AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind Decizia 2011/141/UE a Comisiei de modificare a Deciziei 2007/76/CE a Comisiei referitoare la Sistemul de cooperare pentru protecția consumatorului („SCPC") și privind Recomandarea 2011/136/UE a Comisiei privind orientări pentru punerea în aplicare a normelor privind protecția datelor în cadrul SCPC

(2011/C 217/06)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16,

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 7 și 8,

având în vedere Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date [1],

având în vedere solicitarea unui aviz, formulată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date [2],

ADOPTĂ PREZENTUL AVIZ:

I. **INTRODUCERE**

1. La 1 martie 2011, Comisia Europeană a adoptat o decizie de modificare a Deciziei 2007/76/CE a Comisiei referitoare la SCPC („a doua modificare a CPC") [3]. La aceeași dată Comisia a mai adoptat și Recomandarea Comisiei privind orientări pentru punerea în aplicare a normelor de protecția datelor în cadrul SCPC („Orientările pentru protecția datelor în CPC") [4]. Ambele documente au fost transmise AEPD spre consultare în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001.

2. SCPC este un sistem informatic creat și operat de Comisie în temeiul Regulamentului (CE) nr. 2006/2004 privind cooperarea în materie de protecție a consumatorului („Regulamentul CPC"). SCPC facilitează cooperarea dintre „autoritățile competente" ale statelor membre UE și Comisie în domeniul protecției consumatorului, cu privire la încălcările unui set predefinit de directive și regulamente europene. Pentru a intra sub incidența Regulamentului CPC, încălcările trebuie să aibă caracter transfrontalier și să prejudicieze „interesele colective ale consumatorilor".

3. În cadrul cooperării dintre ei, utilizatorii SCPC fac schimb de informații, inclusiv de date cu caracter personal. Aceste date cu caracter personal pot viza directorii sau angajații unui comerciant sau furnizor suspectat de comiterea unei încălcări, însuși comerciantul sau furnizorul respectiv (dacă este persoană fizică) sau terți precum consumatorii sau reclamanții.

4. Sistemul este menit să ofere un instrument sigur de comunicare între autoritățile competente, precum și o bază de date. SCPC este folosit de către autoritățile competente pentru a solicita informații care să contribuie la investigarea unui caz [5] sau pentru a solicita sprijin în aplicarea legislației [6] („cereri de asistență reciprocă"). În plus, autoritățile competente pot trimite un mesaj de avertizare („alertă") pentru a informa alte autorități competente și Comisia cu privire la o încălcare sau o suspiciune de încălcare [7]. SCPC mai cuprinde și alte funcționalități,

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] Decizia Comisiei din 1 martie 2011 de modificare a Deciziei 2007/76/CE de punere în aplicare a Regulamentului (CE) nr. 2006/2004 al Parlamentului European și al Consiliului în ceea ce privește asistența reciprocă între autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului (2011/141/UE) (JO L 59, 4.3.2011, p. 63).
[4] Recomandarea Comisiei din 1 martie 2011; Orientări pentru punerea în aplicare a normelor privind protecția datelor în cadrul Sistemului de cooperare pentru protecția consumatorilor (SCPC) (2011/136/UE) (JO L 57, 2.3.2011, p. 44).
[5] A se vedea articolul 6 din Regulamentul CPC referitor la „schimbul de informații la cerere".
[6] A se vedea articolul 8 din Regulamentul CPC referitor la „cererile de măsuri executorii".
[7] A se vedea articolul 7 din Regulamentul CPC referitor la „schimbul de informații fără cerere prealabilă" (sau „alertă" pe scurt).

inclusiv un sistem de notificare ([8]) și un forum prin intermediul căruia se efectuează schimburi de date care nu au legătură cu cazul.

5. În prezentul aviz AEPD abordează o serie de probleme de protecție a datelor referitoare la cadrul juridic al SCPC, axându-se în primul rând pe a doua modificare a CPC, adoptată recent. În plus, AEPD face un bilanț al progreselor înregistrate până în acest moment și evidențiază în mod selectiv, pentru viitor, unele dintre preocupările și considerentele rămase nerezolvate. De asemenea, AEPD formulează observații cu privire la unele dispoziții din Orientările pentru protecția datelor în CPC.

6. În paralel cu prezentul aviz [care este adoptat în temeiul articolului 28 alineatul (2) din Regulamentul (CE) nr. 45/2001], AEPD emite și un aviz de verificare prealabilă pentru exercitarea funcției sale de supraveghere (în temeiul articolului 27 din același regulament) („aviz de verificare prealabilă"). Avizul de verificare prealabilă cuprinde o descriere mai detaliată a SCPC, precum și a procesului de prelucrare a datelor cu caracter personal în cadrul acestuia. În avizul de verificare prealabilă, AEPD se concentrează asupra recomandărilor de măsuri specifice care să fie adoptate la nivel practic, tehnic și organizațional pentru a îmbunătăți gradul de respectare a normelor de protecție a datelor în cadrul SCPC. Luând în considerare faptul că și Orientările pentru protecția datelor în CPC sunt strâns legate de aceste măsuri specifice, avizul de verificare prealabilă formulează observații și cu privire la anumite dispoziții din aceste orientări.

