ZALECENIA

ZALECENIE KOMISJI

z dnia 1 marca 2011 r.

w sprawie wytycznych dotyczących wdrażania przepisów dotyczących ochrony danych w systemie współpracy w zakresie ochrony konsumenta (CPCS)

(2011/136/UE)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

a także mając na uwadze, co następuje:

(1) Rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady z dnia 27 października 2004 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów („Rozporządzenie w sprawie współpracy w dziedzinie ochrony konsumentów") [1] (zwane dalej „rozporządzeniem CPC") ma na celu zacieśnienie współpracy w dziedzinie egzekwowania prawa ochrony konsumentów w ramach jednolitego rynku, ustanawia ogólnoeuropejską sieć krajowych organów publicznych odpowiedzialnych za egzekwowania prawa (zwaną dalej „siecią CPC") oraz określa ramy i ogólne warunki, na podstawie których organy publiczne państw członkowskich odpowiedzialne za egzekwowania prawa mają ze sobą współpracować w celu zapewnienia ochrony zbiorowych interesów gospodarczych konsumentów.

(2) Współpraca między krajowymi organami odpowiedzialnymi za egzekwowanie prawa ma zasadnicze znaczenie dla skutecznego funkcjonowania jednolitego rynku, a w ramach sieci CPC każdy organ ma możliwość zwrócenia się do innych organów o pomoc w badaniu ewentualnych naruszeń przepisów prawa ochrony konsumentów UE.

(3) Celem systemu współpracy w zakresie ochrony konsumenta (zwanego dalej „CPCS") jest umożliwienie organom publicznym odpowiedzialnym za egzekwowanie prawa wymiany informacji dotyczących ewentualnych naruszeń przepisów prawa ochrony konsumentów w bezpiecznym i pewnym środowisku.

(4) Wymiana informacji między państwami członkowskimi przy użyciu środków elektronicznych musi być zgodna z przepisami dotyczącymi ochrony danych osobowych określonymi w dyrektywie 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 [2] (zwanej dalej „dyrektywą o ochronie danych") i rozporządzeniu (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych [3] (zwanym dalej „rozporządzeniem o ochronie danych").

(5) W art. 8 Karty praw podstawowych Unii Europejskiej uznaje się prawo do ochrony danych. CPCS powinien gwarantować przejrzystość różnych obowiązków i zadań dzielonych między Komisję i państwa członkowskie w związku z przepisami dotyczącymi ochrony danych oraz udzielanie informacji i możliwość korzystania z łatwo dostępnych mechanizmów osobom, których dane dotyczą, aby mogły egzekwować swoje prawa.

(6) Należy ustanowić wytyczne dotyczące wdrożenia przepisów o ochronie danych w CPCS (zwane dalej „wytycznymi") w celu zapewnienia przestrzegania tych przepisów podczas przetwarzania danych w CPCS.

(7) Urzędnikom odpowiedzialnym za egzekwowanie prawa należy zalecać nawiązanie kontaktu z ich krajowymi organami nadzorczymi ochrony danych w celu uzyskania wskazówek i pomocy w sprawie najlepszego sposobu wdrażania wytycznych zgodnie z przepisami prawa krajowego oraz w razie potrzeby dopilnowanie, aby procedury powiadamiania i kontroli wstępnych w związku z operacjami przetwarzania w CPCS były przeprowadzane na poziomie krajowym.

(8) Należy zdecydowanie zalecać uczestnictwo w sesjach szkoleniowych organizowanych przez Komisję w celu udzielenia pomocy we wdrażaniu tych wytycznych.

(9) Informacje zwrotne na temat wdrażania wytycznych należy przekazać Komisji nie później niż w okresie dwóch lat od przyjęcia niniejszego zalecenia. Komisja powinna następnie dokonać dalszej oceny poziomu ochrony danych w CPCS oraz ustalić, czy konieczne jest wprowadzenie dodatkowych instrumentów, w tym środków regulacyjnych.

[1] Dz.U. L 364 z 9.12.2004, s. 1.

[2] Dz.U. L 281 z 23.11.1995, s. 31.

[3] Dz.U. L 8 z 12.1.2001, s. 1.

(10) Należy podjąć konieczne kroki w celu ułatwienia wdrożenia wytycznych przez podmioty i użytkowników CPCS. Krajowe organy ds. ochrony danych oraz Europejski Inspektor Ochrony Danych powinni uważnie śledzić rozwój sytuacji oraz stan wdrożenia zabezpieczeń w zakresie ochrony danych w odniesieniu do CPCS.

(11) Wytyczne stanowią uzupełnienie decyzji Komisji 2007/76/WE [1] oraz uwzględniają opinię grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołanej na mocy art. 29 [2] dyrektywy o ochronie danych, oraz opinię Europejskiego Inspektora Ochrony Danych [3], ustanowionego na mocy art. 41 rozporządzenia o ochronie danych (zwanego dalej „EIOD"),

PRZYJMUJE NINIEJSZE ZALECENIE:

Państwa członkowskie powinny zastosować się do wytycznych zawartych w załączniku.

Sporządzono w Brukseli dnia 1 marca 2011 r.

W imieniu Komisji
John DALLI
Członek Komisji

[1] Dz.U. L 32 z 6.2.2007, s. 192.
[2] Opinia 6/2007 na temat problematyki ochrony danych związanej z systemem współpracy w zakresie ochrony konsumenta (CPCS) 01910/2007/EN – WP 130 – przyjęta w dniu 21 września 2007 r.
[3] Opinia EIOD, ref. 2010-0692.

ZAŁĄCZNIK

Wytyczne dotyczące wdrażania przepisów dotyczących ochrony danych w systemie współpracy w zakresie ochrony konsumenta (CPCS)

1. WPROWADZENIE

Współpraca między krajowymi organami ds. ochrony konsumentów ma zasadnicze znaczenie dla odpowiedniego funkcjonowania rynku wewnętrznego, ponieważ brak skutecznego egzekwowania przepisów w sprawach transgranicznych podważa zaufanie konsumentów przy przyjmowaniu ofert transgranicznych, a co za tym idzie – ich przekonanie o słuszności wspólnego rynku, a także przyczynia się do zakłócania konkurencji.

