



STANOWISKO RZĄDU

I. METRYKA DOKUMENTU

Tytuł
SPRAWOZDANIE KOMISJI DLA RADY I PARLAMENTU EUROPEJSKIEGO Sprawozdanie z oceny dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE)

Data otrzymania dokumentu przez Parlament RP	Data przyjęcia stanowiska przez Komitet do Spraw Europejskich
2 maja 2011 r.	7 czerwca 2011 r.

Sygnatury			
Komisja Europejska	COM(2011) 225	Rada UE	9324/11

Instytucja wiodąca
Ministerstwo Infrastruktury

Instytucje współpracujące
Ministerstwo Sprawiedliwości Ministerstwo Spraw Wewnętrznych i Administracji

II. CEL DOKUMENTU

Sprawozdanie Komisji przedstawia wyniki, przeprowadzonej na podstawie art. 14 dyrektywy 2006/24/WE, oceny stosowania tej dyrektywy przez państwa członkowskie oraz jej wpływu na podmioty gospodarcze i konsumentów, z uwzględnieniem rozwoju technologii łączności elektronicznej oraz udostępnionych Komisji danych statystycznych. Celem sprawozdania jest określenie ewentualnej potrzeby zmodyfikowania przepisów dyrektywy, zwłaszcza w odniesieniu do zakresu danych oraz okresów zatrzymywania.

III. DOKUMENTY POWIĄZANE

Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE (Dz. Urz. UE L 105 z 13.04.2006, str. 54-63).

IV. STANOWISKO RZĄDU

Rzeczpospolita Polska postrzega instrument zatrzymywania i przechowywania (retencji) danych jako mający istotne znaczenie dla zapewnienia sprawnego i skutecznego wykonywania zadań przez uprawnione podmioty¹, których zadaniem jest zapewnienie bezpieczeństwa państwa i obywateli.

Równocześnie dostrzega konieczność właściwego wyważenia i zabezpieczenia z jednej strony prawa do prywatności, a z drugiej prawa do życia w bezpiecznym otoczeniu.

Rzeczpospolita Polska docenia działania Komisji Europejskiej zmierzające do dokonania oceny funkcjonowania w praktyce przepisów dyrektywy w poszczególnych państwach członkowskich. Rzeczpospolita Polska pozostaje otwarta na dalszą współpracę i dyskusję nad ewentualną potrzebą i zakresem zmian aktualnie funkcjonujących rozwiązań prawnych. Wymaga to jednak dalszej analizy i wymiany poglądów pomiędzy wszystkimi zainteresowanymi stronami.

Odnosząc się do głównych kwestii poruszonych w omawianym sprawozdaniu Rzeczpospolita Polska prezentuje następujące stanowisko:

1. Przedmiot i zakres stosowania dyrektywy, cel zatrzymywania danych – Rzeczpospolita Polska opowiada się za pozostawieniem obecnych rozwiązań.
2. Dostęp do danych: organy, procedura i warunki – Rzeczpospolita Polska pozostaje otwarta na dyskusję odnośnie określenia zasad dostępu do danych.
3. Zakres zatrzymywanych danych i kategorie danych objętych zatrzymaniem – Rzeczpospolita Polska popiera pozostawienie obecnego katalogu zatrzymywanych danych, przy ewentualnym doprecyzowaniu ich zakresów definicyjnych.
4. Okres zatrzymywania – zdaniem Rzeczpospolitej Polskiej, obecny przedział okresu zatrzymywania danych (od 6 miesięcy do dwóch lat) winien – co do zasady - zostać utrzymany. Rzeczpospolita Polska jest otwarta na współpracę w zakresie możliwości zróżnicowania okresów retencji w odniesieniu do poszczególnych rodzajów danych.
5. Wykorzystanie przedpłaconych kart SIM (kart prepaid) – Rzeczpospolita Polska przyjmuje argumenty Komisji odnośnie braku konieczności uregulowania na poziomie Unii Europejskiej kwestii rejestracji kart prepaid.
6. Zwrot wydatków przedsiębiorcom telekomunikacyjnym, poniesionych w związku z retencją danych – Rzeczpospolita Polska opowiada się za pozostawieniem obecnych rozwiązań, tj. pozostawieniem tych kwestii do swobodnej decyzji państw członkowskich.
7. Dane statystyczne – Rzeczpospolita Polska popiera zapowiedzianą w raporcie analizę Komisji w zakresie zasad raportowania i sporządzania statystyk.