II. CADRUL JURIDIC AL SCPC

7. AEPD salută faptul că SCPC se bazează pe un temei juridic solid, mai exact pe un regulament adoptat de către Consiliu și Parlament. În plus, AEPD este mulțumită că temeiul juridic a fost completat în timp, astfel încât să ofere detalii suplimentare și să abordeze preocupările legate de protecția datelor. În mod special, AEPD salută adoptarea Deciziei 2007/76/CE a Comisiei din 22 decembrie 2006 de punere în aplicare a Regulamentului CPC („Decizia de punere în aplicare a CPC"), modificată ulterior la 17 martie 2008 și, mai recent, la 1 martie 2011 prin a doua modificare a CPC. De asemenea, AEPD apreciază adoptarea de către Comisie a Orientărilor pentru protecția datelor în CPC, care abordează în mod specific problemele de protecție a datelor.

8. Deși regretă că nu a fost consultată la momentul adoptării inițiale a Regulamentului CPC și a Deciziei de punere în aplicare a CPC, AEPD se bucură că a fost consultată de Comisie cu ocazia adoptării fiecăreia dintre cele două modificări ale Deciziei de punere în aplicare a CPC, precum și cu privire la Orientările pentru protecția datelor în CPC. De asemenea, AEPD apreciază că, anterior, Comisia a consultat și Grupul de lucru „Articolul 29" pentru protecția datelor („GL29"), care a emis Avizul nr. 6/2007 (WP 139) la 21 septembrie 2007. În sfârșit, AEPD salută faptul că în expunerea de motive a Orientărilor pentru protecția datelor în CPC se face trimitere la aceste consultări.

9. AEPD constată că (i) recomandările sale formulate în cadrul comunicărilor neoficiale anterioare, precum și cele exprimate de GL29 în Avizul nr. 6/2007, au fost atent luate în considerare de Comisie și că (ii) multe dintre aceste recomandări au fost urmate în dezvoltarea ulterioară a cadrului legislativ al SCPC și/sau la nivel practic, tehnic și organizațional. Observațiile AEPD formulate atât în prezentul aviz, cât și în avizul de verificare prealabilă trebuie interpretate în acest context pozitiv.

III. PROBLEME DE PROTECȚIE A DATELOR CU PRIVIRE LA A DOUA MODIFICARE A CPC

3.1. Păstrarea datelor cu caracter personal în SCPC

3.1.1. *Introducere*

10. Ca observație preliminară, AEPD atrage atenția asupra faptului că problema referitoare la închiderea cazurilor și la perioadele de păstrare a datelor nu a fost rezolvată în mod adecvat și complet în Regulamentul CPC ([9]).

11. Într-adevăr, Regulamentul CPC cuprinde doar două norme specifice privind ștergerea datelor și nu prevede nimic referitor la închiderea cazurilor ([10]). În primul rând, acesta impune ca, atunci când o alertă „se dovedește nefondată", autoritatea competentă să o retragă, iar Comisia să elimine fără întârziere informația respectivă din baza de date. În al doilea rând impune ca, atunci când o autoritate competentă notifică încetarea unei încălcări în temeiul articolului 8 alineatul (6) din regulament, datele păstrate să fie șterse la cinci ani după notificare.

12. Regulamentul CPC nu stabilește scopul perioadei de păstrare de cinci ani. De asemenea, nu sunt prevăzute specificații suplimentare cu privire la modul și momentul în care trebuie să se aprecieze dacă o alertă este „nefondată". În plus, regulamentul nu specifică nici cât timp trebuie să rămână informațiile în baza de date în situațiile care nu intră sub incidența celor două norme specifice menționate (de exemplu, nu precizează cât timp se păstrează în baza

([8]) A se vedea articolul 7 alineatul (2) și articolul 8 alineatul (6) din Regulamentul CPC.

([9]) A se vedea și Avizul nr. 6/2007 al Grupului de lucru „Articolul 29" pentru protecția datelor (menționat în partea II de mai sus).

([10]) A se vedea articolul 10 alineatul (2) din Regulamentul CPC.

de date cererile de asistență reciprocă dacă nu s-au soldat cu o măsură executorie care să pună capăt încălcării).

13. AEPD salută faptul că atât Decizia de punere în aplicare a CPC, în forma sa modificată, cât și Orientările pentru protecția datelor în CPC încearcă să aducă clarificări suplimentare. Totuși, AEPD rămâne preocupată de câteva aspecte privind normele de închidere a cazurilor și de păstrare a datelor în SCPC, conform celor discutate la secțiunile 3.1.2-3.1.4 de mai jos.

14. AEPD recomandă ca aceste preocupări să fie rezolvate cu ocazia următoarei revizuiri a cadrului juridic al SCPC, printr-o modificare suplimentară a Deciziei de punere în aplicare a CPC sau, de preferat, chiar printr-o modificare a Regulamentului CPC.

15. Până la momentul în care va fi posibilă o astfel de acțiune legislativă, AEPD recomandă ca preocupările referitoare la perioadele de păstrare a datelor să fie rezolvate la nivel practic, tehnic și organizațional și, de asemenea, să fie explicate clar în „Rețeaua de cooperare pentru protecția consumatorului: orientări privind funcționarea" menționată în secțiunea 3.1.2 de mai jos.

3.1.2. *Închiderea cazurilor în timp util*

16. A doua modificare a CPC nu stabilește data finală până la care trebuie închise cazurile care implică o cerere de asistență reciprocă (cerere de informații sau cerere privind aplicarea legislației).

