OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie decyzji Komisji 2011/141/UE zmieniającej decyzję Komisji 2007/76/WE w sprawie systemu współpracy w zakresie ochrony konsumenta (CPCS) oraz w sprawie zalecenia Komisji 2011/136/UE w sprawie wytycznych dotyczących wdrażania przepisów dotyczących ochrony danych w CPCS

(2011/C 217/06)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych [1],

uwzględniając wniosek o opinię zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych [2],

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. W dniu 1 marca 2011 r. Komisja Europejska przyjęła decyzję Komisji zmieniającą decyzję Komisji 2007/76/WE w sprawie CPCS (zwaną „drugą zmianą CPC") [3]. W tym samym dniu Komisja przyjęła również zalecenie Komisji w sprawie wytycznych dotyczących wdrażania przepisów dotyczących ochrony danych w CPCS („wytyczne dotyczące ochrony danych CPC") [4]. Obydwa dokumenty zostały przekazane EIOD do konsultacji zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001.

2. CPCS jest systemem informatycznym opracowanym i obsługiwanym przez Komisję na podstawie rozporządzenia (WE) nr 2006/2004 w sprawie współpracy w dziedzinie ochrony konsumentów (zwanego „rozporządzeniem CPC"). CPCS ułatwia współpracę między „właściwymi organami" w państwach członkowskich UE i Komisją w obszarze ochrony konsumentów, jeżeli chodzi o naruszanie przepisów wybranych dyrektyw i rozporządzeń UE. Naruszenia objęte zakresem rozporządzenia CPC muszą mieć charakter transgraniczny i szkodzić „zbiorowym interesom konsumentów".

3. W ramach współpracy użytkownicy CPCS przekazują sobie informacje, które obejmują również dane osobowe. Wspomniane dane osobowe mogą dotyczyć dyrektorów lub pracowników sprzedającego lub dostawcy podejrzanego o naruszenie, samego sprzedającego lub dostawcy (jeżeli jest osobą fizyczną), a także osób trzecich, np. konsumentów lub osób składających skargę.

4. System został zaprojektowany jako bezpieczne narzędzie komunikacji między właściwymi organami, a także jako baza danych. Właściwe organy używają CPCS do wyszukiwania informacji pomocnych w prowadzeniu dochodzenia w danej sprawie [5] lub do wnioskowania o pomoc w egzekwowaniu prawa [6] („wnioski o wzajemną pomoc"). Ponadto właściwe organy mogą również przesyłać ostrzeżenie („powiadomienie") w celu poinformowania innych właściwych organów i Komisji o naruszeniu lub podejrzeniu naruszenia [7]. CPCS zawiera również inne funkcje

[1] Dz.U. L 281 z 23.11.1995, s. 31.
[2] Dz.U. L 8 z 12.1.2001, s. 1.
[3] Decyzja Komisji z dnia 1 marca 2011 r. zmieniająca decyzję 2007/76/WE wykonującą rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów w odniesieniu do wzajemnej pomocy (2011/141/UE) (Dz.U. L 59 z 4.3.2011, s. 63).
[4] Zalecenie Komisji z dnia 1 marca 2011 r. w sprawie wytycznych dotyczących wdrażania przepisów dotyczących ochrony danych w systemie współpracy w zakresie ochrony danych konsumenta (CPCS) (2011/136/UE) (Dz.U. L 57 z 2.3.2011, s. 44).
[5] Zob. art. 6 rozporządzenia CPC dotyczący „wymiany informacji na wniosek".
[6] Zob. art. 8 rozporządzenia CPC dotyczący „wniosków o podjęcie środków służących egzekwowaniu prawa".
[7] Zob. art. 7 rozporządzenia CPC dotyczący „wymiany informacji bez wniosku".

obejmujące system notyfikacji ([8]) oraz forum do wymiany danych niezwiązanych z konkretnym przypadkiem.

5. W niniejszej opinii EIOD poruszy szereg kwestii związanych z ochroną danych w odniesieniu do ram prawnych CPCS, koncentrując się przede wszystkim na niedawno przyjętej drugiej zmianie CPC. Ponadto EIOD podsumuje dotychczasowe osiągnięcia oraz wybiórczo omówi niektóre nierozwiane obawy i przedstawi uwagi na przyszłość. Skomentuje również niektóre zapisy w wytycznych dotyczących ochrony danych CPC.

6. Równocześnie z niniejszą opinią (która została przyjęta na podstawie art. 28 ust. 2 rozporządzenia (WE) nr 45/2001) EIOD wydaje również opinię o kontroli wstępnej, działając w charakterze organu nadzorczego (na podstawie art. 27 tego samego rozporządzenia) (zwaną „opinią o kontroli wstępnej"). Opinia o kontroli wstępnej zawiera bardziej szczegółowy opis CPCS, a także przetwarzania danych osobowych w tym systemie. W opinii o kontroli wstępnej EIOD koncentruje się na zaleceniach dotyczących specjalnych środków o charakterze praktycznym, technicznym i organizacyjnym w celu poprawy ochrony danych w CPCS. Mając na uwadze, że wytyczne dotyczące ochrony danych CPC są również ściśle powiązane z takimi specjalnymi środkami, opinia o kontroli wstępnej zawiera również komentarze do wybranych zapisów wytycznych.