CPCS jest narzędziem informatycznym ustanowionym rozporządzeniem CPC, które udostępnia strukturyzowany mechanizm wymiany informacji między krajowymi organami ds. ochrony konsumentów należącymi do sieci CPC. Narzędzie to pozwala organowi publicznemu zwrócić się do innych organów publicznych należących do sieci CPC o pomoc w badaniu i ściganiu ewentualnych naruszeń przepisów prawa UE w zakresie ochrony konsumentów oraz w podejmowaniu działań w zakresie egzekwowania przepisów, aby udaremnić nielegalne praktyki handlowe sprzedawców i dostawców, uderzające w konsumentów mieszkających w innych krajach UE. Składanie wniosków o przekazanie informacji oraz wszelka komunikacja między właściwymi organami publicznymi w zakresie stosowania rozporządzenia CPC odbywa się za pośrednictwem CPCS.

Rozporządzenie CPC ma na celu poprawę egzekwowania prawa ochrony konsumentów na rynku wewnętrznym przez ustanowienie ogólnoeuropejskiej sieci krajowych organów odpowiedzialnych za egzekwowanie prawa oraz ustanowienie warunków wzajemnej współpracy państw członkowskich. W rozporządzeniu CPC przewidziano, że wymiana informacji oraz składanie wniosków o wzajemną pomoc między krajowymi organami odpowiedzialnymi za egzekwowanie prawa będzie odbywać się za pośrednictwem specjalnej bazy danych. W związku z tym zaprojektowano CPCS, aby ułatwić tego rodzaju współpracę administracyjną i wymianę informacji, mając na celu egzekwowanie prawa UE w zakresie ochrony konsumentów.

Zakres współpracy ogranicza się do wewnątrzwspólnotowych naruszeń aktów prawnych wymienionych w załączniku do rozporządzenia CPC, które chronią zbiorowe interesy gospodarcze konsumentów.

2. ZAKRES I CELE NINIEJSZYCH WYTYCZNYCH

Zamierzeniem niniejszych wytycznych jest rozwiązanie problemu, jaki stanowi zapewnienie równowagi między efektywną i skuteczną współpracą w zakresie egzekwowania prawa, prowadzoną przez właściwe organy państw członkowskich, przy jednoczesnym poszanowaniu podstawowych praw do prywatności i ochrony danych osobowych.

Dane osobowe zdefiniowano w dyrektywie o ochronie danych [1] jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość.

Ponieważ urzędnicy krajowych organów odpowiedzialnych za egzekwowanie prawa (osoby prowadzące sprawy), będący użytkownikami CPCS, nie zawsze są ekspertami w dziedzinie ochrony danych i nie zawsze posiadają dostateczną znajomość wymogów w zakresie ochrony danych zawartych w krajowych przepisach o ochronie danych, zaleca się przekazanie użytkownikom CPCS wytycznych objaśniających funkcjonowanie CPCS ochrony danych w praktyce, przedstawiających środki ochronne, w które wyposażono system, oraz informujących o ewentualnym ryzyku związanym z jego użytkowaniem.

Zgodnie z założeniem niniejsze wytyczne obejmują najważniejsze zagadnienia ochrony danych w związku z CPCS i zawierają przystępne objaśnienia, z których mogą korzystać wszyscy użytkownicy CPCS. Nie stanowią one natomiast wyczerpującej analizy wszystkich aspektów ochrony danych w ramach CPCS.

Zdecydowanie zaleca się przeprowadzenie konsultacji również z organami ds. ochrony danych w państwach członkowskich, aby zagwarantować, by dopełnienie dla niniejszych wytycznych stanowiły obowiązki szczegółowo określone w krajowych przepisach o ochronie danych. Użytkownicy CPCS mogą także zwrócić się o dodatkową pomoc i wskazówki do powyższych organów, aby zapewnić spełnienie wymogów w zakresie ochrony danych. Wykaz takich organów oraz dane kontaktowe i odniesienia do stron internetowych znajdują się pod następującym adresem:

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

Powinno być jasne, że dane osobowe należy przetwarzać zgodnie ze szczegółowymi zasadami i warunkami określonymi w dyrektywie o ochronie danych. Osoby prowadzące sprawy zostały upoważnione w kontekście rozporządzenia do wymiany danych, w tym danych osobowych, w ramach CPCS, jeżeli celem czynności przetwarzania jest udaremnienie naruszania przepisów prawa UE w zakresie ochrony konsumentów, wymienionych w załączniku do rozporządzenia CPC. Przed przystąpieniem do przetwarzania takich danych należy jednak dokonać starannej oceny w celu upewnienia się, że zasady dotyczące ochrony danych są przestrzegane i że przetworzenie danych jest absolutnie niezbędne do osiągnięcia celów rozporządzenia CPC.

[1] Artykuł 2 lit. a).

Mając to na uwadze, przed przystąpieniem do przetwarzania danych osoby prowadzące sprawy posiadające dostęp do CPCS muszą przeprowadzić ocenę poszczególnych przypadków [1]. Niniejsze wytyczne mają stanowić pomoc dla osób prowadzących sprawy w dokonywaniu takich ocen, przedstawiając niektóre przewodnie zasady ochrony danych, które należy wziąć pod uwagę.

Celem jest również objaśnienie niektórych złożonych aspektów architektury CPCS w odniesieniu do wspólnych operacji przetwarzania i współadministracji, określając w tym celu rolę Komisji i rolę właściwych organów państw członkowskich jako „współadministratorów" wymiany danych w CPCS.