17. În avizul de verificare prealabilă, AEPD ia notă de o serie de măsuri pragmatice pe care Comisia le adoptă în prezent pentru a asigura închiderea în timp util a cazurilor aflate în stagnare.

18. În prezentul aviz, AEPD recomandă să se stabilească termene maxime pentru cererile de informații și cererile privind aplicarea legislației. Acestea ar trebui precizate în cadrul legislativ la următoarea revizuire a acestuia. Termenele trebuie corelate atât cu tipul cazului, cât și cu activitatea efectivă. În același timp, normele ar trebui să ofere autorităților competente flexibilitatea de a extinde cazurile din motive întemeiate, pentru a se asigura că niciun caz nu este închis prematur, chiar dacă închiderea unui caz complex necesită o perioadă mai lungă decât media.

19. Pentru a realiza acest lucru, AEPD recomandă ca punct de plecare utilizarea documentului intitulat „Rețeaua de cooperare pentru protecția consumatorului: orientări privind funcționarea", avizat de Comitetul CPC la 6 decembrie 2010. La punctul 2.7 din Orientările privind funcționarea, sub titlul „etape și termene într-un caz de CPC", se discută numărul tipic de cazuri și se prevede că cererile de informații trebuie rezolvate, în medie, într-o perioadă de una până la trei luni. Potrivit Orientărilor privind funcționarea, rezolvarea cererilor privind aplicarea legislației ar trebui să se poată face într-un interval mediu de șase până la nouă luni (exceptând cazurile de acțiuni în încetare sau de atacare a unei hotărâri administrative, pentru care un termen mai realist ar fi de un an sau mai mult).

3.1.3. *Alertele*

20. A doua modificare a CPC a introdus un paragraf nou la punctul 2.2.2 din anexa la Decizia de punere în aplicare a CPC, impunând ca alertele „justificate" să fie eliminate din baza de date la cinci ani după ce au fost emise (în ceea ce privește alertele „nejustificate", dispozițiile existente impuneau deja ștergerea lor de îndată ce „o alertă se dovedește a fi nefondată").

21. Pentru a contextualiza această nouă dispoziție, AEPD subliniază că una dintre preocupările sale majore este de a se asigura că datele cu caracter personal nu rămân în baza de date CPC mai mult timp decât este necesar. Aceasta este o problemă sensibilă îndeosebi în ceea ce privește alertele (care au număr mai mare de destinatari decât schimburile bilaterale de informații), iar dintre alerte, în special cu privire la cele referitoare la încălcările suspectate. În practică, absența unui termen-limită clar pentru menținerea unei alerte deschise ar însemna că unele alerte ar putea rămâne nerezolvate pentru o perioadă mai lungă decât este necesar (atâta vreme cât nu se dovedesc în mod clar nefondate). Astfel de acțiuni bazate pe suspiciuni neconfirmate ar prezenta riscuri semnificative pentru dreptul fundamental la protecția datelor, precum și pentru alte drepturi fundamentale, cum ar fi prezumția de nevinovăție.

22. În acest context, AEPD salută faptul că a fost stabilită o perioadă de păstrare a alertelor. AEPD consideră că, pe de altă parte, Comisia nu a furnizat o justificare adecvată pentru a arăta că perioada de păstrare de cinci ani este corect proporționată. AEPD recomandă Comisiei să efectueze o evaluare a proporționalității și să reevalueze durata perioadei de păstrare a alertelor. În principiu, toate alertele raportate ar trebui șterse din baza de date mult mai repede, cu excepția cazului în care o alertă, o încălcare sau o suspiciune de încălcare a dus la formularea unei cereri de asistență reciprocă și investigația transfrontalieră sau măsura executorie este încă în curs. Perioada de păstrare trebuie să fie suficient de lungă pentru a permite fiecărei autorități care primește mesajul să stabilească dacă dorește să ia măsuri de investigare sau executorii suplimentare și dacă dorește să transmită o cerere de asistență reciprocă prin intermediul CPC; însă, perioada de păstrare trebuie să fie suficient de scurtă pentru a minimiza riscul ca alertele să fie folosite în mod abuziv în vederea introducerii pe lista neagră sau a extragerii de date.

23. Din acest punct de vedere, AEPD recomandă Comisiei revizuirea cadrului juridic, astfel încât să se asigure ștergerea alertelor la cel mult șase luni de la introducerea lor, cu excepția cazului în care se justifică o altă perioadă de păstrare, mai adecvată.

24. Acest lucru ar trebui să contribuie în special la asigurarea faptului că, în cazurile în care suspiciunea nu a fost confirmată (sau ancheta nu a fost continuată), persoanele nevinovate care au legătură cu suspiciunea respectivă nu vor fi menținute pe „lista neagră" și nu vor fi considerate „suspecte" pe o perioadă mai lungă decât este necesar și care nu ar fi conformă cu articolul 6 litera (e) din Directiva 95/46/CE.

25. Această limitare este necesară și pentru a asigura conformitatea cu principiul calității datelor [a se vedea articolul 6 litera (d) din Directiva 95/46/CE], precum și cu alte principii juridice importante. Acest aspect ar putea avea ca rezultat un nivel de protecție mai adecvat pentru persoanele fizice și ar trebui, în același timp, să permită organelor de aplicare a legii să se concentreze mai bine asupra cazurilor relevante.

