmaßnahmen durchgeführt werden, sollten Warnmeldungen zurückgezogen und innerhalb von sechs Monaten nach ihrer Ausgabe gelöscht werden (es sei denn, eine andere, angemessenere Aufbewahrungsfrist kann begründet werden); und iii) die Kommission sollte den Zweck und die Angemessenheit einer Aufbewahrung aller Daten im Zusammenhang mit geschlossenen Fällen über einen zusätzlichen Zeitraum von fünf Jahren klarstellen und überdenken.

72. Zudem begrüßt der EDSB, dass die zweite CPC-Änderung den Zugang der Kommission zu Daten im CPCS klarstellt. Insbesondere begrüßt der EDSB, dass die Kommission über keinen Zugang zu vertraulicher Kommunikation zwischen den zuständigen Behörden in den Mitgliedstaaten, wie beispielsweise zu Amtshilfeersuchen, verfügt.

73. Der EDSB begrüßt ebenfalls, dass mit der zweiten CPC-Änderung eine Bestimmung eingeführt wurde, mit der die Verarbeitung besonderer Datenkategorien im CPCS behandelt wird.

74. Der EDSB empfiehlt zusätzlich, dass die Kommission erneut überprüfen sollte, welche zusätzlichen technischen und organisatorischen Maßnahmen ergriffen werden sollten, um sicherzustellen, dass der Schutz der Privatsphäre und der Datenschutz in die Sytemarchitektur des CPCS „eingebaut“ werden („eingebauter Datenschutz“) und dass angemessene Kontrollen eingerichtet sind, mit denen die Einhaltung des Datenschutzes gewährleistet und der Nachweis hierfür erbracht wird („Rechenschaftspflicht“).

75. Falls zudem ein EU-weites Abkommen zwischen der Europäischen Union und Drittländern abgeschlossen werden soll, um die Zusammenarbeit im Verbraucherschutz zu regeln, müssen die Auswirkungen dieser Abkommen sorgfältig abgewogen werden; zur Regelung dieses Austauschs müssen klare Vorschriften festgelegt und angemessene Datenschutzgarantien bereitgestellt werden.

76. Schließlich empfiehlt der EDPS, dass die Kommission die möglichen Synergien untersuchen sollte, die gegebenenfalls entstehen, falls den Datenschutzbehörden ermöglicht wird, in die Gemeinschaft der Nutzer des CPCS aufgenommen zu werden und zur Zusammenarbeit im Bereich der Durchsetzung der „Verbraucherrechte auf Datenschutz“ beizutragen.

Brüssel, den 5. Mai 2011

Giovanni BUTTARELLI

Stellvertretender Europäischer Datenschutzbeauftragter