Stanowisko Izby Gospodarki Elektronicznej dotyczące *Poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw* – druk sejmowy 154 –

Sygnatura pisma: S/LEG/PL/2016001

W dniu 23 grudnia 2015 r. wpłynął do Sejmu RP projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154), zwany dalej „**Projektem**". Autorzy powyższego wyszli z inicjatywą wprowadzenia nowych przepisów, w związku z koniecznością dostosowania systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11). We wspomnianym orzeczeniu, Trybunał zakwestionował konstytucyjność wybranych przepisów m.in. z ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r. poz. 355 i 529) dotyczących trybu i zakresu pozyskiwania przez Policję oraz inne organy, danych w toku czynności podejmowanych w ramach kontroli operacyjnej. Projekt zakłada wprowadzenie nowego katalogu danych, które będzie mogła uzyskiwać Policja i inne organy państwa (danych internetowych), jak również nakłada na przedsiębiorców obowiązek zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie kontroli operacyjnej, **który to obowiązek w przypadku usługodawców świadczących usługi drogą elektroniczną będzie nową powinnością**.

Stanowisko Izby Gospodarki Elektronicznej składa się z następujących części:

I. PODSTAWOWE ZASADY DOSTĘPU SŁUŻB DO DANYCH OBYWATELI

Prace legislacyjne nad zapewnieniem Policji i innym organom państwa skutecznych narzędzi dla efektywnego prowadzenia postępowań i wykrywania przestępstw stanowią duże wyzwanie dla ustawodawcy. Dochodzi bowiem do zderzenia istotnych wartości: przeciwdziałania przestępczości oraz poszanowania prywatności i tajemnicy komunikowania się, które są dobrami chronionymi konstytucyjnie. Zapewnienie właściwego balansu między tymi, czasem przeciwstawnymi wartościami, jest możliwe, choć wymaga zachowania kilku istotnych zasad. Można je sformułować następująco:

Dostęp organów państwa do danych obywateli powinien:

1. **być proporcjonalny do celu, do jakiego służy**, budzić **zaufanie obywateli do korzystania z komunikacji cyfrowej**
   Przepisy powinny **zapewniać równowagę pomiędzy bezpieczeństwem państwa** a **fundamentalnymi prawami człowieka**, takimi jak **prawo do prywatności** oraz w przypadku uzasadnionych indywidualnych interwencji **minimalizować dolegliwość i obciążenia dla pozostałych obywateli;**

2. **nie utrudniać rozwoju gospodarczego przedsiębiorcom**
   Przepisy powinny określać specyficzne rodzaje usług, które mogą być poddane bardziej rygorystycznym i zasadom dostępu do danych (kontrola operacyjna), a sposób i koszt obsługi wymagań powinien być adekwatny do prowadzonej działalności i rodzaju świadczonej usługi, **obowiązki nie powinny zniechęcać do świadczenia usług elektronicznych z terytorium RP.** Udostępnienie danych nie powinno odbywać się wyłącznie na koszt przedsiębiorców;

3. **w sposób precyzyjny i wąski określać dopuszczalne podstawy dostępu przez poszczególne organy państwa do danych obywateli (zakres i zasady)**
   Sformułowane podstawy do dostęp do sensytywnych danych powinny dotyczyć „wystarczająco poważnych przestępstw uzasadniających ingerencję w prawa podstawowe", czego wymagają konkretne wyroki Trybunału Sprawiedliwości;

4. **być poddawany realnej, zewnętrznej kontroli, umożliwiającej łatwe wykrywanie nadużyć i nadmiarowych wniosków o wydanie danych**
   Dostęp do danych powinien być adekwatny do celu, poddawany indywidualnej ocenie - tam gdzie to możliwe uprzedniej, a w szczególnych przypadkach nie cierpiących zwłoki, objęte specjalnymi dodatkowymi następczymi kontrolami;

5. **spełniać wymogi przejrzystości**
   Zbiorcze zestawienia zawierające wolumen i charakter (telekomunikacyjny, pocztowy, internetowy), w tym podstawę prawną zapytań, powinny być po upływie określonego czasu

publikowane zarówno przez służby wnioskujące o dane jak i sąd dokonujący kontroli zgodności prowadzonych działań z przepisami prawa.

Analiza Projektu prowadzi do wniosku, że nie realizuje on w pełni powyższych zasad, jak również pomija część wytycznych zawartych w wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11), a zwłaszcza w zakresie zapewnienia właściwego nadzoru sądowego nad uzyskiwaniem przez Policję dostępu do danych wskazanych w projektowanym brzmieniu art. 20c ustawy o Policji.

II. ZASADNICZE UWAGI DO PROJEKTU W OBCENYM KSZTAŁCIE

Projekt w obecnym kształcie wywołuje istotne wątpliwości co do jego zgodności z Konstytucją Rzeczypospolitej Polskiej oraz doprowadzi do wprowadzenia dodatkowego obciążenia finansowego dla małych i średnich przedsiębiorstw działających na polskim rynku, co grozi zachwianiem dynamiki rozwoju całej branży i co za tym idzie obniżeniem wpływów z podatków (VAT, PIT i CIT) od tego sektora.

1. Ochrona prywatności i tajemnicy komunikowania się

Dokonując wstępnej oceny Projektu należy zwrócić uwagę na dwa dobra chronione konstytucyjnie: prawo do prywatności oraz tajemnicę komunikowania się.

Zgodnie z przepisem art. 47 Konstytucji RP:
„Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym."

Zgodnie z przepisem art. 49 Konstytucji RP:
„Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony."