3.1.4. *Perioada de păstrare a cererilor de asistență reciprocă închise*

26. A doua modificare a CPC a adăugat un paragraf nou la punctul 2.1.5 din anexa la Decizia de punere în aplicare a CPC, în care se prevede că „[t]oate celelalte informații cu privire la cererile de asistență reciprocă în temeiul articolului 6 din (Regulamentul CPC) trebuie eliminate din baza de date la cinci ani după închiderea cazului".

27. Interpretat în legătură cu textul existent, punctul 2.1.5 revizuit impune păstrarea tuturor informațiilor transmise în temeiul articolului 6 timp de cinci ani după închiderea cazului, cu excepția situațiilor în care:

— au fost șterse datele eronate;

— schimbul de informații nu a generat o alertă sau o cerere privind aplicarea legislației; sau

— s-a stabilit că nu s-a produs nicio încălcare în sensul Regulamentului CPC.

28. Într-adevăr, astfel cum se explică în avizul de verificare prealabilă, perioada „standard" de păstrare a datelor aplicată în SCPC în urma închiderii cazului (sub rezerva anumitor excepții) pare să fie de cinci ani atât pentru cererile privind aplicarea legislației, cât și pentru cererile de asistență reciprocă.

29. Textul Deciziei de punere în aplicare a CPC, în forma modificată de a doua modificare a CPC, nu pare să fie pe deplin consecvent cu Regulamentul CPC. Mai exact, articolul 10 alineatul (2) din Regulamentul CPC face distincția între, pe de o parte, informațiile transmise care duc la realizarea executării (respectiv cazurile în care încălcarea a încetat ca urmare a măsurilor executorii adoptate) și, pe de altă parte, informațiile care nu duc la realizarea executării. Pentru prima categorie se prevede o perioadă de păstrare de cinci ani de la închiderea cazului. Pentru cea de a doua categorie nu se prevede nimic specific (cu excepția faptului că alertele nefondate trebuie retrase și șterse).

30. Cu alte cuvinte, Regulamentul CPC impune o perioadă de păstrare a datelor de cinci ani de la închiderea cazului numai cu condiția să se fi adoptat măsuri executorii care să fi determinat încetarea încălcării.

31. Cu toate că AEPD are îndoieli în legătură cu scopul și proporționalitatea păstrării oricăror date timp de cinci ani după închiderea cazului (a se vedea observațiile următoare din secțiunea 3.1.4), distincția între cazurile care s-au încheiat cu realizarea executării și celelalte are o anumită logică din punct de vedere al protecției datelor. Mai exact, păstrarea pentru o perioadă lungă de timp a datelor referitoare la simple suspiciuni prezintă o predispoziție mai mare la inexactități și, de asemenea, riscă să încalce alte principii juridice importante. Prin urmare, se poate afirma, în general, că este mai probabil să se ridice probleme de protecție a datelor prin păstrarea acestor date pentru o perioadă lungă de timp decât prin păstrarea datelor referitoare la delicte efective, care au fost dovedite corespunzător și care au dus la măsuri executorii.

32. Contrar Regulamentului CPC, forma modificată a Deciziei de punere în aplicare a CPC pare să permită, cel puțin în unele cazuri, aplicarea perioadei de păstrare de cinci ani și pentru informații care nu au dus la realizarea unor măsuri executorii.

33. De exemplu, conform Deciziei de punere în aplicare a CPC, o cerere de informații care s-a soldat cu o alertă, dar nu a dus la măsuri executorii, pare să rămână în sistem timp de cinci ani de la „închiderea cazului".

34. Astfel, Regulamentul CPC și Decizia de punere în aplicare a CPC par să urmeze o abordare oarecum diferită. Cu toate că reflectă, într-o anumită măsură, dispozițiile regulamentului, Decizia de punere în aplicare a CPC introduce, în același timp, norme suplimentare importante referitoare la păstrare. Deși clarificarea normelor, în sine, este binevenită, AEPD pune sub semnul întrebării legalitatea stabilirii unor perioade mai lungi de păstrare a datelor în cazurile în care acestea nu erau impuse deja prin Regulamentul CPC. Acest lucru ar restricționa în mod suplimentar dreptul fundamental la protecția datelor, iar această restricționare s-ar produce printr-un act normativ de punere în aplicare, contrar Regulamentului CPC și legislației aplicabile privind protecția datelor.

35. Având în vedere cele menționate anterior, AEPD recomandă Comisiei revizuirea cadrului juridic și reanalizarea aplicabilității perioadei de păstrare de cinci ani în alte cazuri decât cele în care s-a realizat executarea, după cum se specifică în Regulamentul CPC.

36. În plus, AEPD salută faptul că Orientările pentru protecția datelor în CPC intenționează să precizeze scopul păstrării datelor după închiderea cazului, o chestiune importantă pe care nici Regulamentul CPC, nici a doua modificare a CPC nu au abordat-o. Mai exact, Orientările pentru protecția datelor în CPC prevăd că „în cursul perioadei de păstrare, funcționarii autorizați însărcinați cu aplicarea legislației din cadrul unei autorități competente care a tratat inițial un anumit caz pot consulta dosarul pentru a stabili legături cu posibile încălcări repetate, ceea ce contribuie la o aplicare mai bună și mai eficientă a legislației” ([11]).