II. **RAMY PRAWNE CPCS**

7. EIOD z zadowoleniem stwierdza, że CPCS opiera się na solidnej podstawie prawnej, a w szczególności na rozporządzeniu przyjętym przez Radę i Parlament. Ponadto EIOD wyraża zadowolenie z faktu, że podstawa prawna została w międzyczasie uzupełniona, w wyniku czego jest bardziej szczegółowa i odpowiada na obawy dotyczące ochrony danych. EIOD wyraża szczególne zadowolenie z przyjęcia decyzji Komisji 2007/76/WE z dnia 22 grudnia 2006 r. wykonującej rozporządzenie CPC (zwanej „decyzją wykonującą CPC"), a następnie z jej zmiany w dniu 17 marca 2008 r., a ostatnio w dniu 1 marca 2011 r. w ramach drugiej zmiany CPC. EIOD z zadowoleniem przyjmuje również fakt, że Komisja przyjęła wytyczne dotyczące ochrony danych CPC, szczególnie jeżeli chodzi o kwestie związane z ochroną danych.

8. Chociaż EIOD wyraża żal, że nie konsultowano się z nim w momencie przyjmowania rozporządzenia CPC i decyzji wykonującej CPC, cieszy się, że Komisja przeprowadziła takie konsultacje przy okazji przyjmowania każdej z dwóch zmian decyzji wykonującej CPC, a także wytycznych dotyczących ochrony danych CPC. EIOD wyraża również zadowolenie z faktu, że Komisja przeprowadziła również wcześniej konsultacje z Grupą Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, która wydała swoją opinię nr 6/2007 (WP 139) w dniu 21 września 2007 r. EIOD pochwala wreszcie fakt, że odniesienie do tych konsultacji znajduje się w motywach wytycznych dotyczących ochrony danych CPC.

9. EIOD zauważa, że (i) Komisja uważnie przyjrzała się zaleceniom EIOD zawartym w poprzednich nieformalnych wymianach uwag, a także zaleceniom Grupy Roboczej przedstawionym w opinii nr 6/2007; (ii) wiele z tych zaleceń uwzględniono przy dalszych pracach nad ramami prawnymi CPCS oraz na szczeblu praktycznym, technicznym i organizacyjnym. Uwagi Inspektora zawarte w niniejszej opinii, a także we opinii o kontroli wstępnej, należy uwzględniać, zestawiając z tymi pozytywnymi reakcjami.

III. **KWESTIE ZWIĄZANE Z OCHRONĄ DANYCH W ŚWIETLE DRUGIEJ ZMIANY CPC**

3.1. **Przechowywanie danych osobowych w CPCS**

3.1.1. *Wprowadzenie*

10. Na wstępnie EIOD stwierdza, że kwestie zamknięcia sprawy i okresów przechowywania nie zostały odpowiednio i szczegółowo uwzględnione w rozporządzeniu CPC ([9]).

11. Rozporządzenie CPC zawiera jedynie dwa szczegółowe przepisy dotyczące usuwania danych, nie ma w nim natomiast żadnego przepisu odnoszącego się do zamykania spraw ([10]). Zgodnie z pierwszym z nich, właściwy organ powinien wycofać powiadomienie, jeżeli okaże się ono „bezpodstawne", a Komisja powinna niezwłocznie usunąć informację z bazy danych. Drugi przepis zawiera wymóg usunięcia przechowywanych danych pięć lat po notyfikacji, jeżeli właściwy organ notyfikuje ustanie naruszenia zgodnie z art. 8 ust. 6 rozporządzenia CPC.

12. W rozporządzeniu nie przedstawiono uzasadnienia dla pięcioletniego okresu przechowywania informacji. Nie zawiera ono również dodatkowych uściśleń, na temat tego, jak i kiedy należy ocenić, czy powiadomienie jest „bezpodstawne". Ponadto w rozporządzeniu CPC nie sprecyzowano również, jak długo informacje powinny pozostać w bazie danych w przypadkach nieobjętych wymienionymi dwoma szczegółowymi przepisami (np. w rozporządzeniu nie określono, jak długo wnioski o wzajemną pomoc są przechowywane w bazie danych, jeżeli w ich wyniku nie

([8]) Zob. art. 7 ust. 2 i art. 8 ust. 6 rozporządzenia CPC.

([9]) Zob. również opinię nr 6/2007 Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych (o której mowa w części II powyżej).

([10]) Zob. art. 10 ust. 2 rozporządzenia CPC.

podjęto pomyślnych działań służących egzekwowaniu prawa, które powstrzymałyby naruszenie).

13. EIOD wyraża zadowolenie z faktu, że w zmienionej decyzji wykonującej CPC oraz w wytycznych dotyczących ochrony danych CPC podjęto próbę przedstawienia dodatkowych wyjaśnień. Niemniej jednak EIOD wyraża obawy co do wielu aspektów przepisów dotyczących zamykania spraw i przechowywania danych w CPCS, o czym mowa poniżej w sekcjach 3.1.2–3.1.4.

14. EIOD zaleca, aby obawy te uwzględnić podczas następnego przeglądu ram prawnych CPCS, w ramach kolejnej zmiany decyzji wykonującej CPC, a najlepiej w ramach zmiany samego rozporządzenia CPC.

15. Do czasu, gdy możliwe będzie tego rodzaju działanie legislacyjne, EIOD zaleca, aby uwagi dotyczące okresów przechowywania rozstrzygnąć na poziomie praktycznym, technicznym i organizacyjnym, a także precyzyjnie przedstawić w Sieci współpracy w zakresie ochrony konsumenta: wytycznych dotyczących funkcjonowania, o których mowa w sekcji 3.1.2 poniżej.

3.1.2. *Terminowe zamykanie spraw*

16. W drugiej zmianie CPC nie określono ostatecznej daty zamknięcia sprawy obejmującej wniosek o wzajemną pomoc (wniosek o informacje lub wniosek o egzekwowanie prawa).

17. W opinii o kontroli wstępnej EIOD odnotował szereg pragmatycznych środków, które Komisja obecnie wdraża, aby pomóc terminowo zakończyć zawieszone sprawy.