Wskazane przepisy Konstytucji RP gwarantują ochronę wartości istotnych w demokratycznym państwie prawa. Nie są to wprawdzie dobra absolutne tj. takie, których nie można w pewnych przypadkach ograniczyć, jednak musi to następować w uzasadnionych przypadkach i z uwzględnieniem tzw. zasady proporcjonalności, która została wyrażona w art. 31 ust. 3 Konstytucji RP. W swoim orzecznictwie Trybunał Konstytucyjny (np. wyrok z dnia 11 kwietnia 2006 r., sygn. akt 57/04, wyrok z dnia 11 kwietnia 2000 r., sygn. akt K. 15/98) podkreślił, że ograniczenie praw lub wolności konstytucyjnych spełnia zasadę proporcjonalności, gdy:

- ✓ wpisuje się w **zasadę przydatności**, czyli proponowane rozwiązanie ustawowe jest w stanie doprowadzić do zamierzonych skutków,
- ✓ realizuje **zasadę konieczności**, a zatem ograniczenie jest niezbędne dla ochrony ważnego interesu publicznego,
- ✓ efekty ograniczenia pozostają w **proporcji** do ciężarów nakładanych na obywatela.

Tymczasem, Projekt, a zwłaszcza projektowane brzmienie art. 20c ustawy o Policji, nie określa jednoznacznie przypadków, w których wolności powyższe mogą być ograniczane. Proponowana regulacja posługuje się pojęciami niedookreślonymi wskazując na bardzo ogólne sytuacje, w których Policja i inne organy państwa mogą ingerować w prawo do ochrony tajemnicy komunikowania się i

prawo do prywatności. Widać to wyraźnie na przykładzie proponowanego brzmienia art. 20c ustawy o Policji, który ma usankcjonować szeroki dostęp Policji do: danych telekomunikacyjnych, danych pocztowych i danych internetowych. Projekt nie określa katalogu przestępstw, przy których Policja i inne organy państwa będą mogły korzystać z przyznawanych jej przez powyższy artykuł uprawnień. Wystarczające jest bowiem zaistnienie szerokich przesłanek, jak przykładowo „w celu rozpoznawania", czy „w celu zapobiegania". Oznacza to zatem, że właściwie zawsze Policja i inne organy państwa będą dysponowały uprawnieniem dostępu m.in. do danych internetowych bez uprzedniej kontroli sądu. Również brak uprzedniej kontroli sądu należy ocenić jako wątpliwy z punktu widzenia powyższej zasady proporcjonalności. Należy bowiem zaznaczyć, że wymóg uzyskania zgody sądu na dostęp do m.in. danych internetowych jest rozwiązaniem mniej ingerującym w prawo do prywatności i tajemnicę komunikowania się niż uprawnienie Policji do samodzielnego podejmowania takich decyzji. Rozwiązanie z wykorzystaniem uprzedniej kontroli sądu gwarantuje też, że uprawnienia zawarte w Projekcie nie będą nadużywane. Obecne rozwiązanie przewidziane w proponowanym brzmieniu art. 20ca ustawy o Policji przewiduje jedynie następczą kontrolę uzyskiwania dostępu do danych określonych w proponowanym brzmieniu art. 20c ustawy o Policji. Kontrola ta ma być przeprowadzana nie tylko następczo, ale i w półrocznych odstępach czasu. Dodatkowo w ogóle spod kontroli mają zostać wyłączone dane określone w art. 20cb. Należy podkreślić, że tak skonstruowana kontrola sądowa nie wydaje się wystarczającą dla właściwego wykonania wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11).

Podsumowując:
obecne rozwiązania w Projekcie nie uwzględnia w wystarczającym stopniu powyższych wymogów konstytucyjnych i orzecznictwa Trybunału Konstytucyjnego.

2. Dane internetowe

W ścisłym związku z zagadnieniem opisanym w punkcie pierwszym, pozostaje zawarta w proponowanym w Projekcie brzmieniu art. 20c definicja pojęcia „*danych internetowych*". Odwołuje się ona do treści art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422). Powyższa regulacja jest bardzo szeroka i trudna do jednoznacznego zidentyfikowania.

Jako przykład powyższego wskazać można np. treść przepisu art. 18 ust. 4 ustawy o świadczeniu usług drogą elektroniczną, który stanowi, że usługodawca może przetwarzać, za zgodą usługobiorcy **inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną**. Tak określony katalog danych nie pozwala na jednoznaczne stwierdzenie, jakie dane mieszczą się w dyspozycji wspomnianego przepisu. W zasadzie, dyspozycję tego przepisu wypełniają wszystkie dane, jakie gromadzi każdy usługodawca przy wykonywaniu umowy z usługobiorcą, czyli internautą. Oznacza

to zatem, że Policja uzyskałaby dostęp do właściwie wszystkich danych związanych z aktywnością internautów w sieci telekomunikacyjnej od historii zakupów, przez historię przeglądanych stron i komunikację prowadzoną między znajomymi przez wewnętrzne komunikatory portali społecznościowych, aż po wszystkie informacje zawarte w aplikacjach mobilnych. Tak szeroko określony zakres danych, uwzględniający informacje o treści korespondencji czy przechowywanych prywatnych informacjach przez użytkowników, powinien być dostępny wyłącznie na podstawie z uprzedniej zgody sądu.

Podsumowując:
definicja pojęcia *„danych internetowych"* wymaga przeformułowania, zmierzającego do doprecyzowania, jakie dane mają być udostępniane przez usługodawców. W przeciwnym razie konstytucyjnie gwarantowana ochrona prywatności zostanie poważnie ograniczona i to w sposób, który (jak wskazano w punkcie 1) pozostaje wątpliwy z punktu widzenia wymogów zasady proporcjonalności.

3. Koszty dla MŚP i wpływ na branżę gospodarki cyfrowej

Zgodnie z Projektem, warunki techniczne i organizacyjne umożliwiające prowadzenie kontroli operacyjnej przez Policję i inne organy państwa mają być zapewniane przez usługodawców świadczących usługi elektroniczne, na ich własny koszt. Projekt jednocześnie nie precyzuje, jakie warunki techniczne mają być spełnione oraz jakich standardów bezpieczeństwa powinni trzymać się usługodawcy. Nie został również w żaden sposób ograniczony zakres podmiotowy przedsiębiorców świadczących usługi drogą elektroniczną objętych tym obowiązkiem, a więc dotyczyć on będzie wszystkich usługodawców, bez względu na to czy będą świadczyli usługi w niewielkim zakresie np. indywidualny bloger, czy też będą prowadzić serwis o zasięgu kilku milionów użytkowników. Warto podkreślić, że nakładanie na przedsiębiorców obowiązków związanych z ponoszeniem przez nich kosztów powinno następować w sposób na tyle skonkretyzowany, by było jasne do czego będą zobowiązani i jakie koszty mogą się z tym wiązać.