37. Totuși, deși această clarificare este bine-venită, în absența unei justificări suplimentare a necesității acestui acces, AEPD nu este convinsă că proporționalitatea și suficiența acestui scop justifică perioada de păstrare de cinci ani. Prin urmare, AEPD recomandă Comisiei:

— să clarifice mai bine scopul păstrării datelor timp de cinci ani;

— să analizeze dacă o perioadă de păstrare mai scurtă ar permite atingerea acelorași obiective; și

— să analizeze dacă trebuie păstrate toate informațiile prevăzute în prezent sau ar fi suficient numai un subansamblu al acestora (de exemplu, ar trebui să se verifice dacă ar fi suficientă păstrarea exclusiv a notificărilor introduse în temeiul articolului 8.6; de asemenea, ar trebui să se analizeze în mod expres dacă este necesară păstrarea numelor directorilor sau a anexelor care pot conține și alte date cu caracter personal; în același timp, ar trebui să se facă distincția între datele referitoare la încălcări suspectate și cele referitoare la încălcări „dovedite”).

3.2. **Accesul Comisiei la datele din SCPC**

38. AEPD salută faptul că (prin introducerea unui nou punct 4.3 în anexa la Decizia de punere în aplicare a CPC), a doua modificare a CPC clarifică accesul Comisiei la datele din SCPC și că acesta se limitează în mod clar și expres la ceea ce este necesar în temeiul Regulamentului CPC. Mai exact, AEPD apreciază că nu i s-a acordat Comisiei acces la comunicările confidențiale dintre autoritățile competente ale statelor membre, cum ar fi cererile de asistență reciprocă.

39. Această clarificare și limitare este deosebit de importantă, având în vedere faptul că absența clarității ar fi putut duce la o situație în care Comisia să poată accesa informații, inclusiv date cu caracter personal, destinate exclusiv autorităților competente din statele membre.

40. După cum se descrie în secțiunea 5 din Orientările pentru protecția datelor în CPC, „Comisia are acces în scopul de a monitoriza aplicarea Regulamentului CPC și a actelor legislative privind protecția consumatorilor enumerate în anexa la Regulamentul CPC, precum și de a elabora informații statistice relative la îndeplinirea acestor obligații”.

41. Acest lucru nu înseamnă că ar trebui să aibă acces la toate datele transmise de statele membre între ele în cadrul SCPC.

42. Într-adevăr, AEPD subliniază că accesul la bazele de date precum SCPC intră sub incidența definiției prelucrării datelor cu caracter personal. În temeiul articolului 5 litera (a) din Regulamentul (CE) nr. 45/2001, care este relevant pentru drepturile de acces ale Comisiei în cadrul SCPC, instituțiile pot prelucra date cu caracter personal numai dacă acest lucru este necesar pentru îndeplinirea unei sarcini de interes public și doar cu condiția ca prelucrarea să se bazeze pe tratate sau pe legislația secundară.

([11]) A se vedea secțiunea 8 din Orientări, „Câteva recomandări suplimentare; De ce perioada de păstrare a datelor este fixată la 5 ani?” Orientările pentru protecția datelor în CPC mai adaugă și că „perioada de păstrare are obiectivul de a facilita cooperarea dintre autoritățile publice însărcinate cu aplicarea legislației care protejează interesele consumatorilor atunci când acestea se confruntă cu încălcări intracomunitare și de a contribui la buna funcționare a pieței interne, la calitatea și la coerența aplicării legislației care protejează interesele consumatorilor, la monitorizarea protejării intereselor economice ale consumatorilor și la creșterea nivelului și a coerenței aplicării legislației”.

43. AEPD înțelege că, prin aceste cerințe – care decurg direct din dreptul privind protecția datelor consfințit prin articolul 8 din Convenția Europeană a Drepturilor Omului și prin articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene –, Comisiei i se acordă competența de a accesa sistemele de informații ale statelor membre numai dacă acest lucru este prevăzut în dispoziții legale specifice, bazate pe un temei juridic pe deplin adecvat (în mod normal procedura legislativă ordinară). Securitatea juridică și transparența sunt cele două valori de bază care explică de ce existența unui temei juridic specific și sigur pentru accesul Comisiei reprezintă o garanție deosebit de importantă a respectării drepturilor fundamentale ale persoanelor cu privire la protecția datelor.

44. Nici competența generală de monitorizare pe care Comisia o are în calitate de „gardian al tratatelor", nici obligația statelor membre de a asigura o cooperare loială nu sunt suficient de precise pentru a acorda Comisiei acces la bazele de date ce conțin date cu caracter personal. Cooperarea loială presupune obligația statelor membre de a furniza Comisiei informații – în anumite condiții – atunci când li se solicită acest lucru sau când au obligația de a furniza informații în temeiul unei anumite norme. Cu toate acestea, ea nu presupune dreptul Comisiei de a avea acces la bazele de date ale statelor membre.

45. În acest context, AEPD mai subliniază și faptul că Regulamentul CPC exclude posibilitatea accesării de către Comisie a informațiilor cuprinse în cererile de asistență reciprocă și în cererile privind aplicarea legislației. Articolele 6 și 8 din Regulamentul CPC desemnează numai autoritatea solicitată, și nu Comisia, ca destinatar al acestor date.