18. W niniejszej opinii EIOD zaleca, aby ustanowić maksymalne ramy czasowe dotyczące wniosków o informacje i wniosków o egzekwowanie prawa. Należy je sprecyzować w ramach legislacyjnych podczas następnego przeglądu. Ramy czasowe powinny być powiązane z typem sprawy oraz z bieżącą działalnością. Równocześnie należy przewidzieć przepisy zapewniające właściwym organom elastyczność w celu przedłużenia sprawy z uzasadnionych powodów, aby zapobiec przedwczesnemu zamykaniu spraw, nawet jeżeli skomplikowana sprawa zabiera więcej czasu niż przeciętna sprawa.

19. W tym celu EIOD zaleca, aby za punkt wyjścia obrać dokument zatytułowany „Sieć współpracy w zakresie ochrony konsumenta: wytyczne dotyczące funkcjonowania" zatwierdzony przez Komitet ds. Współpracy w dziedzinie Ochrony Konsumentów w dniu 6 grudnia 2010 r. W pkt 2.7 wytycznych dotyczących funkcjonowania zatytułowanym „Etapy i ramy czasowe sprawy dotyczącej CPC" omówiono typowy przebieg sprawy oraz ustalono, że wnioski o informacje należy zazwyczaj rozpatrzyć w okresie od jednego do trzech miesięcy. Zgodnie z wytycznymi dotyczącymi funkcjonowania rozpatrywanie wniosków o egzekwowanie prawa powinno przeciętnie trwać od sześciu do dziewięciu miesięcy (z wyjątkiem przypadków nakazów lub odwołania od decyzji administracyjnej, gdzie okres jednego roku lub dłuższy jest bardziej realistyczny).

3.1.3. *Powiadomienia*

20. W ramach drugiej zmiany CPC dodano nowy ustęp do pkt 2.2.2 załącznika do decyzji wykonującej CPC, zgodnie z którym „uzasadnione" powiadomienia powinny być usuwane z bazy danych pięć lat po ich przesłaniu (ponieważ w przypadku „bezpodstawnych" powiadomień istniejące przepisy przewidują wymóg ich usunięcia, kiedy „powiadomienie okaże się bezpodstawne").

21. Aby pokazać kontekst tego nowego przepisu, EIOD podkreśla, że chce przede wszystkim zagwarantować, aby dane osobowe nie były przechowywane w bazie danych CPCS dłużej niż to konieczne. Jest to delikatna kwestia, zwłaszcza jeżeli chodzi o powiadomienia (które są kierowane do większej liczby odbiorców niż informacje wymieniane dwustronnie), a wśród nich te, które dotyczą podejrzeń naruszenia. W praktyce brak precyzyjnych ram czasowych przechowywania powiadomień oznaczałby, że niektóre powiadomienia pozostawałyby niesklasyfikowane przez bezzasadnie długi okres (do czasu aż nie zostałoby bezsprzecznie dowiedzione, że są uzasadnione). Takie działania opierające się na niepotwierdzonych podejrzeniach mogłyby stanowić istotne zagrożenie dla podstawowego prawa ochrony danych, a także innych podstawowych praw takich jak domniemanie niewinności.

22. W związku z powyższym EIOD wyraża zadowolenie, że wprowadzono okres przechowywania powiadomień. Inspektor uważa jednak, że Komisja niedostatecznie uzasadniła proporcjonalność pięcioletniego okresu przechowywania. EIOD zaleca, aby Komisja przeprowadziła ocenę proporcjonalności i zweryfikowała długość okresu przechowywania powiadomień. Co do zasady wszystkie zgłoszone powiadomienia powinny zostać usunięte z bazy danych dużo wcześniej, chyba że powiadomienie o naruszeniu lub podejrzeniu naruszenia doprowadziło do złożenia wniosku o wzajemną pomoc, a dochodzenie transgraniczne lub działanie służące egzekwowaniu prawa wciąż trwa. Okres przechowywania powinien być dostatecznie długi, aby każdy organ otrzymujący zawiadomienie mógł ustalić, czy zamierza podjąć dalsze działania dochodzeniowe lub służące egzekwowaniu prawa oraz czy zamierza wysłać wniosek o wzajemną pomoc za pośrednictwem CPCS. Powinien on być jednak dostatecznie krótki, aby zminimalizować ryzyko nadużycia powiadomień do tworzenia czarnych list lub wykorzystywania danych.

23. Z tego punktu widzenia EIOD zaleca, aby Komisja dokonała przeglądu ram prawnych celem dopilnowania, aby powiadomienia były usuwane najpóźniej sześć miesięcy po ich wprowadzeniu, chyba że inny, bardziej odpowiedni okres przechowywania znajduje uzasadnienie.

24. Dzięki takiemu rozwiązaniu, zwłaszcza w przypadkach, w których podejrzenie nie zostało potwierdzone (ani nawet nie było przedmiotem dalszego dochodzenia), niewinne osoby fizyczne powiązane z podejrzeniem nie będą figurować na „czarnej liście" lub jako osoby „podejrzane" przez bezzasadnie długi okres, co byłoby sprzeczne z art. 6 lit. e) dyrektywy 95/46/WE.

25. Takie ograniczenie jest również konieczne w celu zagwarantowania zasady jakości danych (zob. art. 6 lit. d) dyrektywy 95/46/WE) a także innych ważnych zasad prawnych. W ten sposób nie tylko będzie można zapewnić bardziej odpowiedni poziom ochrony osób fizycznych, lecz równocześnie umożliwić urzędnikom odpowiedzialnym za egzekwowanie prawa skuteczniejsze skoncentrowanie się na odpowiednich sprawach.