3. CPCS – NARZĘDZIE INFORMATYCZNE DO WSPÓŁPRACY W ZAKRESIE EGZEKWOWANIA PRAWA

CPCS jest narzędziem informatycznym opracowanym i obsługiwanym pod względem technicznym przez Komisję we współpracy z państwami członkowskimi. Celem CPCS jest zapewnienie wsparcia państwom członkowskim przy wdrażaniu w praktyce przepisów UE w zakresie ochrony konsumentów. System jest wykorzystywany w sieci CPC, która składa się z organów publicznych wyznaczonych przez państwa członkowskie i kraje EOG do prowadzenia wzajemnej współpracy i wymiany informacji w zakresie egzekwowania prawa ochrony konsumentów zgodnie z rozporządzeniem CPC.

Artykuł 10 rozporządzenia CPC stanowi, że:

„Komisja prowadzi elektroniczną bazę danych, w której przechowuje i przetwarza informacje uzyskane na podstawie art. 7, 8 i 9. Baza danych jest udostępniana do wglądu wyłącznie właściwym organom …".

Artykuł 12 ust. 3 rozporządzenia CPC stanowi, że:

„Wnioski o pomoc i przekazywanie informacji dokonywane są pisemnie przy użyciu standardowego formularza oraz przesyłane elektronicznie poprzez bazę danych ustanowioną na mocy art. 10.".

CPCS ułatwia współpracę i wymianę informacji ograniczoną do wewnątrzwspólnotowych naruszeń dyrektyw oraz rozporządzeń wymienionych w załączniku do rozporządzenia CPC, zajmującym się szeregiem kwestii, w tym nieuczciwymi praktykami handlowymi, sprzedażą wysyłkową, kredytem konsumenckim, imprezami turystycznymi, nieuczciwymi warunkami umownymi, time-share, handlem elektronicznym i innymi. CPCS nie może być wykorzystywany do wymiany informacji w obszarach prawodawstwa, które nie zostały wyraźnie wymienione we wspomnianym załączniku.

Przykłady:

I. Uczestnik rynku mający siedzibę w Belgii stosuje nieuczciwe warunki wobec konsumentów mieszkających we Francji w sprzeczności z dyrektywą w sprawie nieuczciwych warunków umownych. Organ ds. konsumentów we Francji może złożyć w CPCS wniosek do równoważnego organu w Belgii o podjęcie wszelkich niezbędnych środków egzekwowania prawa dostępnych w Belgii przeciwko danemu uczestnikowi rynku, aby bezzwłocznie udaremnić wewnątrzwspólnotowe naruszanie przepisów.

II. Organ ds. konsumentów w Danii otrzymuje skargi, że na danej stronie internetowej stosuje się nielegalne i zwodnicze praktyki handlowe na szkodę konsumentów. Strona ta znajduje się na szwedzkim serwerze. Duński organ ds. konsumentów potrzebuje informacji dotyczących przedmiotowej strony internetowej. W związku z tym może złożyć w CPCS wniosek o przekazanie informacji do szwedzkiego organu ds. konsumentów, który ma obowiązek dostarczyć potrzebne informacje.

Informacje są przesyłane przez państwa członkowskie, przechowywane w CPCS, udostępniane do wglądu państwom członkowskim będącym adresatami informacji oraz usuwane przez Komisję [2]. CPCS jest wykorzystywany jako miejsce przechowywania danych oraz jako środek do wymiany informacji w efektywnym i bezpiecznym systemie komunikacyjnym.

Z perspektywy ochrony danych ustanowienie tego rodzaju bazy zawsze stwarza pewne ryzyko w odniesieniu do podstawowego prawa do ochrony danych osobowych: udostępnianie większej ilości danych niż jest to absolutnie niezbędne do celów efektywnej współpracy, przetrzymywanie danych, które należało usunąć, oraz przechowywanie nieaktualnych lub niepoprawnych danych; oraz niezapewnianie przestrzegania praw osób, których dane dotyczą, i wypełniania obowiązków przez administratorów. Należy zatem podjąć odpowiednie kroki wobec takiego ryzyka, dbając w tym celu, aby użytkownicy CPCS mieli dobrą znajomość przepisów dotyczących ochrony danych i odpowiednie przeszkolenie w tej dziedzinie oraz potrafili zapewnić zgodność z mającymi zastosowanie przepisami o ochronie danych.

4. RAMY PRAWNE I NADZORCZE DOTYCZĄCE OCHRONY DANYCH

W 1995 r. Unia Europejska ustanowiła ramy prawne dotyczące ochrony danych, a mianowicie dyrektywę o ochronie danych [3], która reguluje przetwarzanie danych osobowych przez państwa członkowskie, oraz rozporządzenie o ochronie danych [4], regulujące przetwarzanie danych osobowych przez instytucje i organy Unii Europejskiej. Stosowanie przepisów dotyczących ochrony danych zależy obecnie od tego, kto jest podmiotem lub użytkownikiem CPCS.

---

[1] Należy zauważyć, że zasady ochrony danych mają zastosowanie zarówno do danych przechowywanych w formie elektronicznej, jak i w formie papierowej.

[2] Aby zapoznać się ze szczegółowymi przepisami dotyczącymi usuwania danych, zob. decyzja 2007/76/WE oraz „Sieć współpracy w zakresie ochrony konsumenta: wytyczne dotyczące funkcjonowania".

[3] Dyrektywa 95/46/WE.

[4] Rozporządzenie (WE) nr 45/2001.

Czynności związane z przetwarzaniem danych przez Komisję reguluje rozporządzenie o ochronie danych, natomiast czynności związane z przetwarzaniem danych przez osoby prowadzące sprawy we właściwych krajowych organach odpowiedzialnych za egzekwowanie prawa są regulowane w przepisach krajowych transponujących dyrektywę o ochronie danych.

Jako dwa główne podmioty pełniące określone funkcje w CPCS, zarówno Komisja, jak i wyznaczone właściwe organy, działając w charakterze współadministratorów, są zobowiązane do zgłaszania i przedstawiania przeprowadzonych przez siebie operacji przetwarzania danych w celu przeprowadzenia kontroli wstępnej przez właściwy organ nadzorczy oraz do zapewniania zgodności z przepisami o ochronie danych. Wspomniane przepisy krajowe transponujące dyrektywę o ochronie danych mogą ustanawiać wyłączenia z wymogów dotyczących zarówno powiadamiania, jak i kontroli wstępnej.