Co więcej, zaproponowane rozwiązanie nie pozostanie bez wpływu na kondycję finansową małych i średnich przedsiębiorstw działających w branży e-Commerce, a warto podkreślić, że to na nich opiera się polski handel elektroniczny. Przygotowanie odpowiedniej infrastruktury może okazać się dla nich zbyt dużym wyzwaniem, któremu nie będą mogli podołać.

Ponadto, w ostatecznym rozrachunku koszty wdrożenia odpowiednich warunków technicznych, zostaną przeniesione na konsumentów, co może zmniejszyć dynamikę rozwoju branży e-Commerce, gdyż dla polskich konsumentów niezwykle istotnym kryterium decyzji zakupowych jest cena. W dobie rozwoju handlu transgranicznego, dodatkowe koszty po stronie polskich e-przedsiębiorców i ich wpływ

na podwyższenie cen, mogą doprowadzić do migracji konsumentów w kierunku atrakcyjniejszej cenowo oferty sklepów i portali zagranicznych. To z kolei może przełożyć się na spowolnienie dynamiki rozwoju e-handlu w Polsce, a zatem obniżyć wpływy z podatków od tego sektora. Trzeba pamiętać, że jeśli nie uda się przedsiębiorcom zrekompensować kosztów, ich rentowność oraz pozycja konkurencyjna może zostać utracona, a w ich pozycję rynkową mogą zająć zagraniczni przedsiębiorcy, których nie obciążają podobne obowiązki, a którzy podatki odprowadzają poza Polską.

Podsumowując:
planowana regulacja może w sposób istotny negatywnie wpłynąć na kondycję finansową małych i średnich przedsiębiorstw działających na rynku polskim.

III. PROPOZYCJE ZMIAN

W naszym przekonaniu, by Projekt spełniał przedstawione przez nas podstawowe zasady dostępu do danych obywateli powinny zostać wprowadzone do niego wskazane poniżej zmiany. Jednocześnie podkreślamy, że celowe jest przemyślenie dodania proponowanych przepisów do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r. poz. 1422). Jest to bowiem podstawowa ustawa dla handlu elektronicznego i dobrą praktyką powinno być umieszczanie w niej wszystkich przepisów adresowanych do branży. Zwiększa to przejrzystość regulacji i pozwala przedsiębiorcom łatwiej zorientować się w ciążących na nich obowiązkach.

1) **Zakres podstaw do żądania danych obywateli przez policjantów i funkcjonariuszy służb** - podstawy prawne powinny być **precyzyjne i wąsko określać upoważnienia dostępu do danych przez organy państwa, adekwatne do rodzaju służby oraz rodzaju sprawy i kategorii danych**.

2) **Zmiana zaproponowanej zasady zbiorczej kontroli następczej** - **standardem powinna być indywidualna kontrola zasadności wniosku o udostępnienie danych**, a odstępstwa od tej reguły wąsko określonymi wyjątkami, w których stosowana może być kontrola następcza.

3) Ograniczenie **nieuzasadnionego znacznie szerszego wnioskowania o wydanie danych internetowych niż tryb wskazany w UŚUDE**, znacząco wykraczającego poza ramy prowadzonych postępowań.

4) **Zawężenie listy podmiotów świadczących usługi drogą elektroniczną**, na które nakładany jest obowiązek zapewnienia na własny koszt warunków technicznych i organizacyjnych **umożliwiających prowadzenie kontroli operacyjnej - proponowane zapisy dotyczą praktycznie wszystkich usługodawców internetowych (od blogerów po duże podmioty)**.

5) **Uprawnienia wywiadu skarbowego nie powinny być identyczne jak upoważnienia organów ścigania** takich jak Policja, ABW, CBA itp. - urzędy powinny współpracować nad konkretnymi postępowaniami z organami ścigania w celu uzyskania danych służących identyfikacji przestępstw a nie korzystać z uprawnienia praktycznie nieograniczonego dostępu.

6) **Wymuszenie nieodpłatnego trybu udostępniania danych**, co najmniej od operatorów usług świadczonych drogą elektroniczną.

UWAGA:
Zapisy projektów ustaw dotyczących usługodawców świadczących usługi drogą elektroniczną, nowe obowiązki wykraczające poza UŚUDE będącą transpozycją

Dyrektywy E-Commerce, w szczególności te dotyczące żądania wydania danych oraz kontroli operacyjnej będą dotyczyły wyłącznie ***podmiotów zlokalizowanych na terytorium RP****.*

Szerokie nałożenie obowiązków na ***wszystkich usługodawców internetowych****, oznacza* ***znaczące zmniejszenie konkurencyjności polskiego prawa jako środowiska przyjaznego przedsiębiorcom*** *i może grozić* ***zatrzymaniem inwestycji w projekty internetowe w Polsce lub wręcz migracją istniejących przedsiębiorców do krajów o bardziej przyjaznych użytkownikom przepisach****, stosujących bardziej przejrzyste i uzasadnione podstawy ingerencji w prywatność obywateli.*

Obowiązki zapewnienia możliwości kontroli operacyjnej zostały nałożone dotychczas na operatorów telekomunikacyjnych, zazwyczaj bardzo dużych przedsiębiorców, wraz z dodatkowymi zapisami, umożliwiającymi mniejszym podmiotom współpracę nad wykonaniem obowiązków poprzez powierzenie w drodze umowy innemu przedsiębiorcy telekomunikacyjnemu ich realizację (Art 180b 2 PT), a także możliwość współfinansowania przez państwo niezbędnych interfejsów danych (Art 179 4a PT).

Nie dość, że podobnych zapisów nie zaproponowano, to na dodatek wprowadzono zapis o nieodpłatnym udostępnianiu danych obciążając w całości firmy internetowe - głównie MŚP poważnymi kosztami.