3.3. **Categorii speciale de date din SCPC**

46. AEPD se bucură că a doua modificare a CPC a introdus, la punctul 4.4 din anexa la Decizia de punere în aplicare a CPC, o dispoziție care se referă la prelucrarea unor categorii speciale de date din SCPC. Mai exact, AEPD salută faptul că dispoziția respectivă limitează această prelucrare la cazurile în care îndeplinirea obligațiilor care decurg din Regulamentul CPC ar fi „altfel imposibilă" și că prelucrarea unor astfel de date este supusă condiției suplimentare de a fi „permisă în temeiul Directivei 95/46/CE".

IV. **RESPONSABILITATEA ȘI LUAREA ÎN CONSIDERARE A VIEȚII PRIVATE ÎNCEPÂND CU MOMENTUL CONCEPERII**

47. După ce în partea III a discutat problemele specifice ridicate de a doua modificare a CPC, în părțile IV-VI AEPD dorește să atragă atenția Comisiei asupra câtorva aspecte care ar trebui avute în vedere pentru a îmbunătăți în continuare cadrul juridic al SCPC.

4.1. **Luarea în considerare a vieții private începând cu momentul conceperii**

48. În ultima perioadă, AEPD a încurajat Comisia și alte instituții UE să adopte măsuri tehnologice și organizaționale de integrare a protecției și securității datelor ca parte fundamentală a procesului de concepere și implementare a sistemelor lor de informații („luarea în considerare a vieții private începând cu momentul conceperii") ([12]).

49. Deși salută și recunoaște faptul că s-au adoptat unele măsuri în această direcție, AEPD recomandă Comisiei realizarea unei evaluări cuprinzătoare a garanțiilor suplimentare care ar mai putea fi încorporate în arhitectura sistemului SCPC pentru a lua în considerare viața privată începând cu momentul conceperii. Printre altele, ar trebui avute în vedere și implementate, după necesități, următoarele:

— soluții de luare în considerare a vieții private începând cu momentul conceperii, care să ghideze utilizatorii sistemului pentru a lua decizii „adecvate" de protecție a datelor (a se vedea secțiunea 3.2 din avizul de verificare prealabilă);

— măsuri de facilitare a închiderii și ștergerii cazurilor în timp util (*idem*, secțiunea 3.3);

— proceduri de facilitare a drepturilor de informare și de acces ale persoanelor vizate (*idem*, secțiunea 3.5);

— proceduri clare pentru orice modificare efectuată în mod direct la nivelul bazei de date, acces prin înregistrare, argumentarea acțiunii și aprobare la nivelul adecvat (*idem*, secțiunea 3.6); și

— stocare „codificată" a informațiilor în baza de date, astfel încât operatorii IT să nu le poată accesa (cel puțin pentru unele date, precum anexele confidențiale) (*idem*, secțiunea 3.6).

4.2. **Responsabilitatea**

50. În continuare, în conformitate cu principiul „responsabilității" ([13]), AEPD mai recomandă și stabilirea unui cadru clar al răspunderii, care să asigure respectarea protecției datelor și să furnizeze dovezi în acest sens, cum ar fi:

([12]) A se vedea secțiunea 7 din Avizul AEPD privind Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor – „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană", emis la 14 ianuarie 2011 (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

([13]) Idem.

— adoptarea și actualizarea, după necesități, a unei politici de protecție a datelor care să fie aprobată la cel mai înalt nivel de conducere din cadrul DG SANCO. Această politică de protecție a datelor ar trebui să cuprindă și un plan de securitate (a se vedea și secțiunea 3.6 din avizul de verificare prealabilă) ([14]);

— efectuarea unor audituri periodice care să evalueze continuitatea adecvării și respectarea politicii de protecție a datelor (inclusiv auditarea planului de securitate, *idem*, secțiunea 3.6);

— publicarea (măcar parțială) a rezultatelor acestor audituri pentru a asigura părțile interesate cu privire la respectarea protecției datelor; și

— semnalarea cazurilor de încălcare a securității datelor și a altor atentate la adresa securității către responsabilul cu protecția datelor din cadrul Comisiei și către persoanele vizate (precum și către alte părți interesate și autorități în cazurile relevante) ([15]).

V. TRANSMITEREA DATELOR CU CARACTER PERSONAL ÎN AFARA UNIUNII EUROPENE

5.1. Acorduri bilaterale

51. Articolul 14 alineatul (2) din Regulamentul CPC prevede că autoritatea competentă poate, de asemenea, să transmită unei autorități dintr-o țară terță, în cadrul unui acord bilateral de asistență încheiat cu țara în cauză, informații transmise în conformitate cu Regulamentul CPC, cu condiția ca (i) autoritatea competentă care a furnizat inițial informațiile să consimtă și (ii) comunicarea să fie în conformitate cu legislația comunitară aplicabilă privind protecția datelor.

52. Articolele 25 și 26 din Directiva 95/46/CE supun comunicările de informații către țări terțe unor condiții suplimentare. Aceste condiții sunt menite să asigure o protecție adecvată a datelor în străinătate. În plus, articolele respective prevăd și o serie de excepții. Punerea în aplicare și interpretarea acestor dispoziții ale Directivei 95/46/CE pot varia de la un stat membru la altul.