Zharmonizowanie przepisów dotyczących ochrony danych miało na celu zapewnienie wysokiego poziomu ochrony danych oraz zabezpieczenie podstawowych praw osób fizycznych, umożliwiając jednocześnie swobodny przepływ danych osobowych między państwami członkowskimi. Biorąc pod uwagę, że w wyniku wdrożenia krajowych środków wykonawczych mogą obowiązywać różne przepisy, w celu zapewnienia zgodności z przepisami o ochronie danych usilnie zaleca się użytkownikom CPCS omówienie niniejszych wytycznych z krajowymi organami ds. ochrony danych, ponieważ zasady mogą się różnić, np. w zależności od rodzaju informacji przekazywanych osobom fizycznym bądź obowiązku zgłoszenia niektórych operacji związanych z przetwarzaniem danych organom ds. ochrony danych.

Znaczącą cechą ram prawnych UE dotyczących ochrony danych jest sprawowanie nad nimi nadzoru przez niezależne organy ds. ochrony danych. Obywatele mają prawo do składania skarg do takich organów oraz szybkiego rozstrzygnięcia spraw z zakresu ochrony danych bez udziału sądu. Przetwarzanie danych osobowych na poziomie krajowym nadzorują krajowe organy ds. ochrony danych, natomiast przetwarzanie danych osobowych w instytucjach unijnych nadzoruje Europejski Inspektor Ochrony Danych (EIOD) [1]. Działania Komisji są zatem objęte nadzorem EIOD, a działania innych użytkowników CPCS nadzorem krajowych organów ds. ochrony danych.

5. KTO JEST KIM W CPCS – KWESTIA WSPÓŁADMINISTRACJI

CPCS stanowi wyraźny przykład wspólnych operacji przetwarzania i współadministracji. Podczas gdy właściwe organy w państwach członkowskich zajmują się gromadzeniem, rejestrowaniem, ujawnianiem i wymianą danych osobowych, Komisja odpowiada za przechowywanie i usuwanie takich danych na swoich serwerach. Komisja nie ma dostępu do przedmiotowych danych osobowych, ale jest uznawana za kierownika i operatora systemu.

Podział różnych zadań i obowiązków między Komisję i państwa członkowskie można zatem przedstawić w następujący sposób:

— Każdy właściwy organ jest administratorem danych w zakresie swoich czynności związanych z przetwarzaniem danych.

— Komisja nie jest użytkownikiem, ale operatorem systemu, odpowiedzialnym głównie za obsługę techniczną i bezpieczeństwo architektury systemu. Komisja posiada jednak również dostęp do powiadomień, informacji zwrotnych oraz innych informacji dotyczących spraw [2]. Dostęp 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. Komisja nie ma natomiast dostępu do informacji zawartych we wnioskach o wzajemną pomoc i egzekwowanie prawa, ponieważ informacje te są kierowane tylko dla właściwych organów państw członkowskich zajmujących się określoną przedmiotową sprawą. Wspomniane rozporządzenie CPC przewiduje jednak możliwość, by Komisja pomagała właściwym organom w przypadku pewnych sporów [3] i aby była wzywana do uczestnictwa w skoordynowanym dochodzeniu obejmującym więcej niż dwa państwa członkowskie [4].

— Podmioty CPCS ponoszą wspólną odpowiedzialność w zakresie legalności przetwarzania, dostarczania informacji, praw dostępu oraz praw do wniesienia sprzeciwu i do sprostowania.

— Pełniąc role administratorów, Komisja oraz właściwe organy ponoszą indywidualną odpowiedzialność za dopilnowanie, aby przepisy dotyczące ich operacji przetwarzania danych były zgodne z przepisami dotyczącymi ochrony danych.

6. PODMIOTY I UŻYTKOWNICY W CPCS

W ramach CPCS istnieją różne profile dostępu: prawo dostępu do bazy danych jest ograniczone i przypisane wyłącznie do wskazanego z nazwiska urzędnika właściwego organu (uwierzytelnionego użytkownika) i nie podlega przenoszeniu. Dostęp do CPCS może zostać przyznany jedynie urzędnikom zgłoszonym Komisji przez właściwe organy państw członkowskich. Przy uzyskiwaniu dostępu do systemu wymagane jest wprowadzenie identyfikatora logowania/hasła, które można uzyskać za pośrednictwem jednolitego urzędu łącznikowego.

Tylko użytkownicy w ramach właściwego organu, do którego się zwrócono, i właściwego organu wnioskującego mają pełny dostęp do całości wymienianych informacji dotyczących danej sprawy, w tym do wszystkich załączników dokumentacji sprawy w pliku umieszczonym w CPCS. Jednolite urzędy łącznikowe mają dostęp jedynie do kluczowych informacji dotyczących sprawy, pozwalających identyfikować właściwe organy, którym należy przekazać wniosek. Nie mają one dostępu do poufnych dokumentów dołączonych do wniosku lub powiadomienia.

[1] http://www.edps.europa.eu/EDPSWEB/edps/EDPS
[2] Artykuły 8, 9 i 15 rozporządzenia CPC (WE) nr 2006/2004.
[3] Artykuł 8 ust. 5 rozporządzenia CPC (WE) nr 2006/2004.
[4] Artykuł 9 rozporządzenia CPC (WE) nr 2006/2004.

W sprawach dotyczących egzekwowania prawa do ogólnych informacji mają dostęp użytkownicy we wszystkich właściwych organach zgłoszonych jako odpowiedzialne za akty prawne, których naruszenia się dopuszczono. Odbywa się to za pośrednictwem powiadomień. W powiadomieniach tych należy ogólnie opisać daną sprawę i unikać podawania danych osobowych. Od tej zasady mogą istnieć wyjątki, takie jak nazwisko sprzedawcy lub dostawcy (jeśli jest to osoba fizyczna).