¹ Podmioty, o których mowa w art. 179 ust. 3 pkt 1 lit. a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.): Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne, wywiad skarbowy

V. UZASADNIENIE STANOWISKA RZĄDU

Sprawozdanie Komisji Europejskiej jest dokumentem o charakterze informacyjnym, który będzie stanowił tło późniejszych zmian legislacyjnych dotyczących zatrzymywania danych. Stanowisko Rzeczypospolitej Polskiej jest wobec tego odpowiednio ogólne, pozostawiając dyskutowane kwestie otwartymi i zachowując właściwą elastyczność negocjacyjną. Na obecnym wczesnym etapie przeglądu dyrektywy 2006/24/WE nie jest możliwe zidentyfikowanie konsekwencji gospodarczych, budżetowych, społecznych oraz legislacyjnych przyszłych zmian.

Stanowisko Rzeczypospolitej Polskiej przedstawione w punkcie IV w odniesieniu do niektórych istotnych kwestii wynikających z implementacji i stosowania dyrektywy, ma charakter kierunkowy i nie przesądzający o ostatecznym stanowisku dotyczącym konkretnych przyszłych rozwiązań.

W uzasadnieniu do głównych kwestii poruszonych w sprawozdaniu:

1. Przedmiot i zakres stosowania dyrektywy, cel zatrzymywania danych - m.in. definicja poważnego przestępstwa (*serious crime*)

Zgodnie z art. 1 dyrektywy, jej celem jest zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego.

W ocenie Rzeczypospolitej Polskiej, sprecyzowany w powyższy sposób przedmiot i zakres stosowania przepisów odnoszących się do retencji danych wciąż pozostaje korzystnym, kompromisowym rozwiązaniem. Należy bowiem mieć na uwadze różnorodność porządków prawnych państw członkowskich oraz rozwiązań dotyczących funkcjonowania służb porządku publicznego, prokuratury oraz sądownictwa. Ewentualne zmiany przedmiotu i zakresu stosowania dyrektywy muszą uwzględniać wyżej wskazaną różnorodność porządków prawnych państw członkowskich i nie ograniczać możliwości skutecznego i szybkiego działania organów państwa na rzecz bezpieczeństwa obywateli i państwa.

W przypadku rozpatrywania różnych propozycji zdefiniowania pojęcia poważnego przestępstwa (*serious crime*) należy mieć na uwadze w szczególności różnice w zagrożeniu karą tego samego przestępstwa w poszczególnych państwach członkowskich. Przyjęcie sztywnej definicji w oparciu np. o wymiar kary nie jest rozwiązaniem, które pozwoli na harmonizację wykorzystania danych retencyjnych. Wskazane byłoby, aby poza kryterium zagrożenia karą pozbawienia wolności definicja umożliwiała wykorzystanie danych retencyjnych w przypadku ścigania sprawców przestępstw popełnianych głównie

za pomocą sieci telekomunikacyjnych np. grooming², stalking³ lub tzw. pozytywna pedofilia. Można również rozważyć zawarcie zapisów umożliwiających wykorzystanie danych retencyjnych do ratowania życia ludzkiego jak i poszukiwania osób, np. w przypadku osób, które planują targnąć się na własne życie.