53. Având în vedere cele menționate anterior, AEPD poate accepta garanțiile cuprinse în Regulamentul CPC, și anume ca orice transmitere de date către o țară terță să fie condiționată atât de (i) consimțământul autorității competente care a furnizat inițial informațiile, cât și de (ii) legislația UE aplicabilă privind protecția datelor.

54. De asemenea, AEPD salută faptul că Orientările pentru protecția datelor în CPC recomandă ca – în cazul în care țara terță nu asigură un nivel adecvat de protecție – orice acord bilateral de asistență să prevadă garanții adecvate de protecție a datelor, precum și ca – atunci când acest lucru este necesar – acordul să fie notificat și autorităților relevante de supraveghere a protecției datelor.

55. Cu toate acestea, acordurile prevăzute în Regulamentul CPC nu sunt ideale. Aplicarea acestora este complexă: o autoritate competentă care decide dacă să transmită sau nu informații unei țări terțe ar avea nevoie să țină seama nu doar de acordul bilateral al țării sale cu țara terță respectivă, de legislația proprie privind protecția datelor și de propria sa evaluare a adecvării transmiterii datelor către țara terță în cauză, efectuată pe baza legislației proprii privind protecția datelor, ci ar trebui să ia în calcul și dacă celelalte autorități competente implicate care au contribuit la dosar (și acestea pot fi mai multe) au consimțit sau nu, pe baza propriilor legislații privind protecția datelor.

56. Din punct de vedere al protecției datelor, această complexitate produce incertitudini în legătură cu drepturile persoanelor vizate, în special incertitudini privind transmiterea sau netransmiterea în străinătate a datelor acestora și condițiile în care se poate realiza acest lucru. De asemenea, persoanele vizate nu beneficiază în cea mai mare măsură posibilă de o legislație comunitară solidă și armonizată privind protecția datelor. În plus, din punct de vedere al autorităților competente este probabil ca această complexitate să împiedice cooperarea între autorități și să creeze o sarcină administrativă.

57. Având în vedere cele menționate anterior, AEPD încurajează încheierea unor acorduri comunitare care să prevadă garanții adecvate de protecție a datelor și, în același timp, să contribuie la evitarea aplicării unor criterii eterogene și, în consecință, a creșterii sarcinii administrative a autorităților competente.

5.2. Acordurile la nivelul UE

58. În plus față de posibilitatea cooperării bilaterale prevăzută la articolul 14, articolul 18 din Regulamentul CPC referitor la acordurile internaționale mai prevede și că „Comunitatea cooperează cu țările terțe și cu organizațiile internaționale competente” și că „modalitățile de cooperare, inclusiv stabilirea unor înțelegeri de asistență reciprocă, pot să facă obiectul unor acorduri între Comunitate și țările terțe în cauză”.

([14]) Comisia ar trebui să ia în considerare, după necesități, realizarea a cel puțin o evaluare parțială a impactului asupra protecției datelor și a vieții private, care să se concentreze asupra scopului, duratei și modalităților perioadei de păstrare a datelor și, eventual, să discute alte probleme rămase nerezolvate care încă nu au fost abordate în mod cuprinzător.

([15]) A se vedea secțiunea 6.3 din avizul AEPD din 14 ianuarie 2011 menționat anterior.

59. Din motivele prevăzute la secțiunea 5.1 de mai sus, AEPD susține Comisia în inițiativa sa de a negocia și de a încheia acorduri comunitare cu garanții adecvate de protecție a datelor, armonizate la nivelul UE, care să înlocuiască acordurile bilaterale actuale.

60. Sprijinul AEPD față de astfel de acorduri la nivel UE este însă condiționat de angajamentul Comisiei și al legiuitorilor UE de a asigura cel mai înalt nivel de protecție în cazul schimburilor de date cu caracter personal cu țările terțe. Implicațiile acordurilor de cooperare internațională cu țările terțe trebuie analizate cu atenție din punct de vedere al protecției datelor, trebuie instituite norme clare care să reglementeze aceste schimburi și trebuie prevăzute garanții adecvate de protecție a datelor, pe baza consultării AEPD și, când este cazul, a autorităților naționale de protecție a datelor.

61. Cu toate că articolul 18 din Regulamentul CPC nu abordează în mod expres chestiunea accesului direct la SCPC al autorităților din țările terțe, acest lucru poate fi posibil din punct de vedere tehnic. AEPD nu dorește să descurajeze includerea în SCPC a unor noi funcționalități care să permită accesarea selectivă și strict limitată a sistemului de către autoritățile competente din țările terțe, prin intermediul unui mecanism anume conceput (canal de comunicare și interfață). Acest lucru ar putea spori cu adevărat eficiența cooperării.

62. Totuși, un astfel de acces direct prezintă riscurile sale și, prin urmare, implicațiile privind protecția datelor, modalitățile tehnice/organizaționale și garanțiile necesare trebuie abordate în mod expres. Orice astfel de funcționalitate tehnică ar trebui construită folosind principiile „luării în considerare a vieții private începând cu momentul conceperii". De asemenea, securitatea trebuie să reprezinte o prioritate clară. În sfârșit, trebuie consultată AEPD, precum și autoritățile naționale de protecție a datelor acolo unde este cazul.