Komisja nie ma dostępu do wniosków o udzielenie informacji i egzekwowanie prawa ani do poufnych dokumentów, wpływają do niej jednak notyfikacje i powiadomienia.

7. ZASADY OCHRONY DANYCH MAJĄCE ZASTOSOWANIE DO WYMIANY INFORMACJI

Przetwarzanie danych osobowych przez użytkowników CPCS w państwach członkowskich może odbywać się tylko na warunkach i zgodnie z zasadami ustanowionymi w dyrektywie o ochronie danych. Administrator danych odpowiada za zapewnienie przestrzegania zasad ochrony danych podczas przetwarzania danych osobowych w ramach CPCS.

Należy również zwrócić uwagę na fakt, że w odniesieniu do CPCS zastosowanie mają zarówno zasady dotyczące poufności, jak i ochrony danych. Zasady dotyczące poufności i zasady dotyczące tajemnicy służbowej mogą mieć ogólne zastosowanie do danych, natomiast zasady ochrony danych ograniczają się do danych osobowych.

Należy pamiętać o tym, że użytkownicy CPCS w państwach członkowskich są odpowiedzialni za wiele innych operacji przetwarzania i mogą nie być ekspertami w dziedzinie ochrony danych. Zapewnienie zgodności ochrony danych w CPCS nie powinno być nadmiernie złożone lub stwarzać nadmiernych obciążeń administracyjnych. Nie musi również tworzyć jednolitego i uniwersalnego systemu. Niniejsze wytyczne należy traktować jako zalecenia dotyczące sposobu postępowania z danymi osobowymi, przy czym należy przypomnieć, że nie wszystkie dane wymieniane w ramach CPCS są danymi osobowymi.

Przed wprowadzeniem informacji do CPCS urzędnicy odpowiedzialni za egzekwowanie prawa powinni rozważyć, czy dane osobowe, które zamierzają przesłać, są absolutnie niezbędne do osiągnięcia celu wydajnej współpracy i zastanowić się, komu je wysyłają. Urzędnik odpowiedzialny za egzekwowanie prawa powinien zastanowić się, czy przekazywane informacje są odbiorcy absolutnie niezbędne w celach związanych z powiadomieniem lub wnioskiem o wzajemną pomoc.

Przedstawiona poniżej lista podstawowych zasad dotyczących ochrony danych ma pomóc urzędnikom odpowiedzialnym za egzekwowanie prawa, posiadającym dostęp do CPCS, w ocenie poszczególnych przypadków, mającej na celu ustalenie, czy przepisy w zakresie ochrony danych dotyczące przetwarzania danych osobowych są przestrzegane za każdym razem, gdy przetwarzają dane w systemie. Urzędnicy odpowiedzialni za egzekwowanie prawa powinni również pamiętać, że w odniesieniu do stosowania zasad ochrony danych na poziomie krajowym mogą występować wymienione poniżej wyłączenia i ograniczenia, i dlatego zaleca się, by konsultowali się ze swoimi krajowymi organami ds. ochrony danych [1].

Jakich zasad ochrony danych należy przestrzegać?

Ogólne zasady dotyczące ochrony danych, o których należy pamiętać przed przystąpieniem do przetwarzania jakichkolwiek danych osobowych, zostały zaczerpnięte z dyrektywy o ochronie danych. Ponieważ dyrektywa ta została transponowana do prawa krajowego, osobom prowadzącym sprawy przypomina się, że w kwestii stosowania wymienionych poniżej zasad powinny się konsultować ze swoimi krajowymi nadzorczymi organami ds. ochrony danych, i zaleca się im sprawdzenie, czy w odniesieniu do stosowania tych zasad istnieją jakiekolwiek wyłączenia lub ograniczenia.

Zasada przejrzystości

Zgodnie z dyrektywą o ochronie danych osoba, której dane dotyczą, ma prawo być poinformowana, gdy przetwarzane są jej dane osobowe. Administrator musi podać swoją nazwę i adres, cel przetwarzania, informację o odbiorcach danych oraz wszelkie inne informacje wymagane w celu zapewnienia rzetelności przetwarzania danych [2].

Dane można przetwarzać jedynie w następujących okolicznościach [3]:

— gdy osoba, której dane dotyczą, wyraziła na to zgodę,

— gdy przetwarzanie danych jest konieczne dla realizacji lub zawarcia umowy,

— gdy przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego,

— gdy przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, których dane dotyczą,

[1] Artykuł 11 ust. 2 i art. 13 dyrektywy 95/46/WE.
[2] Artykuły 10 i 11 dyrektywy 95/46/WE.
[3] Artykuł 7 dyrektywy 95/46/WE.

— przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane,

— przetwarzanie danych jest konieczne na potrzeby wynikających z uzasadnionych interesów administratora danych, osoby trzeciej lub osób, którym dane są ujawniane.

Zasada zgodności z prawem i rzetelności

Dane osobowe nie mogą być gromadzone lub przetwarzane w nierzetelny lub bezprawny sposób, nie powinny być również wykorzystywane w celach niezgodnych z celami wskazanymi w rozporządzeniu CPC. By przetwarzanie danych było zgodne z prawem, osoby prowadzące sprawy muszą upewnić się, że są w stanie wskazać wyraźne przyczyny uzasadniające potrzebę dokonania takiego przetworzenia. Dane należy przetwarzać do określonych, jednoznacznych i legalnych celów, a ich dalsze przetwarzanie nie może być niezgodne z tymi celami ([1]). Takie cele mogą zostać przewidziane wyłącznie w rozporządzeniu CPC.

By przetwarzanie danych było rzetelne, osoby, których dotyczą dane, muszą zostać poinformowane o przyczynach, dla których ich dane mają zostać przetworzone, i o istnieniu prawa do dostępu, sprostowania i sprzeciwu.