3.1.4. *Okres przechowywania rozpatrzonych wniosków o wzajemną pomoc*

26. W wyniku drugiej zmiany CPC dodano nowy ustęp w pkt 2.15 załącznika do decyzji wykonującej CPC, aby wprowadzić wymóg, zgodnie z którym „wszystkie inne informacje dotyczące wniosków o wzajemną pomoc zgodnie z art. 6 (rozporządzenia CPC) są usuwane z bazy danych pięć lat po zamknięciu sprawy".

27. W połączeniu z istniejącym tekstem zmieniony pkt 2.15 zawiera wymóg przechowywania informacji wymienionych na podstawie art. 6 przez pięć lat po zamknięciu sprawy z wyjątkiem następujących sytuacji:

— kiedy usunięte zostały błędne dane,

— kiedy wymienione informacje nie doprowadziły do przekazania powiadomienia bądź złożenia wniosku o egzekwowanie prawa, albo

— kiedy dowiedziono, że naruszenie w rozumieniu rozporządzenia CPC nie miało miejsca.

28. Zgodnie z wyjaśnieniem zawartym w opinii o kontroli wstępnej „standardowy" okres przechowywania informacji stosowany w CPCS po zamknięciu sprawy (poza szczególnymi wyjątkami) wynosi pięć lat zarówno w przypadku wniosków o informacje, jak i wniosków o egzekwowanie prawa.

29. Tekst decyzji wykonującej CPC w brzmieniu po przyjęciu drugiej zmiany CPC nie wydaje się być w pełni spójny z rozporządzeniem CPC. W szczególności art. 10 ust. 2 rozporządzenia CPC wprowadza rozróżnienie między wymianą informacji prowadzącą do pomyślnego egzekwowania prawa (tj. przypadkami, w których naruszenie zostało usunięte w wyniku działań służących egzekwowaniu prawa) a informacjami, które nie doprowadziły do pomyślnego egzekwowania prawa. W pierwszym przypadku przewiduje się pięcioletni okres przechowywania danych od momentu zamknięcia sprawy. W drugim przypadku nie przewidziano szczegółowych przepisów (z wyjątkiem zapisu, że nieuzasadnione powiadomienia należy wycofywać, a informacje o nich usunąć).

30. Innymi słowy rozporządzenie CPC zawiera wymóg pięcioletniego okresu przechowywania danych po zamknięciu sprawy tylko wtedy, gdy podjęto działania służące egzekwowaniu prawa i gdy działania umożliwiły skuteczne usunięcie naruszenia.

31. Chociaż EIOD ma wątpliwości co do celu i proporcjonalności przechowywania danych przez pięć lat po zamknięciu sprawy (zob. dalsze komentarze w sekcji 3.1.4), rozróżnienie między sprawami zakończonymi pomyślnym egzekwowaniem prawa a przypadkami, w których prawo nie było egzekwowane, jest w pewnym stopniu logiczne z punktu widzenia ochrony danych. Zwłaszcza przechowywanie danych dotyczących zwykłych podejrzeń przez długi okres czasu może w większym stopniu być potencjalnie nietrafne, a ponadto wiąże się z ryzykiem naruszenia innych ważnych zasad prawnych. Można zatem ogólnie powiedzieć, że przechowywanie takich danych przez długi okres z większym prawdopodobieństwem może wywołać problemy w obszarze ochrony danych niż przechowywanie danych dotyczących bieżących nadużyć, które zostały należycie dowiedzione, a ich wynikiem było podjęcie działań służących egzekwowaniu prawa.

32. W przeciwieństwie do rozporządzenia CPC decyzja wykonująca CPC wraz ze zmianami raczej umożliwia, przynajmniej w niektórych przypadkach, stosowanie pięcioletniego okresu przechowywania również w odniesieniu do informacji, których wynikiem nie było podjęcie skutecznych działań służących egzekwowaniu prawa.

33. Na przykład zgodnie z decyzją wykonującą CPC wniosek o informację prowadzący do powiadomienia, lecz nieskutkujący działaniem służącym egzekwowaniu prawa będzie figurował w systemie przez pięć lat jako „zamknięcie sprawy".

34. Wydaje się zatem, że rozporządzenie CPC i decyzja wykonująca CPC są wyrazem nieco innego podejścia. Chociaż decyzja wykonująca CPC odzwierciedla w pewnym stopniu przepisy rozporządzenia CPC, wprowadza również ważne dodatkowe uregulowania dotyczące przechowywania. Pomimo że wyjaśnienie przepisów jest samo w sobie pożądane, EIOD kwestionuje zgodność z prawem wprowadzania dłuższych okresów przechowywania w sytuacji, gdy nie było to wymagane w rozporządzeniu CPC. Wiązałoby się to z dalszymi ograniczeniami podstawowego prawa do ochrony danych, również w przepisach wykonawczych, co jest sprzeczne z rozporządzeniem CPC i mającymi zastosowanie przepisami w dziedzinie ochrony danych.

35. W związku z powyższym EIOD zaleca, aby Komisja dokonała przeglądu ram prawnych i rozważyła, czy pięcioletni okres przechowywania danych powinien mieć zastosowanie do wszystkich innych przypadków poza tymi, w których miało miejsce pomyślne egzekwowanie prawa, tak jak stanowi rozporządzenie CPC.

36. Ponadto EIOD wyraża zadowolenie, że celem wytycznych dotyczących ochrony danych CPC jest sprecyzowanie celu przechowywania danych po zamknięciu sprawy. To ważna kwestia, która została pominięta zarówno w rozporządzeniu CPC, jak i w drugiej zmianie CPC. Wytyczne dotyczące ochrony danych CPC stanowią w szczególności, że „[w] okresie przechowywania upoważnieni urzędnicy odpowiedzialni za egzekwowanie prawa, pracujący dla właściwego organu, który pierwotnie zajmował się sprawą, mogą zapoznać się z jej aktami w celu określenia związków z ewentualnie ponawiającymi się naruszeniami, co przyczynia się do lepszego i skuteczniejszego egzekwowania prawa” ([11]).