VI. **„DREPTURILE CONSUMATORILOR PRIVIND PROTECȚIA DATELOR" ȘI CONSOLIDAREA COOPERĂRII AUTORITĂȚILOR DE PROTECȚIE A DATELOR PRIN INTERMEDIUL SCPC**

63. AEPD are convingerea că, dacă se urmează recomandările sale (inclusiv cele din avizul de verificare prealabilă), SCPC poate constitui un instrument eficient de aplicare transfrontalieră a legislației împotriva încălcării drepturilor consumatorilor din piața internă, care să ofere în același timp o protecție adecvată a datelor.

64. Odată cu dezvoltarea comerțului electronic și cu utilizarea pe scară tot mai largă a rețelelor electronice de comunicare de către consumatorii diverselor produse și servicii, vor fi prelucrate datele din ce în ce mai multor persoane atunci când acestea joacă rolul de consumatori. Astfel, consumatorii se pot confrunta cu tot mai multe cazuri de încălcare a drepturilor privind protecția datelor. În consecință, este nevoie ca și autoritățile de protecție a datelor să coopereze eficient pentru a pune capăt acestor încălcări.

65. Printre cele mai frecvente cazuri de încălcare a „drepturilor consumatorilor privind protecția datelor" se numără comunicațiile comerciale nesolicitate (spam), furtul de identitate, stabilirea ilegală a profilului, publicitatea comportamentală ilegală și atentatele la adresa securității.

66. Dat fiind că este probabil ca numărul de cazuri cu caracter transfrontalier să crească în societatea informațională, AEPD încurajează Comisia să ia în considerare eventuale măsuri legislative care să protejeze drepturile consumatorilor privind protecția datelor și să consolideze cooperarea transfrontalieră între autoritățile competente: autoritățile de protecție a datelor și autoritățile de protecție a consumatorilor.

67. Mai exact, luând în considerare și alte opțiuni posibile, trebuie analizat cu atenție dacă se va permite autorităților de protecție a datelor accesul adaptat la SCPC pentru a coopera atât între ele, cât și cu alte autorități competente care au deja acces la SCPC.

68. Accesul autorităților de protecție a datelor trebuie să fie limitat în mod clar la ceea ce este necesar pentru a-și îndeplini sarcinile în domeniile proprii de competență și în conformitate cu sinergiile identificate. Desigur, trebuie să se asigure un cadru de participare a autorităților de protecție a datelor elaborat, astfel încât să țină seama de independența acestora.

VII. **CONCLUZII**

69. AEPD salută faptul că SCPC se întemeiază pe un temei juridic care prevede și garanții specifice pentru protecția datelor. Pentru a răspunde oricăror preocupări nerezolvate în legătură cu protecția datelor, AEPD constată că la următoarea revizuire a cadrului juridic al SCPC ar trebui avute în vedere recomandările sintetizate în cele ce urmează.

70. Între timp, măsurile suplimentare adoptate la nivel practic, tehnic și organizațional (conform recomandărilor din avizul de verificare prealabilă) pot constitui o soluție parțială și temporară de rezolvare a acestor preocupări. În așteptarea modificărilor legislative, unele modificări pot fi introduse și prin intermediul Orientărilor privind funcționarea SCPC.

71. Cu privire la perioada de păstrare a datelor, AEPD recomandă ca (i) cererile de asistență reciprocă să fie închise în anumite termene-limită desemnate în mod expres; (ii) dacă nu se află în curs o investigație sau măsură de executare, alertele să fie retrase și șterse în termen de șase luni de la emitere (cu excepția cazului în care se justifică o altă perioadă de păstrare, mai adecvată); și (iii) Comisia să clarifice și să reconsidere scopul și proporționalitatea păstrării timp de încă cinci ani a tuturor datelor referitoare la cazurile închise.

72. În plus, AEPD se bucură că a doua modificare a CPC clarifică accesul Comisiei la datele din SCPC. Mai exact, AEPD apreciază că nu i s-a acordat Comisiei acces la comunicările confidențiale dintre autoritățile competente din statele membre, precum cererile de asistență reciprocă.

73. De asemenea, AEPD salută faptul că a doua modificare a CPC a introdus o dispoziție care vizează prelucrarea categoriilor speciale de date din SCPC.

74. Ca puncte suplimentare, AEPD recomandă Comisiei să reevalueze măsurile tehnice și organizaționale suplimentare care trebuie adoptate pentru a se asigura că protecția datelor și confidențialitatea sunt „concepute" în arhitectura sistemului SCPC („luarea în considerare a vieții private începând cu momentul conceperii") și că se instituie controale adecvate care să asigure respectarea protecției datelor și să furnizeze dovezi în acest sens („responsabilitatea").

75. În continuare, dacă urmează să se încheie un acord comunitar între Uniunea Europeană și o țară terță pentru reglementarea cooperării în domeniul protecției datelor consumatorilor trebuie cântărite cu atenție implicațiile acestor acorduri, trebuie instituite norme clare pentru reglementarea acestor schimburi de date și trebuie prevăzute garanții adecvate de protecție a datelor.

76. În sfârșit, AEPD recomandă Comisiei să analizeze eventualele sinergii care s-ar putea produce dacă li s-ar permite autorităților de protecție a datelor să se alăture comunității de utilizatori ai SCPC pentru a coopera în vederea asigurării respectării „drepturilor consumatorilor privind protecția datelor".

Adoptat la Bruxelles, 5 mai 2011.

Giovanni BUTTARELLI

Adjunct al Autorității Europene pentru Protecția Datelor