2. Dostęp do danych: organy, procedura i warunki

Z uwagi na skomplikowaną materię i konieczność wyważenia różnych wartości kwestia właściwych organów i procedur dostępu do danych wymaga dalszej pogłębionej analizy i debaty. Dążąc do stworzenia warunków, w których ingerencja organów państwa w prywatność obywateli zostanie ograniczona do niezbędnego minimum i będzie skutecznie kontrolowana w toku przewidzianych prawem procedur, należy również mieć na uwadze potrzebę umożliwienia odpowiednim służbom i organom prowadzenia skutecznych działań mających na celu ochronę struktur zarówno poszczególnych państw członkowskich jak i Unii Europejskiej jako całości, a także ochronę bezpieczeństwa obywateli Unii Europejskiej.

Rzeczpospolita Polska pozostając otwarta na dyskusję odnośnie określenia zasad dostępu do danych, wskazuje przy tym, że:

- priorytetową kwestią jest zapewnienie szybkiego i sprawnego uzyskania przez właściwe służby informacji koniecznych do wykonywania zadań związanych ze zwalczaniem przestępczości,
- postulat kontroli sądowej wszystkich przypadków pozyskiwania danych wydają się być mało funkcjonalny. Godne rozważenia byłyby natomiast inne koncepcje niezależnej kontroli działania organów pozyskujących dane, które zapewnią szybkie i sprawne pozyskiwanie danych, np. kontrola następcza,
- zasady muszą uwzględniać specyfikę postępowań przygotowawczych i sądowych w poszczególnych państwach członkowskich,
- rozważyć można przykładowo możliwość ograniczenia zbierania danych przez uprawnione instytucje w zależności od rodzaju ściganych przez nie przestępstw.

Odnośnie zapytań o udostępnienie danych w Rzeczpospolitej Polskiej podkreślić należy, że na liczbę zapytań mogą mieć wpływ czynniki natury technicznej. W przypadku Rzeczpospolitej Polskiej liczba zapytań w dużej mierze może być spowodowana brakiem jednego systemu ewidencjonującego abonentów poszczególnych przedsiębiorców telekomunikacyjnych, przez co ustalenie abonenta skutkuje zapytaniem o ten sam numer (abonenta) do wielu przedsiębiorców telekomunikacyjnych. Ponadto systemy informatyczne, które wykorzystywane są do uzyskiwania takich danych zmuszają do dzielenia zapytań (np. dotyczących bilingów) na czasokresy. Przykładowo zapytanie o biling za 1 rok powoduje często konieczność kierowania 4 zapytań za 3 miesięczne

² Grooming - działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć jego opory i później je seksualnie wykorzystać. Pot. uwodzenie dzieci za pośrednictwem Internetu

³ Stalking - uporczywe, złośliwe nagabywanie, które może wywołać poczucie zagrożenia

okresy. Porównując liczby zapytań należy mieć zatem na względzie zasady liczenia skierowanych zapytań.

3. Zakres zatrzymywanych danych i kategorie danych objętych zatrzymaniem

Zdaniem Rzeczypospolitej Polskiej katalog danych nie wymaga dokonania zmian. Natomiast konieczne może się okazać doprecyzowanie niektórych danych, w taki sposób aby były one jednoznacznie interpretowane przez państwa członkowskie.

Dalszej analizie, w tym w zakresie praktycznej możliwości wykonywania, wymaga propozycja Parlamentu Europejskiego dotycząca poszerzenia katalogu o dane dotyczące wyszukiwarek „*w celu szybkiego uporania się z pornografią dziecięcą oraz przestępstwami seksualnymi, rozpowszechnianą i popełnianymi z wykorzystaniem internetu*”⁴ (pisemna opinia Parlamentu Europejskiego z dnia 19 kwietnia 2010 r., dok. 0029/2010).