37. Jednakże, chociaż to wyjaśnienie jest pożądane, wobec braku precyzyjniejszego uzasadnienia konieczności takiego dostępu, EIOD nie jest przekonany, że cel ten jest na tyle proporcjonalny i dostateczny, aby uzasadniał pięcioletni okres przechowywania danych. EIOD zaleca zatem Komisji, aby:

— dokładniej wyjaśnić, jaki jest cel pięcioletniego okresu przechowywania danych,

— ocenić, czy krótszy okres przechowywania pozwoliłby osiągnąć te same cele, oraz

— ocenić, czy wszystkie obecnie uwzględniane informacje muszą być przechowywane, czy też wystarczyłyby tylko niektóre z nich (np. należy rozważyć, czy nie wystarczyłoby przechowywanie powiadomień przekazywanych na podstawie art. 8 ust. 6; należy również szczegółowo ocenić, czy przechowywanie nazwisk dyrektorów lub załączników, które mogą zawierać dodatkowe dane osobowe, jest konieczne; należałoby również wprowadzić rozróżnienie między danymi dotyczącymi podejrzeń naruszenia i „dowiedzionych” naruszeń).

3.2. **Dostęp Komisji do danych w CPCS**

38. EIOD wyraża zadowolenie z faktu, że w drugiej zmianie CPC wyjaśniono dostęp komisji do danych w CPC (poprzez dodanie nowego punktu 4.3 w załączniku do decyzji wykonującej CPC) oraz że taki dostęp jest jasno i wyraźnie ograniczony do wymogów wynikających z rozporządzenia CPC. EIOD wyraża szczególne zadowolenie z faktu, że Komisja nie ma dostępu do poufnych komunikatów właściwych organów w państwach członkowskich, takich jak wnioski o wzajemną pomoc.

39. To wyjaśnienie i ograniczenie jest szczególnie ważne, jeżeli weźmie się pod uwagę, że brak precyzji mógł prowadzić do sytuacji, w której Komisja miałaby dostęp do informacji, w tym danych osobowych, które są przeznaczone wyłącznie dla właściwych organów w państwach członkowskich.

40. Zgodnie z opisem w sekcji 5 wytycznych dotyczących ochrony danych CPC „[d]ostęp ten umożliwiony jest w celu monitorowania stosowania rozporządzenia CPC oraz przepisów w zakresie ochrony konsumentów wymienionych w załączniku do tego rozporządzenia, a także w celu opracowywania informacji statystycznych w związku z wykonywaniem tych obowiązków”.

41. Nie znaczy to, że Komisja powinna mieć dostęp do wszystkich danych wymienianych między państwami członkowskimi w CPCS.

42. EIOD podkreśla, że dostęp do baz danych takich jak CPCS podlega definicji przetwarzania danych osobowych. Na mocy art. 5 lit. a) rozporządzenia (WE) nr 45/2001, który ma zastosowanie do praw dostępu Komisji do danych w CPCS, instytucje mogą przetwarzać dane osobowe tylko wtedy, gdy jest to konieczne do wykonania zadania w interesie publicznym, pod warunkiem, że przetwarzanie odbywa się na podstawie traktatów lub aktów prawa wtórnego.

([11]) Zob. sekcję 8 wytycznych: „Dodatkowe wytyczne; Dlaczego okres przechowywania danych określono na 5 lat?”. W wytycznych dotyczących ochrony danych CPC dodano również, że „[c]elem okresu przechowywania jest ułatwianie współpracy między organami publicznymi odpowiedzialnymi za egzekwowanie przepisów prawnych, które chronią interesy konsumentów w przypadkach, w których dochodzi do naruszeń wewnątrzwspólnotowych, przyczynianie się do należytego funkcjonowania rynku wewnętrznego, jakości, spójności egzekwowania przepisów prawnych, które chronią interesy konsumentów, monitorowania ochrony interesów ekonomicznych konsumentów oraz przyczynianie się do zwiększenia jakości i konsekwentości egzekwowania prawa”.

43. Zdaniem EIOD wymogi te – które wynikają bezpośrednio z prawa do ochrony danych gwarantowanego w art. 8 europejskiej konwencji praw człowieka oraz w art. 7 i 8 Karty praw podstawowych Unii Europejskiej – oznaczają, że Komisja jest upoważniona do dostępu do systemów informacyjnych państw członkowskich tylko wtedy, gdy takie upoważnienie zostało ustanowione w szczegółowych przepisach prawnych mających całkowicie adekwatną podstawę prawną (zazwyczaj jest to zwykła procedura legislacyjna). Pewność prawa i przejrzystość stanowią dwie podstawowe wartości, które tłumaczą, dlaczego specjalna i bezpieczna podstawa prawna dla dostępu Komisji do danych stanowi szczególnie ważną gwarancję respektowania podstawowych praw obywateli w obszarze ochrony danych.

44. Ani ogólne uprawnienie Komisji jako „strażniczki traktatu" do monitorowania, ani obowiązek państw członkowskich do lojalnej współpracy nie są dostatecznie precyzyjne, aby zapewnić Komisji dostęp do baz danych zawierających dane osobowe. Lojalna współpraca oznacza, że państwa członkowskie powinny – na określonych warunkach – przekazywać Komisji informacje, gdy otrzymują taki wniosek lub gdy spoczywa na nich obowiązek dostarczenia informacji na podstawie konkretnego przepisu. Nie oznacza to jednak, że Komisja powinna mieć dostęp do ich baz danych.