IV. UZASADNIENIE ZMIAN

1. Uzasadniony dostęp do danych

Według aktualnego Projektu organy państwa będą mogły żądać dostępu do danych zawsze, gdy ich działanie zaledwie dotyczy "przestępstwa" – *"w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych ratowniczych"* - **czyli de facto nie tylko czynu zagrożonego karą, niezależnie od tego czy w danej sprawie toczy się postępowanie czy tylko istnieje ogólne podejrzenie potencjalnego wystąpienia naruszenia przepisów bądź wystąpienia niedookreślonej sytuacji zagrożenia dla człowieka**.

Tak sformułowane zapisy nie spełniają kryterium „wystarczająco poważnych przestępstw uzasadniających ingerencję w prawa podstawowe" czego wymagają konkretne wyroki Trybunału Sprawiedliwości.

Szerokie upoważnienia są nadane nie tylko organom ścigania, ale także organom wywiadu skarbowego, podczas gdy zakres nie powinien być identyczny we wszystkich przypadkach. W praktyce bardzo szerokiego zakresu podstaw i zbiorczej kontroli następczej - oznacza to w kontekście szerokiego katalogu podstaw prawnych w praktyce możliwość nieograniczonego śledzenia korzystania z Internetu w zakresie aktywności handlowej (zakupów przez Internet).

2. Kontrola wniosków o udostępnienie danych

Według aktualnych przepisów, kontrola operacyjna może być realizowana na podstawie uprzednio wyrażonej zgody w indywidualnej sprawie, potwierdzonej zgodą sądu, a w incydentalnych przypadkach możliwa była kontrola następcza. Nowe przepisy stawiają za standard sprawowanie nadzoru poprzez kontrolę następczą.

Zgodnie z wytycznymi zawartymi w orzeczeniach Trybunału Sprawiedliwości UE oraz Trybunału Konstytucyjnego, przedłożony projekt ustawy powinien zapewnić wprowadzenie **rzeczywistej, skutecznej kontroli nad działaniami służb** uprawnionych podmiotów państwowych w zakresie pozyskiwania danych telekomunikacyjnych.

Obecnie projekt przewiduje jedynie **zbiorczą następczą kontrolę** ilości i rodzajów danych, dokonywaną przez Sąd Okręgowy raz na 6 miesięcy. Oznacza to, że zdecydowana większość przypadków dostępu do danych obywateli nie będzie poddawana indywidualnej ocenie.

Rozwiązanie to jest wysoce niewystarczające, biorąc pod uwagę rosnącą ilość danych o życiu osobistym i zawodowym, która przekazywana jest obecnie za pomocą środków komunikacji elektronicznej i stanowi realne zagrożenie utraty zaufanie obywateli do korzystania z komunikacji cyfrowej w Polsce oraz lokalizacji usług świadczonych drogą elektroniczną na terytorium RP.

3. Ograniczenie dla danych internetowych

Projekt ustawy daje nieuzasadnioną możliwość znacznie szerszego wnioskowania o wydanie danych internetowych niż upoważnienie wskazane w UŚUDE, wykraczając poza ramy prowadzonych postępowań, rozszerza katalog spraw na zakres czynności operacyjno-rozpoznawczych prowadzonych przez służby.

a. Aktualny stan prawny a proponowane zapisy projektu Ustawy

Aktualnie, każdy rodzaj działalności (telekomunikacyjnej, pocztowej, usług świadczonych drogą elektroniczną) posiada **określony w branżowych ustawach sprecyzowany katalog uprawnień organów państwa zapytań o dane oraz stosownych obowiązków nakładanych na poszczególne rodzaje przedsiębiorców**.

Przykładowo, zgodnie z UŚUDE, organy państwa mają prawo żądać udostępnienia danych wyłącznie na potrzeby prowadzonych przez nie postępowań, co w sposób szeroki a zarazem stosunkowo precyzyjny definiuje przypadki w których możliwe jest żądanie udostępnienia określonych danych.

Projekt ustawy zakłada zrównanie podstaw do wnioskowania o udostępnienie danych w formie katalogu otwartego, w żaden sposób nieskorelowanego z toczonymi postępowaniami i stanowi pole do potencjalnych niekorzystnych interpretacji i nadużyć skutkujących naruszeniem prywatności obywateli.

ZAKRES ZAPYTAŃ O DANE WG UŚUDE	ZAKRES ZAPYTAŃ O DANE WG PROJEKTU USTAWY
Art. 18, ust. 6. Usługodawca udziela informacji o danych, o których mowa w ust. 1–5, organom państwa na potrzeby prowadzonych przez nie postepowań. *1. oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa*	*6a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 6, polegające na:* *1) uzyskiwaniu i utrwalaniu obrazu w pomieszczeniach, o których mowa w art. 15 ust. 1 pkt 4a;* *2) uzyskiwaniu danych w trybie art. 20c* *6b. Realizacja czynności, o których mowa w ust. 6a* ***nie wymaga zgody sądu.***

w ust. 1; 2. *oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca;* 3. *informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;* 4. *informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.*	*„Art. 20c. 1.* ***W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw*** *albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane:* *1) określone w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”,* *2) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”* ***3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.)****, zwane dalej „danymi internetowymi”* *– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.* *2. Przedsiębiorca telekomunikacyjny, operator pocztowy* ***lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie*** *dane, o których mowa w ust. 1:* *1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;* *2) na ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;* *3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1;* *3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1,* ***odbywa się bez udziału pracowników przedsiębiorcy*** *telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną,* ***lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu*** *zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.*

b. Uzasadnienie dla modyfikacji projektu Ustawy

Proponowany Art. 20c nie określa w sposób precyzyjny podstawy na jakiej może odbywać się wnioskowanie o wydanie danych, rodzi więc uzasadnione wątpliwości o potencjalne nadużycia nieudokumentowanego lub niezasadnego wnioskowania o wydanie danych przez zobowiązane podmioty.