4. Okres zatrzymywania

W ocenie Rzeczypospolitej Polskiej określony w dyrektywie przedział okresu zatrzymywania danych (od 6 miesięcy do dwóch lat) winien - co do zasady - zostać utrzymany. Umożliwia bowiem elastyczne podejście i dostosowanie przewidzianych prawem wewnętrznym okresów zatrzymywania danych do uwarunkowań prawnych i organizacyjnych poszczególnych państw członkowskich.

Regulacje dotyczące retencji danych pełnią ważną rolę w postępowaniu karnym na etapie postępowania przygotowawczego, jak i sądowego. Dane uzyskiwane przez m.in. Policję, prokuraturę lub sąd stanowią istotny materiał dowodowy, który może służyć do wykrycia sprawcy przestępstwa, czy ustalenia źródeł dowodowych (najczęściej świadków), dzięki którym możliwe jest ustalenie winy sprawcy i jego ostateczne skazanie (lub uniewinnienie). Tym samym przepisy regulujące kwestię retencji przedmiotowych danych przyczyniają się do wzmocnienia skuteczności postępowania karnego.

Ewentualna modyfikacja okresu przechowywania danych znacząco ograniczy zakres stosowania dyrektywy, stawiając pod znakiem zapytania efektywność działań operacyjnych organów ścigania oraz czynności procesowych dokonywanych w toku postępowania karnego, co będzie miało zdecydowanie negatywny wpływ na ich tok i wynik, utrudniając walkę z przestępczością, zwłaszcza zorganizowaną. Z praktyki wynika, że dane starsze niż 6 miesięcy, a nawet rok niezbędne są zwłaszcza w przypadku skomplikowanych spraw dotyczących grup przestępczych. Zbyt krótki okres przechowywania danych może okazać się niewystarczający do ich efektywnego wykorzystania, a zdobywane dane będą mogły służyć jedynie w niektórych postępowaniach dotyczących przestępstw, co do których organy ścigania zostały zawiadomione niezwłocznie po ich popełnieniu. Dla ścigania innych czynów zabronionych przepisy dotyczące retencji danych staną się bezprzedmiotowe i bezużyteczne.

Rzeczpospolita Polska pozostaje otwarta na współpracę w zakresie możliwości różnicowania okresów retencji w odniesieniu do poszczególnych rodzajów danych.

Przykładowo możliwe do zaakceptowania byłoby skrócenie górnej granicy okresu retencji w odniesieniu do danych uzyskiwanych przez podmioty świadczące usługi drogą elektroniczną (tzw. internet data).

Odnosząc się do danych statystycznych zawartych w raporcie zauważyć należy, że z danych ilościowych wynika, że 90 % danych, o które zwracają się uprawnione podmioty jest młodsza niż 6 miesięcy, przy czym tylko w 6 państwach członkowskich okres retencji przekracza 1 rok, a w części państw okres zatrzymywania danych wynosi właśnie 6 miesięcy. Oczywistym zatem pozostaje, że w znacznej części państw nie jest możliwe składanie zapytań o dane starsze niż 6 miesięcy. Statystyki te, bez uwzględniania powyższego zróżnicowania przepisów wewnętrznych, mogą zatem być mylące. Celowym byłoby ustalenie przez Komisję Europejską, w ilu przypadkach i w sprawach o jakim ciężarze gatunkowym, w państwach członkowskich, zbyt krótki okres zatrzymywania danych uniemożliwił wykrycie i ukaranie sprawców przestępstw, a tym samym spowodował zagrożenia dla bezpieczeństwa państwa i obywateli.

5. Wykorzystanie przedpłaconych kart SIM (kart prepaid)

Rzeczpospolita Polska przychyła się do stanowiska Komisji Europejskiej zawartego w sprawozdaniu odnośnie braku konieczności uregulowania kwestii na poziomie unijnym.

Większość państw członkowskich uważa, iż rejestracja pre-paidów może być trudna do zrealizowania, także ze względu na duże koszty wynikające z rejestracji dla przedsiębiorców.