45. W tym kontekście EIOD podkreśla również, że rozporządzenie CPC wyklucza również możliwość dostępu Komisji do informacji zawartych we wnioskach o wzajemną pomoc i egzekwowanie prawa. W art. 6 i 8 rozporządzenia CPC tylko organ, do którego wniosek jest skierowany, nie zaś Komisja, został wskazany jako odbiorca tych danych.

3.3. **Specjalne kategorie danych w CPCS**

46. EIOD wyraża zadowolenie, że podczas drugiej zmiany CPC w pkt 4.4 załącznika do decyzji wykonującej CPC dodano przepis regulujący przetwarzanie specjalnych kategorii danych w CPCS. EIOD szczególnie pochwala fakt, że zgodnie z tym przepisem przetwarzanie jest ograniczone do przypadków, w których wypełnienie zobowiązań wynikających z rozporządzenia CPC byłoby „inaczej niemożliwe", oraz że podlega ono warunkowi, zgodnie z którym przetwarzanie powinno być „dopuszczalne na mocy dyrektywy 95/46/WE".

IV. **UWZGLĘDNIANIE OCHRONY PRYWATNOŚCI W FAZIE PROJEKTOWANIA I ODPOWIEDZIALNOŚĆ**

47. Po omówieniu w części III szczegółowych kwestii wynikających z drugiej zmiany CPC EIOD zamierza w części IV–VI zwrócić uwagę Komisji na kilka innych punktów, które można uwzględnić w dalszych pracach nad ramami prawnymi CPCS.

4.1. **Uwzględnianie ochrony prywatności w fazie projektowania**

48. Od pewnego czasu EIOD zachęca Komisję i inne instytucje do przyjęcia środków technologicznych i organizacyjnych łączących ochronę danych i bezpieczeństwo jako część działań na etapie projektowania i wdrażania systemów informacyjnych („uwzględnianie ochrony prywatności na etapie projektowania") ([12]).

49. Chociaż EIOD pochwala i uznaje fakt, że niektóre środki w tym kierunku zostały podjęte, zaleca, aby Komisja przeprowadziła szczegółową ocenę dalszych zabezpieczeń ochrony prywatności w fazie projektowania, które można by wprowadzić do architektury systemu CPCS. Spośród różnych rozwiązań następujące kwestie należy koniecznie rozważyć i wdrożyć:

— rozwiązania dotyczące ochrony prywatności w fazie projektowania, aby wskazać użytkownikom systemu „adekwatne działania" służące ochronie danych (zob. sekcja 3.2 opinii o kontroli wstępnej),

— środki służące ułatwieniu terminowego zamykania i usuwania spraw (zob. sekcja 3.3 opinii o kontroli wstępnej),

— procedury ułatwiające informowanie i zapewnianie prawa dostępu podmiotom danych (zob. sekcja 3.5 opinii o kontroli wstępnej),

— jasne procedury zmian dokonywanych bezpośrednio w bazie danych, dostęp na podstawie rejestracji danych, racjonalizacja działania i zatwierdzanie na odpowiednim poziomie (zob. sekcja 3.6 opinii o kontroli wstępnej), oraz

— „szyfrowane" przechowywanie informacji w bazie danych, tak aby operator informatyczny nie miał do nich dostępu (przynajmniej niektórych danych takich jak poufne załączniki) (zob. sekcja 3.6 opinii o kontroli wstępnej).

4.2. **Odpowiedzialność**

50. Ponadto zgodnie z zasadą „odpowiedzialności" ([13]) EIOD zaleca również ustanowienie jasnych ram odpowiedzialności gwarantujących ochronę danych i przewidujących potwierdzenie takiej ochrony, w tym:

([12]) Zob. sekcja 7 opinii EIOD w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej" wydanej w dniu 14 stycznia 2011 r. (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

([13]) Idem.

— przyjęcie i aktualizację, w razie potrzeby, polityki ochrony danych zatwierdzanej na najwyższym szczeblu kierowniczym w DG SANCO. Polityka ochrony danych powinna również obejmować plan bezpieczeństwa (zob. sekcja 3.6 opinii o kontroli wstępnej) ([14]),

— przeprowadzanie okresowych audytów w celu oceny stałej adekwatności polityki ochrony danych i zgodności z tą polityką (w tym audyt planu bezpieczeństwa, zob. sekcja 3.6 opinii o kontroli wstępnej),

— podanie do publicznej wiadomości (przynajmniej częściowo) wyników tych audytów, aby upewnić partnerów o gwarantowaniu ochrony danych, oraz

— powiadamianie inspektora ochrony danych w Komisji, zainteresowane podmioty danych (a także, w razie potrzeby, inne zainteresowane strony i organy) o naruszeniach dotyczących danych osobowych i innych incydentach związanych z bezpieczeństwem ([15]).

V. **PRZESYŁANIE DANYCH OSOBOWYCH POZA UNIĘ EUROPEJSKĄ**

5.1. **Ustalenia dwustronne**

51. Artykuł 14 ust. 2 rozporządzenia CPC stanowi, że informacje przekazane na podstawie rozporządzenia CPC mogą również zostać przekazane organowi kraju trzeciego na podstawie umowy w sprawie dwustronnej pomocy z krajem trzecim, pod warunkiem (i) uzyskania zgody właściwego organu, który jako pierwszy przekazał informacje oraz (ii) zgodnie z prawem unijnym w zakresie ochrony danych.

52. Zgodnie z art. 25 i 26 dyrektywy 95/46/WE przesyłanie danych do krajów trzecich podlega pewnym dodatkowym warunkom. Celem tych warunków jest zapewnienie odpowiedniej ochrony danych zagranicą. Ponadto przepisy te przewidują określone wyjątki. Wdrożenie i wykładnia tych przepisów dyrektywy 95/46/WE może różnić się w poszczególnych państwach członkowskich.