Rekomendujemy uściślenie, iż wydanie danych może odbywać się wyłącznie na potrzeby prowadzonych postępowań, a więc tak jak dotychczas usługodawca będzie mógł zapoznać się z podstawą prawną i numerem prowadzonej sprawy, co pozwala na udokumentowanie spełniania obowiązków przetwarzania danych osobowych wobec nadzoru (GIODO) i stanowi dodatkowo zabezpieczenie, że wraz z konkretną sprawą związana będzie procedura usunięcia udostępnionych uprzednio danych.

Mocno kontrowersyjne jest także wprowadzenie szerokiej klauzuli „ratowania życia lub zdrowia ludzkiego" jako podstawy żądania wydania danych, która jest niezgodna z orzeczeniem Trybunału Konstytucyjnego i zasadami przejrzystości i pewności. Popierając co do zasady możliwe użycie takiej podstawy w szczególnych przypadkach, warto jest opracować na tę okoliczność specjalną procedurę i zasady dedykowanego nadzoru nad jej wykonaniem (np. sądu i GIODO), ze względu na to że tak szeroko określona kategoria podstaw może prowadzić do największych naruszeń prywatności.

c. Rekomendacje zmian w projekcie Ustawy

Rekomendujemy pozostawienie wprowadzenie warunku uzyskania danych na zasadach identycznych jak dotychczas w brzmieniu UŚUDE lub rozważenie wprowadzenie następujących ograniczeń:

- zawężenie do prowadzonego formalnego postępowania,
- zawężenie katalogu przestępstw i skonkretyzowanie, tak by obejmował jedynie te przestępstwa, w stosunku do których możliwe jest prowadzenie kontroli rozmów telefonicznych i innych rozmów czy przekazów informacji zgodnie z art. 237 § 3 Kodeksu postępowania karnego (dalej jako „k.p.k.") oraz 241 k.p.k..

Aktualnie brzmienie w Projekcie	Proponowane brzmienie
"Art. 20c. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw albo w celu ratowania życia lub	*"Art. 20c. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów*

zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane"	*przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane"* *1) określone w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi",* *2) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi"* ~~*3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi"*~~ *– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.* *20d.* ***Policja na potrzeby prowadzonych postępowań może uzyskiwać dane określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.)****, zwane dalej „danymi internetowymi"* *– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.*
Identyczna treść proponowana w odniesieniu do poszczególnych organów państwa	*Analogicznie, jak w propozycji dla Policji.*

4. Ograniczenie dla kontroli operacyjnej

Konieczne jest zawężenie listy podmiotów świadczących usługi drogą elektroniczną, na które nakładany jest obowiązek zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie kontroli operacyjnej.

a. Aktualny stan prawny a proponowane zapisy projektu Ustawy

Aktualnie usługodawcy świadczący usługi drogą elektroniczną nie są zobowiązani do zapewnienia możliwości realizacji kontroli operacyjnej. Aktualne brzmienie Projektu zobowiązuje **wszystkie podmioty, które świadczą usługi drogą elektroniczną do zapewnienia możliwości realizacji kontroli operacyjnej**, podczas gdy definicja **usługodawcy świadczącego usługi drogą elektroniczną jest bardzo szeroka** i w praktyce oznacza niemal każdy podmiot, który prowadzi serwis internetowy polegający na zautomatyzowanym dostępie do treści.

Zważywszy na planowany termin wejścia w życie projektowanej ustawy, projekt nie przewiduje żadnego czasu dla przedsiębiorców na dostosowanie się do przepisów, podczas gdy jego realizacja wymaga nie tylko olbrzymich nakładów finansowych, ale także czasu na analizę optymalnego wdrożenia, co w praktyce powoduje, iż wszystkie podmioty z dniem wejścia w życie ustawy nie będą realizowały tak ustalonego obowiązku.

Projekt nie przewiduje możliwości powierzenia spełniania tego obowiązku dedykowanemu podmiotowi, co mogłoby znacząco obniżyć koszt potencjalnego dostosowania się do obowiązku poprzez dzielenie kosztów infrastruktury i procedur z innymi przedsiębiorcami.

b. Uzasadnienie dla modyfikacji projektu Ustawy

Zaproponowane zobowiązanie **nie dotyczy wyłącznie firm, które świadczą zaawansowane usługi umożliwiające komunikację przez Internet** jak np. komunikatory internetowe (tekstowe, audio, wideo), systemy masowego udostępniania poczty elektronicznej, serwisy społecznościowe umożliwiające multimedialną wymianę informacji pomiędzy użytkownikami, dla których przygotowanie dedykowanej infrastruktury do kontroli operacyjnej można wyobrazić sobie może być przydatne, **ale także wszystkie małe i średnie przedsiębiorstwa będące usługodawcami usług elektronicznych**, które świadczą serwisy tak jak portale tematyczne dostarczające informacji politycznych,	***UŚUDE:*** ***świadczenie usługi drogą elektroniczną*** *– wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;*

kulturalnych, artystycznych, sportowych, naukowych, rozrywkowych, wszystkie sklepy internetowe czy usługi w postaci aplikacji mobilnych prezentujące użytkownikom rozkłady jazdy komunikacji miejskiej lub blogerów udostępniających usługę korzystania z newslettera z codziennymi informacjami.	***usługodawca*** *– oznacza osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługi drogą elektroniczną*

W związku z powyższym proponujemy, aby obowiązkiem tym nie byli automatycznie objęci wszyscy przedsiębiorcy, ale wyłącznie Ci, wobec których zasadne jest objęcie gromadzonych danych użytkowników potencjalną kontrolą operacyjną popartą uprzednio dużą liczbą zapytań, którzy zostaną uprzednio zawiadomieni. Obowiązek ten winien dotyczyć wyłącznie przedsiębiorców świadczących usługi drogą elektroniczną o charakterze komunikatora internetowego, tj. usług natychmiastowej komunikacji elektronicznej pomiędzy dowolnymi użytkownikami umożliwiających swobodne porozumiewanie się na odległość za pomocą treści tekstowych, audio lub wideo pomiędzy dwoma lub większą liczbą urządzeń końcowych poprzez sieć komputerową oraz usług masowego udostępniania kont poczty elektronicznej.