6. Zwrot wydatków.

Przedstawione w sprawozdaniu Komisji dane nie stanowią wystarczającego uzasadnienia dla dokonania zmiany istniejącego stanu prawnego na poziomie unijnym w odniesieniu do zwrotu kosztów przedsiębiorcom telekomunikacyjnym, poniesionych w związku z retencją danych. Na chwilę obecną kwestia ta winna zostać w pozostawiona do swobodnej decyzji państw członkowskich.

7. Dane statystyczne

Rzeczpospolita Polska pozostaje otwarta na dalszą współpracę celem wypracowania jak najlepszych zasad przekazywania danych niezbędnych dla sporządzania statystyk. W konsekwencji Rzeczpospolita Polska popiera zapowiedzianą w raporcie analizę Komisji w przedmiotowym zakresie.

⁴ Oryg. - *in order to tackle online child pornography and sex offending rapidly*

VI. STANOWISKO PARTNERÓW SPOŁECZNYCH

Spośród konsultowanych partnerów społecznych w stosunku do sprawozdania stanowisko zajęli Pracodawcy RP.

Zdaniem Pracodawców RP, przeprowadzenie przez Komisję Europejską przeglądu dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE należy uznać za pożyteczne.

Tematyka dyrektywy należy do trudnych z tego względu, iż dotyczy wszystkich obywateli Unii Europejskiej. Implementacja dyrektywy okazała się skomplikowanym przedsięwzięciem, o czym świadczy chociażby fakt, iż w Austrii i Szwecji projekt przepisów implementujących jest nadal przedmiotem debaty krajowej⁵. Obydwa te państwa zostały uznane przez Trybunał Sprawiedliwości za winne naruszenia zobowiązań wynikających z prawa Unii Europejskiej. W trzech z krajów⁶ Unii, które dokonały implementacji dyrektywy sądy konstytucyjne uchylły krajowe przepisy. Państwa te nie dokonały ponownej transpozycji. Wnioski, do których doszła Komisja Europejska w związku z przeprowadzonym przeglądem pozwalają sądzić, iż zmiana dyrektywy 2006/24/WE będzie szła w kierunku korzystnym nie tylko dla przedsiębiorców telekomunikacyjnych, ale również dla ogółu społeczeństwa.

Na dzień dzisiejszy Pracodawcy RP zauważają, iż:

1. Polska poszła za daleko w implementacji dyrektywy 2006/24/WE i wprowadziła maksymalny dwuletni okres retencji danych, chociaż nie jest państwem szczególnie zagrożonym np. terroryzmem. W państwach Unii, w których miały miejsce ataki terroryzmu, jak Wielka Brytania czy Hiszpania, okres retencji danych wynosi jeden rok. W Polsce tak długi i niezwykle kosztowny dla operatorów okres przetrzymywania danych w naszej ocenie jest niczym nie uzasadniony. Można stwierdzić, iż takie podejście jest spowodowane zbyt długim czasem postępowania wymiaru sprawiedliwości niż faktycznym zagrożeniem bezpieczeństwa. W związku z powyższym należałoby obligatoryjnie zmniejszyć czas przechowywania danych poddanych retencji do jednego roku.
2. Prawo do sięgania po dane retencyjne jest masowo w Polsce wykorzystywane do spraw błahych. Potrzebne byłoby określenie w dyrektywie kategorii spraw, przy których można sięgać po dane. Należy ocenić pozytywnie fakt, iż Komisja dostrzega potrzebę zmian dyrektywy w tym zakresie, zalecając *„spójne stosowanie zasady celowości w odniesieniu do zatrzymywanych danych oraz określenie przestępstw, w przypadku których można uzyskać dostęp do danych i korzystać z nich”*.
3. Komisja zaleca ograniczenie liczby organów upoważnionych do dostępu do danych oraz zagwarantowanie niezależnego nadzoru nad wnioskami o uzyskanie dostępu, a także zbadanie ogólnego reżimu zatrzymywania danych i uzyskiwania do nich dostępu we wszystkich państwach członkowskich. W Polsce też powinno się podjąć prace w tym zakresie. Obok Malty, Irlandii i Słowacji, gdzie do uzyskania danych konieczne jest jedynie złożenie wniosku, tylko w Polsce (na 22 kraje członkowskie) stosowana jest również taka procedura.
4. Należałoby zastanowić się czy udostępnianie danych nie powinno być traktowane jako odpłatna usługa. W Polsce po ostatniej nowelizacji ustawy - Prawo telekomunikacyjne