53. W świetle powyższych uwag EIOD może zaakceptować zabezpieczenia przewidziane w rozporządzeniu CPC, tj. że przesłanie danych do kraju trzeciego wymaga zarówno (i) zgody właściwego organu, który jako pierwszy przekazał informacje, jak i (ii) zgodności z unijnym prawem ochrony danych.

54. EIOD wyraża również zadowolenie, że w wytycznych dotyczących ochrony danych CPC znajduje się zalecenie, aby – o ile kraj trzeci nie zapewni odpowiedniego poziomu ochrony – wszelkie umowy w sprawie dwustronnej pomocy powinny zapewniać właściwe zabezpieczenie w zakresie ochrony danych, a odpowiednie organy nadzorcze ds. ochrony danych były o nich powiadamiane, jeżeli istnieje taki wymóg.

55. W świetle powyższych uwag ustalenia przyjęte w rozporządzeniu CPC nie są idealne. Ich stosowanie jest skomplikowane: właściwy organ decydujący, czy przesłać daną informację do kraju trzeciego, musi uwzględnić nie tylko umowę dwustronną między swoim krajem a krajem trzecim, przepisy w dziedzinie ochrony danych obowiązujące w jego kraju, a także własną ocenę adekwatności przesłania danych do kraju trzeciego na podstawie krajowych przepisów w dziedzinie ochrony danych, lecz również stwierdzić, czy właściwe organy, które przekazały informacje w danej sprawie (a może być ich kilka), wyraziły na to zgodę na podstawie obowiązujących ich przepisów w dziedzinie ochrony danych.

56. Z punktu widzenia ochrony danych kompleksowość prowadzi do niepewności co do praw podmiotu danych, a w szczególności do niepewności, czy i na jakich warunkach jego dane są przesyłane zagranicę. Podmioty danych nie korzystają również w możliwie najpełniejszym zakresie z solidnego i zharmonizowanego europejskiego prawa ochrony danych. Ponadto, z punktu widzenia właściwych organów, ta kompleksowość może również utrudniać współpracę właściwych organów oraz prowadzić do obciążeń administracyjnych.

57. W świetle powyższych uwag EIOD zachęca do zawarcia ogólnounijnych umów, które zapewnią odpowiednie zabezpieczenia ochrony danych, a jednocześnie pomogą uniknąć stosowania niejednorodnych kryteriów i wynikających z tego obciążeń administracyjnych dla właściwych organów.

5.2. **Porozumienia ogólnounijne**

58. Oprócz możliwości dwustronnej współpracy przewidzianej w art. 14, art. 18 rozporządzenia CPC w sprawie umów międzynarodowych również przewiduje, że „Wspólnota współpracuje z państwami trzecimi i właściwymi organizacjami międzynarodowymi" oraz że „[u]stalenia dotyczące współpracy, w tym ustanowienie ustaleń o wzajemnej pomocy, mogą być przedmiotem umów między Wspólnotą a zainteresowanymi państwami trzecimi".

([14]) Komisja powinna również rozważyć konieczność przeprowadzenia przynajmniej częściowej oceny wpływu ochrony danych i prywatności na cel, długość i zasady przechowywania danych oraz ewentualnie omówić pozostałe kwestie, które nie zostały jeszcze szczegółowo rozstrzygnięte.

([15]) Zob. sekcja 6.3 opinii EIOD z dnia 14 stycznia 2011 r., o której mowa powyżej.

59. Z powodów przedstawionych w sekcji 5.1 powyżej EIOD popiera inicjatywę Komisji dotyczącą wynegocjowania i zawarcia ogólnounijnych umów zapewniających adekwatne i zharmonizowane na poziomie UE zabezpieczenia w obszarze ochrony danych, aby zastąpić istniejące ustalenia dwustronne.

60. Poparcie EIOD dla takich ogólnounijnych umów podlega jednak warunkowi, że Komisja oraz prawodawca unijny zobowiążą się do zapewnienia najwyższego poziomu ochrony w przypadku wymiany danych osobowych z krajami trzecimi. Implikacje międzynarodowych umów o współpracy z krajami trzecimi należy uważnie ocenić z punktu widzenia ochrony danych, należy ustanowić jasne zasady przeprowadzania takiej wymiany oraz adekwatne zabezpieczenia w obszarze ochrony danych na podstawie konsultacji z EIOD oraz, w stosownym przypadku, krajowych organów ochrony danych.

61. Chociaż art. 18 rozporządzenia CPC nie porusza w sposób szczególny kwestii bezpośredniego dostępu organów kraju trzeciego do CPCS, może to być technicznie możliwe. EIOD nie zamierza zniechęcać do umieszczania nowych funkcji w CPCS, które umożliwiałyby właściwym organom w krajach trzecich ściśle ograniczony i wybiórczy dostęp do danych za pomocą specjalnie zaprojektowanego mechanizmu (kanału komunikacyjnego i interfejsu). Może to bowiem poprawić efektywność współpracy.

62. Niemniej jednak taki bezpośredni dostęp wiąże się z ryzykiem, a zatem należy zająć się jego implikacjami w obszarze ochrony danych oraz niezbędnymi techniczno-organizacyjnymi ustaleniami i zabezpieczeniami. Tego rodzaju techniczna funkcja musi zostać opracowana zgodnie z zasadami uwzględniania ochrony prywatności w fazie projektowania. Wyraźnym priorytetem musi być również bezpieczeństwo. Na koniec należy przeprowadzić konsultacje z EIOD, a także, w stosownym przypadku, z krajowymi organami odpowiedzialnymi za ochronę danych.