Zasada proporcjonalności, prawidłowości i okresów przechowywania

Informacje muszą być proporcjonalne, adekwatne, właściwe i nie mogą wykraczać poza cele, dla których są gromadzone lub dalej przetwarzane. Dane muszą być prawidłowe oraz, w razie konieczności, aktualizowane; należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane; dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osób, których dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których zostały zgromadzone lub dla których były przetwarzane. Należy ustanowić odpowiednie środki zabezpieczające dla danych przechowywanych przez dłuższe okresy na potrzeby historyczne, statystyczne i naukowe.

Osoby prowadzące sprawy powinny zastanowić się, czy informacje, które przetwarzają, są absolutnie niezbędne do osiągnięcia wyznaczonych celów.

Zasada celowości

Dane osobowe muszą być zbierane w określonych, jednoznacznych i uzasadnionych celach, o których należy poinformować osobę, której dotyczą dane, i nie mogą być dalej przetwarzane w sposób niezgodny z tymi celami. Osoby prowadzące sprawy powinny przetwarzać dane osobowe tylko wtedy, gdy istnieje ku temu wyraźny powód, tj. w rozporządzeniu CPC wskazane zostały podstawy prawne uzasadniające przekazanie.

Prawa dostępu

Zgodnie z dyrektywą o ochronie danych ([2]) osobom, których dane dotyczą, przysługuje prawo bycia informowanym o fakcie przetwarzania ich danych osobowych, celach tego przetwarzania, odbiorcach, którym dane te są przekazywane, oraz o tym, że przysługują im określone prawa, tj. prawo do informacji i sprostowania. Osoba, której dane dotyczą, ma prawo dostępu do wszystkich tych przetwarzanych danych. Osoba ta ma również prawo zwrócić się z wnioskiem o sprostowanie, usunięcie lub zablokowanie danych, które są niekompletne, nieprawidłowe lub przetwarzane niezgodnie z przepisami o ochronie danych ([3]).

Dane szczególnie chronione

Przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych i danych dotyczących stanu zdrowia, życia seksualnego, popełnionych przestępstw i wyroków skazujących jest zabronione. Dyrektywa o ochronie danych ([4]) przewiduje jednak pewne odstępstwa od tej zasady i dane szczególnie chronione mogą być przetwarzane na określonych warunkach ([5]). Ponieważ użytkownicy CPCS mogą znaleźć się w sytuacji, w której będą mieli styczność z danymi szczególnie chronionymi ([6]), zaleca się zachowanie ostrożności w odniesieniu do takich danych. Użytkownikom CPCS zaleca się skonsultowanie się ze swoim krajowym organem ochrony danych, czy w stosunku do przetwarzania szczególnie chronionych danych mają zastosowanie odstępstwa.

Wyłączenia

Dyrektywa o ochronie danych dopuszcza pewne wyłączenia w kontekście zapobiegania, badania, wykrywania i karania przestępstw. Osobom prowadzącym sprawy zaleca się zapoznanie się z prawem krajowym w celu dokonania oceny, czy i w jakim zakresie możliwe jest zastosowanie takich wyłączeń ([7]). Przy stosowaniu tego rodzaju wyłączeń zaleca się, by były one wyraźnie wskazane w oświadczeniu o ochronie prywatności każdego właściwego organu.

([1]) Artykuł 6 ust. 1 lit. b) dyrektywy 95/46/WE.
([2]) Artykuły 10, 11 i 12 dyrektywy 95/46/WE.
([3]) Artykuł 12 dyrektywy 95/46/WE.
([4]) Artykuł 8 ust. 2 dyrektywy 95/46/WE.
([5]) Artykuł 8 dyrektywy 95/46/WE.
([6]) Rozdział 4 załącznika do decyzji 2007/76/WE.
([7]) Opinia 6/2007 na temat problematyki ochrony danych związanej z systemem współpracy w zakresie ochrony konsumenta (CPCS) 01910/2007/EN – WP 130 – przyjęta w dniu 21 września 2007 r., s. 24–26.

Stosowanie zasad ochrony danych

Stosowanie przedmiotowych zasad ochrony danych w zakresie funkcjonowania CPCS prowadzi do sformułowania następujących zaleceń:

1. Stosowanie CPCS powinno ograniczać się wyłącznie do celów wyznaczonych w rozporządzeniu CPC. W art. 13 ust. 1 rozporządzenia CPC stwierdza się, że przekazane informacje mogą być wykorzystywane wyłącznie w celu zapewnienia przestrzegania przepisów prawnych chroniących interesy konsumentów. Przedmiotowe przepisy prawne wymienione są w załączniku do rozporządzenia CPC.

2. Zaleca się, aby urzędnicy odpowiedzialni za egzekwowanie prawa wykorzystywali informacje uzyskane za pośrednictwem wniosku o wzajemną pomoc lub powiadomienia wyłącznie w celach związanych z tą konkretną sprawą, w pełnej zgodności z wymogami przepisów prawa w zakresie ochrony danych, oraz oceniali *ex ante* konieczność przetwarzania w kontekście dochodzeń prowadzonych w szerszym interesie publicznym.

3. Przy przekazywaniu danych urzędnicy odpowiedzialni za egzekwowanie prawa dokonują oceny poszczególnych przypadków pod kątem odbiorców przetwarzanych informacji.

4. Użytkownicy CPCS powinny uważnie wybierać pytania zadawane we wniosku o wzajemną pomoc i nie powinni wnosić o uzyskanie większej ilości danych, niż jest to konieczne. Nie chodzi jedynie o kwestię przestrzegania zasad dotyczących jakości danych, ale również o kwestię zmniejszenia obciążenia administracyjnego.

5. Zgodnie z dyrektywą o ochronie danych [1] dane osobowe muszą być prawidłowe i aktualizowane. Zaleca się, aby właściwy organ, który dostarczył informacje, uczestniczył w zapewnieniu prawidłowości danych przechowywanych w CPCS. Do funkcji CPCS dodano komunikaty typu pop-up w celu okresowego przypominania osobom prowadzącym sprawy o sprawdzeniu prawidłowości i aktualności danych osobowych.