⁵ Art. 15 dyrektywy 2006/24/WE przewidywał termin implementacji do 15 września 2007 r.

⁶ Republika Czeska, Niemcy, Rumunia

zniesiono jakąkolwiek odpłatność za udostępnianie danych, nawet w sprawach karnych i cywilnych. Nie ma żadnego uzasadnienia, aby w sprawach np. cywilnych udostępnianie danych odbywało się na koszt operatora. Taki stan rzeczy powoduje, że prokuratury i sądy nie dokonują celowościowej analizy jaki zakres danych będzie im potrzebny w sprawie i czy żądanie o udostępnienie danych jest zasadne. Zdarzają się więc przypadki, że do operatora trafia wnioski o sprawdzenie np. 300 numerów IP w sprawie cywilnej o 70 zł. Biorąc za przykład dane z Finlandii można wyliczyć, że za zrealizowanie 4070 wniosków o udostępnienie danych operatorzy otrzymali zwrot 1 mln euro, co daje 245 euro / 1 wniosek. Przyjmując, iż w Polsce rozpatrzono 1 048 318 wniosków daje to kwotę ok. 257 mln euro, czyli ok. 1 mld zł. Przystosowanie techniczne sieci, retencja danych (w Polsce – najdłuższa w Europie) i ich późniejsze udostępnianie są bardzo kosztowne dla operatorów. Dostrzega to w swoim sprawozdaniu Komisji i zapowiada rozważenie sposobów zapewnienia spójnego systemu zwrotu wydatków operatorom.

Pracodawcy RP uważają, że warto wspomnieć o raporcie⁷ przygotowanym przez Naczelną Radę Adwokacką (NRA) o skali inwigilacji i retencji danych, którym NRA chce zmusić policję i służby specjalne do odpowiedzi na szereg pytań stawianych od lat przez instytucje zaufania społecznego. NRA zwraca uwagę, jak bardzo służby nadużywają prawa i nie liczą się z ochroną prywatności nie tylko obywateli, ale i całych grup społecznych takich jak dziennikarze, lekarze czy adwokaci. Zgodnie z opracowanym raportem Polacy to najczęściej „prześwietlani” przez służby specjalne obywatele Unii Europejskiej. Służby te dysponują niemal nieograniczonym dostępem do informacji na temat obywateli. Sytuacja ta jest bez precedensu.

Według Pracodawców RP kluczowe problemy dotyczące retencji danych i sięgania po billingi to:

- Dyrektywa 2006/24/WE określająca minimalne standardy dotyczące retencji danych, pozwala państwom na wprowadzenie bardziej restrykcyjnych regulacji. Polska skorzystała z tego przywileju. Mamy najdłuższy okres przetrzymywania danych w porównaniu do reszty Europy. W Polsce wynosi on 24 miesiące, w większości krajów to 6 miesięcy.
- Katalog spraw, w których można sięgać po dane, jest otwarty. Nie jest to praktykowane w innych krajach.
- Polska zajmuje pierwsze miejsce w Europie pod względem składanych wniosków do firm telekomunikacyjnych o dane swoich klientów. W roku 2010 zanotowano 1,3 mln zapytań o billingi klientów.
- ABW, Służby Kontrwywiadu Wojskowego, CBA nie obejmuje żadną zewnętrzną kontrolą.
- Gromadzenie określonych danych telekomunikacyjnych dotyczy wszystkich abonentów bez względu na fakt, czy dana osoba popełnia jakiegokolwiek przestępstwo, czy zagraża bezpieczeństwu państwa.