Przedsiębiorcy, którzy zostali objęci nowymi obowiązkami powinni mieć czas na przygotowanie stosownych rozwiązań do realizacji nałożonych obowiązków - konieczne jest **vacatio legis dla obowiązywania wybranych zapisów proponowanej ustawy**.

c. Rekomendacje zmian w projekcie Ustawy

Aktualnie brzmienie w Projekcie	Proponowane brzmienie
"12. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej."	**Wariant 1:** *12a. Przedsiębiorca telekomunikacyjny, operator pocztowy ~~oraz usługodawca świadczący usługi drogą elektroniczną~~ jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej."* *12b. Przedsiębiorca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej, przy czym zasady świadczenia dostępu oraz rodzaje działalności lub*

	rodzaje przedsiębiorców świadczących usługi drogą elektroniczną podlegających obowiązkowi udostępniania danych w ramach kontroli operacyjnej określa w drodze rozporządzenia właściwy Minister ds. cyfryzacji. **Wariant 2:** **Z wykorzystaniem zapisów analogicznych jak w ustawie Prawo Telekomunikacyjne** *12a. Przedsiębiorca telekomunikacyjny, operator pocztowy ~~oraz usługodawca świadczący usługi drogą elektroniczną~~ jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej."* *12b. Przedsiębiorca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej, przy czym Minister ds. Cyfryzacji określi, w drodze Rozporządzenia:* *1) rodzaje działalności lub rodzaje przedsiębiorców świadczących usługi drogą elektroniczną podlegających obowiązkowi zapewnienia warunków dostępu i utrwalania, kierując się zakresem i rodzajem świadczonych usług drogą elektroniczną lub wielkością usługi świadczonej drogą elektroniczną przez przedsiębiorców;* *2) wymagania i sposób zapewnienia warunków dostępu i utrwalania, z wyłączeniem spraw uregulowanych w art. 242 Kodeksu postepowania karnego, kierując się zasadą osiągania celu przy jak najniższych nakładach. Warunki dostępu i utrwalania mogą być zapewniane za pomocą interfejsów zlokalizowanych w miejscach obejmowanych przez sieć przedsiębiorcy świadczącego usługi drogą elektroniczną na zasadach określonych w umowach zawartych przez uprawnione podmioty z przedsiębiorcą świadczącym usługę drogą elektroniczną. Umowa może*

	określać współudział stron w kosztach zastosowania interfejsów. W przypadku braku uzgodnień w zakresie lokalizacji interfejsu uprawnione podmioty wskazują miejsce lokalizacji pozostające w obrębie sieci telekomunikacyjnej przedsiębiorcy świadczącego usługi drogą elektroniczną, umożliwiające: techniczną realizację interfejsu, niezbędną ochronę tego miejsca wynikającą z przepisów odrębnych oraz minimalizację nakładów ponoszonych przez przedsiębiorcę świadczącego usługi drogą elektroniczną i podmioty uprawnione. *3) wymagania techniczne i eksploatacyjne dla interfejsów, o których mowa w ust.2, umożliwiających wykonywanie zadań i obowiązków, tworzone kierując się zasadą minimalizacji nakładów przedsiębiorcy telekomunikacyjnego i podmiotów uprawnionych.* **KOMENTARZ:** Warte rozważenia jest oparcie przepisów adresowanych w tym zakresie do usługodawców świadczących usługi drogą elektroniczną, na rozwiązaniach obowiązujących na podstawie ustawy z dnia z dnia 23 listopada 2012 r. Prawo pocztowe (Dz.U. z 2012 r. poz. 1529) i ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243) i wydanych na ich podstawie przepisów wykonawczych. Doprecyzowanie obowiązków usługodawców internetowych pozwoli na zwiększenie pewności prawa. Da to także możliwość dopasowania zakresu tych obowiązków do wielkości danego usługodawcy i profilu jego działalności. *12c.* *1) Przedsiębiorca świadczący usługi drogą elektroniczną zapewnia warunki dostępu i utrwalania od dnia wejścia w życie rozporządzenia, o którym mowa w ust. 12b,*

	2) *Przedsiębiorca świadczący usługi drogą elektroniczną może powierzyć realizację obowiązku, o którym mowa w art. 12b, w drodze umowy, innemu przedsiębiorcy. Powierzenie to nie zwalnia powierzającego z odpowiedzialności za realizację tego obowiązku.*
„13. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Straż Graniczną kontroli operacyjnej."	*Zapis jak w/w dla Policji z podmianą nazwy organu państwa*
"10. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez wywiad skarbowy kontroli operacyjnej."	*"12a. Przedsiębiorca telekomunikacyjny, operator pocztowy ~~oraz usługodawca świadczący usługi drogą elektroniczną~~ jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej."* *12b. Przedsiębiorca świadczący usługi drogą elektroniczną określony w rozporządzeniu Ministra ds. cyfryzacji jest obowiązany do zapewnienia warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej. Zasady świadczenia dostępu do danych w ramach kontroli operacyjnej określa w drodze rozporządzenia właściwy Minister ds. cyfryzacji.*
13. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Żandarmerię Wojskową kontroli operacyjnej.	*Analogicznie, jak w propozycji dla Policji.*
„12. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez ABW kontroli operacyjnej."	*Analogicznie, jak w propozycji dla Policji.*

"11. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez SKW kontroli operacyjnej."	*Analogicznie, jak w propozycji dla Policji.*
„12. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez CBA kontroli operacyjnej."	*Analogicznie, jak w propozycji dla Policji.*

5. Ograniczenia dla wywiadu skarbowego

W ocenie e-Izby, dostęp do danych przez wywiad skarbowy powinien odbywać się wyłącznie w konkretnej, indywidualnej sprawie, w ramach prowadzonego postępowania. W przeciwnym wypadku na podstawie dotychczasowych doświadczeń można przewidywać iż zapytania kierowane ze strony organów kontroli skarbowej będą dotyczyły ogólnego dostępu do danych, będą kierowane przekrojowo i nie odnosiły się do konkretnej sprawy. W przypadku bardziej zaawansowanych spraw o charakterze wykrywania zorganizowanej przestępczości, organy mogą zawsze współpracować z organami ścigania w celu uzyskania większego dostępu do danych.