6. Praktycznym sposobem informowania osób, których dane dotyczą, o przysługujących im prawach jest stworzenie strony internetowej zawierającej wyczerpującą informację o polityce prywatności. Zaleca się, aby każdy właściwy organ posiadał stronę z informacją o polityce prywatności na swoich stronach internetowych. Każda informacja o polityce prywatności powinna być zgodna ze wszystkimi wymogami w zakresie informacji ustanowionymi w dyrektywie o ochronie danych i powinna zawierać odsyłacz do strony internetowej Komisji zawierającej informację o polityce prywatności oraz dalsze szczegóły, w tym dane kontaktowe danego właściwego organu, jak i wszelkie krajowe ograniczenia prawa dostępu lub prawa do informacji. Wszyscy zaangażowani administratorzy danych odpowiedzialni są za dopilnowanie, aby opublikowano informacje o polityce prywatności.

7. Osoba, której dane dotyczą, może wystosować wniosek o udzielenie dostępu do swoich danych osobowych, ich poprawienie lub usunięcie w odniesieniu do większej liczby źródeł niż jedno. Mimo że każdy właściwy organ jako administrator danych odpowiada za swoje własne operacje przetwarzania danych, należy udzielać skoordynowanej odpowiedzi na wnioski dotyczące spraw o charakterze transgranicznym. Zaleca się, aby w takich przypadkach właściwe organy informowały pozostałe zainteresowane właściwe organy o otrzymaniu wniosku.

   Jeżeli właściwy organ uzna, że pozytywne rozpatrzenie wniosku może mieć wpływ na postępowanie wyjaśniające lub egzekucyjne prowadzone przez inne właściwe organy, powinien zwrócić się do takich właściwych organów o wydanie opinii przed pozytywnym rozpatrzeniem wniosku.

   Osoba, której dane dotyczą, może również zwrócić się z wnioskiem do Komisji. Komisja może pozytywnie rozpatrzeć wniosek jedynie w odniesieniu do danych, do których ma dostęp. Po otrzymaniu wniosku Komisja powinna skonsultować się z właściwym organem, który dostarczył informacje. W przypadku braku zastrzeżeń lub odpowiedzi ze strony właściwego organu we właściwym czasie Komisja może podjąć decyzję w zakresie rozpatrzenia wniosku na podstawie rozporządzenia o ochronie danych. Komisja powinna również zwrócić się o opinię do właściwych organów, których działania dochodzeniowe lub działania w zakresie egzekwowania prawa mogą być narażone w rezultacie pozytywnego rozpatrzenia wniosku. Komisja powinna zbadać, czy wprowadzenie do CPC dodatkowych funkcji technicznych ułatwiłoby taką wymianę.

8. Decyzja wykonawcza CPC 2007/76/WE zapewnia ustanowienie pól danych w CPCS przeznaczonych na wprowadzenie nazwisk dyrektorów przedsiębiorstw. Urzędnicy odpowiedzialni za egzekwowanie prawa muszą ocenić, czy włączenia tego rodzaju danych osobowych jest konieczne dla rozwiązania sprawy. Oceny poszczególnych przypadków co do konieczności zamieszczenia nazwiska dyrektora przedsiębiorstwa w przeznaczonym do tego polu danych należy dokonywać przed każdym wprowadzeniem informacji do CPCS i przed wysłaniem powiadomienia lub wniosku o wzajemną pomoc do innego właściwego organu.

9. Zgodnie z decyzją wykonawczą CPC 2007/76/WE właściwy organ zamieszczający wnioski o udzielenie informacji lub wnioski o egzekwowanie prawa, lub powiadomienia musi określić, czy dane informacje mają być traktowane jako poufne. Decyzję tę należy podejmować oddzielnie dla każdej sprawy. Podobnie organ, do którego się zwrócono, musi określić przy dostarczaniu informacji, czy informacje mają być traktowane jako poufne. CPCS posiada funkcję wartości domyślnej, za pomocą której użytkownicy CPCS muszą wyraźnie udzielić dostępu do dokumentów poprzez odznaczenie flagi poufności.

[1] Artykuł 6 ust. 1 lit. d) dyrektywy 95/46/WE.

8. CPCS A OCHRONA DANYCH

Środowisko przyjazne ochronie danych

CPCS został zaprojektowany z uwzględnieniem wymogów przepisów o ochronie danych:

— CPCS wykorzystuje sieć s-TESTA (*secured Trans European Services for Telematics between Administrations* – zabezpieczona transeuropejska telematyczna sieć komunikacyjna między organami administracji). Oferuje ona zarządzaną, wiarygodną i bezpieczną platformę ogólnoeuropejskiej komunikacji dla krajowych i europejskich organów administracji. Sieć s-TESTA opiera się na wyspecjalizowanej infrastrukturze prywatnej, całkowicie odrębnej od Internetu. Do projektu systemu wprowadzono odpowiednie środki bezpieczeństwa w celu zapewnienia możliwie najlepszej ochrony sieci. Sieć jest przedmiotem akredytacji w zakresie bezpieczeństwa po to, by za jej pośrednictwem można było przekazywać informacje niejawne opatrzone klauzulą „EU Restricted".

— Wprowadzono szereg funkcji technicznych: bezpieczne i indywidualne hasła dla zgłoszonych właściwych urzędników w wyznaczonych organach, zastosowanie bezpiecznej sieci (s-TESTA), wyskakujące komunikaty, które przypominają osobom prowadzącym sprawy o uwzględnieniu przepisów dotyczących ochrony danych podczas przetwarzania danych osobowych, tworzenie różnych profili użytkowników o różnym stopniu dostępu do informacji w zależności od roli użytkownika (właściwy organ, jednolity urząd łącznikowy, Komisja), możliwość ograniczenia dostępu do dokumentów dzięki zdefiniowaniu ich jako poufne i wiadomość na stronie głównej CPCS wskazująca przepisy dotyczące ochrony danych.

— Przepisy wykonawcze [1], których zakres obejmuje kluczowe aspekty zapewniania przestrzegania ochrony danych: jasne przepisy dotyczące usuwania danych (rodzaju informacji, sposobu i czasu usuwania danych); przepisy określające rodzaje dostępu do informacji (wyłącznie bezpośrednio zaangażowane właściwe organy mają pełny dostęp, a pozostałe organy posiadają jedynie ogólne informacje).