Zdaniem Pracodawców RP obecny stan prawny jest niezgodny z Konstytucją RP oraz z Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności.

⁷ Raport dostępny jest pod adresem <http://adwokatura.pl/wp-content/uploads/2011/05/Raport-pdf.pdf>

VII. WNIOSKI

- 1) Sprawozdanie Komisji stanowi bardzo cenny materiał kompleksowo oceniający wdrożenie dyrektywy 2006/24/WE w państwach członkowskich. Przedstawia ono szczegółowe informacje przekazane przez państwa członkowskie, identyfikuje różnice w sposobie implementacji dyrektywy w państwach członkowskich oraz wskazuje na obszary, które powinny być szczególnie poddane analizie.
- 2) Biorąc pod uwagę liczbę uprawnionych podmiotów i innych urzędów zaangażowanych w problematykę związaną z dyrektywą 2006/24/WE, a także specyfikę obszaru regulowanego wymagającego gruntownej znajomości zagadnień związanych z wykorzystywaniem zatrzymanych danych, wymagać będzie ścisłej współpracy pomiędzy tymi podmiotami i urzędami, w procesie przeglądu i nowelizacji dyrektywy. Zadanie to powinno zostać zrealizowane przez resort wiodący oraz resorty współpracujące.
- 3) Przedstawienie przez Komisję propozycji zmian do dyrektywy 2006/24/WE poprzedzone zostanie spotkaniami konsultacyjnymi Komisji z reprezentantami organów ścigania państw członkowskich, sektora telekomunikacyjnego, grup konsumenckich, organów ochrony danych osobowych oraz organizacji społeczeństwa obywatelskiego. Spotkania te będą miały miejsce w czerwcu i lipcu 2011 r. Udział w nich ekspertów rządowych jest niezbędny dla uzyskania wpływu na kształt nowelizacji, którą zaproponuje Komisja.

W ramach Komisji pracuje grupa ekspertów pn. „*Platforma ds. zatrzymywania danych elektronicznych w celu dochodzenia, wykrywania i ścigania poważnych przestępstw*”, powołana decyzją Komisji 2008/324/WE z 25 marca 2008 r., której zadaniem jest doradzanie w sprawach związanych z zatrzymywaniem danych. W pracach grupy uczestniczą przedstawiciele organów ścigania państw członkowskich (wybranych państw członkowskich), posłów do Parlamentu Europejskiego, stowarzyszeń branży łączności elektronicznej, przedstawiciele organów ochrony danych, Europejskiego Inspektora Ochrony Danych.

W okresie 1 lipca 2011 r. – 31 grudnia 2012 r. w pracach ww. grupy będzie brał udział przedstawiciel Komendy Głównej Policji.

- 4) W celu przedstawiania na forum UE odpowiednio uzasadnionego stanowiska, poszczególne polskie instytucje wykorzystujące instrument retencji w praktyce, winny przygotować szczegółowych dane ilościowe i jakościowe (liczbowe dane statystyczne jak i opisy konkretnych spraw) uzasadniających istnienie oraz zasady korzystania z tego instrumentu.
- 5) Stanowisko prezentowane przez Rzeczpospolitą Polską odnośnie ewentualnych zmian w dyrektywie powinno uwzględniać ustalenie i wyniki prac powołanego przez Prezesa Rady Ministrów w ramach Kolegium do Spraw Służb Specjalnych zespołu roboczego, którego zadaniem jest wypracowanie stanowiska w sprawie zakresu zmian legislacyjnych dotyczących pozyskiwania przez uprawnione podmioty informacji objętych tajemnicą telekomunikacyjną oraz przygotowanie propozycji tych zmian.