Dotychczasowe przepisy są wystarczające i zapewniają bezpieczeństwo.

Należy zwrócić uwagę, że - przynajmniej na rynku świadczeniodawców usług elektronicznych - istnieje silna konkurencja zagraniczna. Wnikliwe i nieograniczone działania wywiadu skarbowego nie spowodują zmniejszenia ilości naruszeń prawa podatkowego, ale spowodują ich mniejszą wykrywalność. Osoby, mające na celu ukrycie dochodów będą korzystać z zagranicznych odpowiedników i staną się zupełnie nie wykrywalni. Dotychczasowe zapisy w bardzo dyskretny sposób zapewniają organom skarbowym dostęp do stosownych danych.

ART.3 *Art. 36b* *"1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, wywiad skarbowy może uzyskiwać dane"*	*"W ramach prowadzonego indywidualnego postępowania w celu ~~rozpoznawania, zapobiegania, zwalczania, wykrywania albo~~ uzyskania i utrwalenia dowodów przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, wywiad skarbowy może uzyskiwać dane"*
ART.12 1a) *w art. 75d* *„1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celna może uzyskiwać dane"*	*„1. W ramach prowadzonego indywidualnego postępowania w celu ~~rozpoznawania, zapobiegania, zwalczania, wykrywania albo~~ uzyskania i utrwalenia dowodów przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celna może uzyskiwać dane"*
ART.12 2) *Art. 75db.* *1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego Służba Celna może uzyskiwać dane*	*Art. 75db. 1. W ramach prowadzonego indywidualnego postępowania w celu ~~rozpoznawania, zapobiegania, zwalczania, wykrywania albo~~ uzyskania i utrwalenia dowodów przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego Służba Celna może uzyskiwać dane*

6. ODPŁATNOŚĆ ZA UDOSTĘPNIANIE DANYCH

a. Aktualny stan prawny i proponowane zapisy projektu Ustawy

Aktualnie, zgodnie z ustawą Prawo Telekomunikacyjne, wydawanie danych przez operatorów telekomunikacyjnych w odpowiedzi na zapytania upoważnionych organów państwa realizowane jest nieodpłatnie. Przepisy przewidują jednak, że dostęp do danych odbywać się może za pomocą uzgodnionych w ramach umowy interfejsów, a zawarta umowa może określać współudział stron w kosztach zastosowania interfejsów (Art 179 4a PT). Dodatkowo, ustawa przewiduje możliwość współpracy operatorów w wykonywaniu obowiązków, co pozwala ograniczyć koszty realizacji obowiązku.

Usługodawcy usług świadczonych drogą elektroniczną natomiast nie są objęci zobowiązaniem do nieodpłatnego realizowania nałożonych obowiązków wynikających z art. 18 ust.6 UŚUDE i nie ma też żadnych uregulowań dotyczących obowiązków zapewnienia infrastruktury do potencjalnej kontroli operacyjnej, ani obowiązków retencyjnych.

Należy zwrócić uwagę na fakt, że w przeciwieństwie do operatorów telekomunikacyjnych, którzy mają od dawna wykształcone procedury i ustandaryzowane sposoby udostępniania oczekiwanych danych (np. bilingowych), usługi świadczone drogą elektroniczną ze względu na swoją indywidualną charakterystykę w przypadku każdej firmy są zupełnie odmienne. Co więcej, firmy świadczące usługi drogą elektroniczną w przeważającej większości stanowią małe i średnie przedsiębiorstwa, które na potrzeby zapytań muszą ponieść istotne dla nich koszty zarówno kadrowe jak i często informatyczne, związane z przetwarzaniem danych na potrzeby konkretnego, często niestandardowego zapytania.

Po stronie składających zapytania, zarówno sposób formułowania zapytań jak i oczekiwania odnośnie sposobu prezentacji danych bywają znacząco różne w ramach każdego organu upoważnionego, a żądania rzadko bazują na doświadczeniach w innych sprawach, co w przypadku braku jednorodności rodzajów danych i formatów często powoduje dodatkowe koszty po stronie przedsiębiorców odpytywanych o dane.

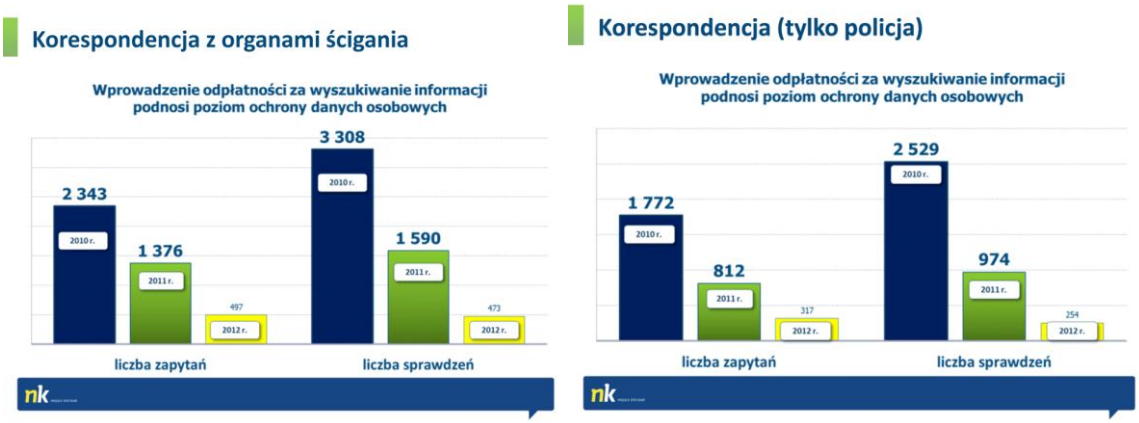
b. Uzasadnienie dla modyfikacji projektu Ustawy

Nałożone na usługodawców usług świadczonych drogą elektroniczną obowiązki udostępniania danych nie powinny mieć charakteru co do zasady nieodpłatnego. Za wykonanie obowiązków należeć się powinno stosowne wynagrodzenie lub rekompensata.