VI. **„PRAWA KONSUMENTÓW DO OCHRONY DANYCH" ORAZ ZACIEŚNIONA WSPÓŁPRACA ORGANÓW ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH ZA POŚREDNICTWEM CPCS**

63. Mając na uwadze, że zalecenia EIOD, w tym zalecenia zawarte w opinii o kontroli wstępnej) zostały uwzględnione, Inspektor nie ma obaw, że CPCS może być skutecznym i przyjaznym z punktu widzenia ochrony danych narzędziem służącym transgranicznemu egzekwowaniu prawa w przypadkach naruszania praw konsumentów na rynku wewnętrznym.

64. Wraz z rozwojem handlu elektronicznego i coraz większym wykorzystywaniem sieci komunikacji elektronicznej przez konsumentów różnych towarów i usług coraz więcej danych dotyczących osób fizycznych działających w charakterze konsumentów będzie przedmiotem przetwarzania. Konsumenci mogą spotkać się również z coraz większą liczbą przypadków naruszenia ich praw w obszarze ochrony danych. W konsekwencji organy odpowiedzialne za ochronę danych powinny skutecznie współpracować, aby powstrzymać takie naruszenia.

65. Wśród najpowszechniejszych przypadków naruszenia „praw konsumentów do ochrony danych" znajdują się niepożądane komunikaty handlowe (spam), kradzież tożsamości, nielegalne profilowanie, niezgodne z prawem reklama behawioralna i naruszanie danych osobowych (naruszanie bezpieczeństwa).

66. Mając na uwadze, że liczba przypadków o charakterze transgranicznym może wzrosnąć w społeczeństwie informacyjnym, EIOD zachęca Komisję do rozważenia ewentualnych środków legislacyjnych służących ochronie „praw konsumentów do ochrony danych" i zacieśnienia współpracy transgranicznej między właściwymi organami – organami odpowiedzialnymi za ochronę danych, jak i organami zajmującymi się ochroną konsumentów.

67. Rozważając również inne możliwe warianty, należy w szczególności uważnie ocenić, czy zapewnić organom odpowiedzialnym za ochronę danych specjalnie dostosowany dostęp do CPCS w celu umożliwienia współpracy między nimi oraz z innymi właściwymi organami, które już mają dostęp do CPCS.

68. Dostęp organów odpowiedzialnych za ochronę danych powinien wyraźnie ograniczać się do tego, co jest konieczne do wykonywania ich zadań w właściwych im obszarach kompetencji oraz zgodnie z ustaloną synergią. Oczywiście należy również zagwarantować takie stworzenie ram udziału organów odpowiedzialnych za ochronę danych, które będzie należycie uwzględniać ich niezależność.

VII. **WNIOSKI**

69. EIOD wyraża zadowolenie, że CPCS opiera się na podstawie prawnej, która gwarantuje również specjalne zabezpieczenia w obszarze ochrony danych. Aby rozpatrzyć wszelkie pozostałe aspekty ochrony danych, przedstawione poniżej zalecenia EIOD należy uwzględnić podczas kolejnego przeglądu ram prawnych CPCS.

70. W międzyczasie dodatkowe środki o charakterze praktycznym, technicznym i organizacyjnym (zgodnie z zaleceniami w opinii o kontroli wstępnej) mogą stanowić tymczasowe i częściowe rozwiązanie tych problemów. W oczekiwaniu na zmiany legislacyjne niektóre zmiany można wprowadzić, wykorzystując wytyczne dotyczące funkcjonowania CPCS.

71. Jeżeli chodzi o okres przechowywania, EIOD zaleca, aby (i) wnioski o wzajemną współpracę były zamykane w specjalnie wyznaczonych ramach czasowych; (ii) o ile dochodzenie lub środki służące egzekwowaniu prawa nie są w toku, powiadomienia były wycofywane i usuwane w ciągu sześciu miesięcy od momentu ich przekazania (chyba że można uzasadnić inny, odpowiedniejszy okres przechowywania), a Komisja wyjaśniła i ponownie rozważyła proporcjonalność przechowywania wszystkich danych związanych z zamkniętymi sprawami przez pięć dodatkowych lat.

72. Ponadto EIOD wyraża zadowolenie, że podczas drugiej zmiany CPC sprecyzowano dostęp Komisji do danych CPCS. EIOD w szczególności pochwala fakt, że Komisja nie ma dostępu do poufnych komunikatów przesyłanych między właściwymi organami w państwach członkowskich, takich jak wnioski o wzajemną pomoc.

73. EIOD wyraża również zadowolenie, że podczas drugiej zmiany CPC wprowadzono przepis regulujący przetwarzanie specjalnych kategorii danych w CPCS.

74. Dodatkowo EIOD zaleca, aby Komisja ponownie oceniła dodatkowe środki techniczne i organizacyjne, aby uwzględnić ochronę prywatności i danych w architekturze systemu CPCS (uwzględnianie ochrony prywatności w fazie projektowania) i zapewnić adekwatne kontrole gwarantujące respektowanie ochrony danych i potwierdzające takie respektowanie („odpowiedzialność").

75. Ponadto, jeżeli ogólnounijna umowa między Unią Europejską a dowolnym krajem trzecim ma zostać zawarta w celu uregulowania współpracy w obszarze ochrony konsumentów, należy uważnie uwzględnić implikacje takich ustaleń, ustanowić jasne przepisy wymiany danych oraz adekwatne zabezpieczenia w obszarze ochrony danych.

76. Na koniec EIOD zaleca, aby Komisja zbadała możliwość synergii, w przypadku gdy organy odpowiedzialne za ochronę danych miałyby możliwość dołączenia do użytkowników CPCS w celu współpracy na rzecz egzekwowania „praw konsumentów do ochrony danych".

Sporządzono w Brukseli dnia 5 maja 2011 r.

Giovanni BUTTARELLI

Zastępca Europejskiego Inspektora Ochrony Danych