— Wytyczne operacyjne [2] z dalszymi wyjaśnieniami, co należy uwzględnić przy wypełnianiu różnych pól danych oraz w jaki sposób wprowadzać niniejsze wytyczne [3].

— Przeglądy roczne w celu dopilnowania, aby właściwe organy weryfikowały prawidłowość danych osobowych (planowane jest znakowanie, ale nie zostało dotychczas wdrożone), a także w celu dopilnowania, aby zamykano sprawy lub je usuwano jak przewidziano w przepisach, aby mieć pewność, że sprawy nie zostaną zapomniane. Komisja wraz z państwami członkowskimi organizuje regularnie systematyczny przegląd spraw, które były otwarte przez okres znacznie dłuższy niż średni okres zajmowania się sprawą.

— Automatyczne usuwanie spraw dotyczących wzajemnej pomocy po 5 latach od zamknięcia sprawy zgodnie z wymogami rozporządzenia CPC.

— CPCS to rozwijające się narzędzie informatyczne, które ma być przyjazne dla ochrony danych. Do architektury systemu wbudowano wiele funkcji zabezpieczających, które opisano powyżej. Zgodnie z wymogami Komisja zamierza wprowadzać dalsze usprawnienia.

Dodatkowe wytyczne

Jak długo należy przechowywać sprawę i kiedy należy ją zamknąć i usunąć?

Wyłącznie Komisja może usuwać informacje z CPCS [4] i zazwyczaj dokonuje tego na wniosek właściwego organu. Występując z takim wnioskiem, właściwy organ musi określić podstawy wniosku o usunięcie. Jedynym wyjątkiem są wnioski w sprawie egzekwowanie prawa. Komisja usuwa je automatycznie po 5 latach od zamknięcia sprawy przez wnioskujący organ.

Przepisy podające terminy ustanowiono w celu zapewnienia usuwania danych, które nie są w dalszym ciągu wymagane, są nieprawidłowe, okazały się bezpodstawne lub osiągnęły maksymalny okres przechowywania.

Dlaczego okres przechowywania danych określono na 5 lat?

Celem 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 i spójności egzekwowania przepisów prawnych, które chronią interesy konsumentów, monitorowania ochrony interesów ekonomicznych konsumentów oraz przyczynianie się do zwiększenia jakości i konsekwentności egzekwowania prawa. 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.

[1] Decyzja 2007/76/WE.
[2] Sieć współpracy w zakresie ochrony konsumenta: wytyczne operacyjne – zatwierdzone przez Komitet ds. Współpracy w dziedzinie Ochrony Konsumentów dnia 8 czerwca 2010 r.
[3] Treść niniejszych wytycznych zostanie włączona do przyszłych szkoleń w zakresie CPCS.
[4] Artykuł 10 rozporządzenia CPC (WE) nr 2006/2004 i rozdział 2 załącznika do decyzji wykonawczej CPC 2007/76/WE.

Jakie informacje obejmuje zakres forum dyskusyjnego?

Do CPCS dołączone zostało forum dyskusyjne, które jest narzędziem przeznaczonym do wymiany informacji w kwestiach takich jak nowe uprawnienia w zakresie egzekwowania prawa i najlepsze praktyki. Zasadniczo forum dyskusyjne, mimo że rzadko korzystają z niego urzędnicy odpowiedzialni za egzekwowanie prawa, nie powinno służyć do wymiany danych związanych ze sprawami i nie powinno zawierać odniesień do danych osobowych.

Jakie dane można zamieszczać w krótkich streszczeniach i dołączonych dokumentach?

W decyzji wykonawczej CPC 2007/76/WE przewidziano pole danych „dołączone dokumenty" w przypadku powiadomień, wniosków o udzielenie informacji i wniosków o egzekwowanie prawa. Krótkie streszczenia to pola, w których należy opisać naruszenie. Zaleca się, aby nie umieszczać danych osobowych w krótkich streszczeniach, ponieważ celem tego pola danych jest uzyskanie ogólnego opisu naruszenia. Dane osobowe zawarte w dołączonych dokumentach, które nie są ściśle wymagane, należy zaczernić lub usunąć.

Co oznacza „uzasadnione podejrzenie" – to, że miało miejsce naruszenie?

Uzasadnione podejrzenie należy interpretować zgodnie z prawem krajowym. Zaleca się jednak, aby podejrzewane naruszenie włączać do CPCS tylko, jeżeli istnieją dowody na poparcie sprawy, że doszło do naruszenia lub że zajście naruszenia jest prawdopodobne.

A co w kwestii przekazywania informacji państwom trzecim?

Zgodnie z rozporządzeniem CPC [1] informacje przekazane na podstawie rozporządzenia CPC mogą również zostać przekazane organowi państwa trzeciego przez państwo członkowskie na podstawie umowy w sprawie dwustronnej pomocy, pod warunkiem uzyskania zgody właściwego organu, który jako pierwszy przekazał informacje, oraz spełnienia wymogów przepisów w zakresie ochrony danych.

Zaleca się, aby wobec braku międzynarodowej umowy Unii Europejskiej w sprawie ustaleń o wzajemnej pomocy [2] z państwem trzecim wszelkie umowy w sprawie dwustronnej pomocy zawierane z danym państwem trzecim zapewniały właściwe zabezpieczenie w zakresie ochrony danych i aby odpowiednie organy nadzorcze ds. ochrony danych były o nich powiadamiane, tak aby można było przeprowadzić wcześniejszą kontrolę, chyba że Komisja ustaliła, że dane państwo trzecie zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z Unii zgodnie z art. 25 dyrektywy o ochronie danych.

---

[1] Artykuł 14 ust. 2 rozporządzenia CPC (WE) nr 2006/2004.
[2] Artykuł 18 rozporządzenia CPC (WE) nr 2006/2004.