1. **Odpłatność za udostępniane dane w sposób znaczący przyczynia się do większej efektywności prowadzonych postępowań**

Odpłatność za udostępniane dane w sposób znaczący przyczynia się do większej efektywności prowadzonych postępowań dzięki racjonalności zapytań - lepszego formułowania zapytań, żądania danych niezbędnych zamiast nadmiarowych, a zatem a przy okazji istotnego ograniczenia ponoszonych kosztów przez przedsiębiorców.

Jak wskazują przeprowadzone analizy i publikowane doświadczenia, wprowadzenie odpłatności za wyszukiwanie informacji powoduje zmniejszenie liczby zapytań i podnosi poziom ochrony danych osobowych. Wnioski wskazują, że organy składają zapytania wyłącznie o te dane, które są potrzebne do danego postępowania i dokonują uprzedniej analizy zasadności żądania danych. Rozwiązanie takie stanowi skuteczny środek zapobiegający nieproporcjonalnie szerokim i kosztownym zapytaniom ze strony organów państwa, których doświadczenie w tym zakresie jest stosunkowo nieduże.



http://www.siis.org.pl/uploads/Przyszlosc_retencji_danych_w_Polsce_M_Pajecki.pdf

2. **Rekomendacja Komisji Europejskiej do refundacji ponoszonych kosztów**

Porównanie praktyk legislacyjnych w państwach europejskich pokazuje, że kraje o dłuższej tradycji demokracji i wyższej praworządności podjęły decyzję o refundowaniu kosztów udostępniania danych telekomunikacyjnych. Refundowanie kosztów udostępniania danych również jest popierane przez Komisję Europejską.

W raporcie Komisji Europejskiej i Rady w sprawie dyrektywy DRD: Evaluation report on the Data Retention Directive (Directive 2006/23/EC) przedstawione jest zestawienie w ramach

Evaluation report, obrazujące udział władz państwowych w kosztach udostępnia danych telekomunikacyjnych[1]:

PAŃSTWO	OPŁATY OPERACYJNE PONOSZONE PRZEZ PAŃSTWO	OPŁATY INWESTYCYJNE PONOSZONE PRZEZ PAŃSTWO
Finlandia	tak	tak
Wielka Brytania	tak	tak
Belgia	tak	Nie
Dania	tak	Nie
Estonia	tak	Nie
Francja	tak	Nie
Holandia	tak	Nie
Litwa	tak	Nie
Niemcy*	tak	-
Szwecja*	tak	-
Cypr	Nie	Nie
Bułgaria	Nie	Nie
Grecja	Nie	Nie
Hiszpania	Nie	Nie
Irlandia	Nie	Nie
Łotwa	Nie	Nie
Luksemburg	Nie	Nie
Malta	Nie	Nie
Polska	Nie	Nie
Portugalia	Nie	Nie
Słowacja	Nie	Nie
Słowenia	Nie	Nie
Węgry	Nie	Nie
Austria	-	-
Czechy	-	-
Rumunia	-	-
Włochy	-	-

[1] **REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Evaluation report on the Data Retention Directive (Directive 2006/24/EC) /* COM/2011/0225** (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0225:EN:HTML)

3. Koszty obsługi mogą stanowić istotne obciążenie dla przedsiębiorcy

W przypadku przedsiębiorców, do których kierowana jest większa liczba zapytań o dane, koszty obsługi stanowią też istotny koszt od strony zapotrzebowania na wyspecjalizowaną kadrę oraz politykę retencyjną danych. Inwestycje dokonywane na potrzeby współpracy z organami państwa pozwoliły w wielu przypadkach na utrzymywanie danych w sposób umożliwiający bardzo szybki dostęp i możliwość podjęcia błyskawicznej reakcji w sytuacji nie cierpiącej zwłoki. Jedynym sposobem na częściową rekompensatę ponoszonych kosztów jest skromna rekompensata.

c. Rekomendacje zmian w projekcie Ustawy

Aktualnie brzmienie w Projekcie	Proponowane brzmienie
Art. 10b ust. 2, art. 20c ust. 2, art. 18 ust.2, art. 28 ust. 2, art. 30, art. 32 ust. 2, art. 36b: "Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:"	*Art. 10b ust. 2, art. 20c ust. 2, art. 18 ust.2, art. 28 ust. 2, art. 30, art. 32 ust. 2, art. 36b: "Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia ~~nieodpłatnie~~ dane, o których mowa w ust. 1:"* *lub* *Art. 20c "Przedsiębiorca telekomunikacyjny, operator pocztowy ~~lub usługodawca świadczący usługi drogą elektroniczną~~ udostępnia nieodpłatnie dane, o których mowa w ust. 1:"*
Art. 8. W ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422) w art. 18 ust. 6 otrzymuje brzmienie: „6.Usługodawca nieodpłatnie udostępnia dane, o których mowa w ust. 1-5, organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postepowań.".	*Art. 8. W ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422) w art. 18 ust. 6 otrzymuje brzmienie: „6.Usługodawca ~~nieodpłatnie~~ udostępnia dane, o których mowa w ust. 1-5, organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postepowań.".* *Uwaga: aktualnie w ustawie jest zapis: "Usługodawca udziela informacji o danych, o których mowa w ust. 1–5, organom państwa na potrzeby prowadzonych przez nie postepowań."*

Art. 75d ust. 2 *„Przedsiębiorca telekomunikacyjny lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane telekomunikacyjne lub internetowe:”,*	*Art. 75d ust. 2* *„Przedsiębiorca telekomunikacyjny lub usługodawca świadczący usługi drogą elektroniczną udostępnia ~~nieodpłatnie~~ dane telekomunikacyjne lub internetowe:”,* *Art. 75d ust. 2* *„Przedsiębiorca telekomunikacyjny ~~lub usługodawca świadczący usługi drogą elektroniczną~~ udostępnia nieodpłatnie dane telekomunikacyjne lub internetowe:”,*