SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VI kadencja
Prezes Rady Ministrów
RM 10-162-08

Druk nr 1448

Warszawa, 30 października 2008 r.

Pan
Bronisław Komorowski
Marszałek Sejmu
Rzeczypospolitej Polskiej

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw wraz z projektami aktów wykonawczych.

Projekt ma na celu wykonanie prawa Unii Europejskiej.

W załączeniu przedstawiam także opinię dotyczącą zgodności proponowanych regulacji z prawem Unii Europejskiej.

Ponadto uprzejmie informuję, że do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Infrastruktury.

(-) Donald Tusk

Projekt

U S T A W A

z dnia

o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw[1)2)]

Art. 1. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]) wprowadza się następujące zmiany:

1) w art. 2 pkt 48 otrzymuje brzmienie:

„48) usługa telekomunikacyjna – usługę polegającą głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej;”;

2) art. 6 otrzymuje brzmienie:

„Art. 6. 1. Przedsiębiorca telekomunikacyjny lub podmiot, który uzyskał pozwolenie radiowe, rezerwację częstotliwości lub zasobów orbitalnych lub przydział numeracji, z wyłączeniem osób fizycznych i podmiotów, o których mowa w art. 4, jest obowiązany do przekazywania na żądanie Prezesa UKE informacji niezbędnych do wykonywania przez Prezesa jego uprawnień i obowiązków, określonych w art. 192 ust. 1.

2. Żądanie, o którym mowa w ust. 1, powinno być proporcjonalne do celu, jakiemu ma służyć, oraz zawierać:

1) wskazanie Prezesa UKE oraz przedsiębiorcy lub podmiotu, o którym mowa w ust. 1;
2) datę żądania;
3) wskazanie żądanych informacji oraz okresu, których dotyczą;
4) wskazanie celu, jakiemu informacje mają służyć;

[1)] Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia 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 (Dz. Urz. UE L 105 z 13.4.2006, str. 54).

[2)] Niniejszą ustawą zmienia się ustawy: ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 12 października 1990 r. o Straży Granicznej, ustawę z dnia 28 września 1991 r. o kontroli skarbowej, ustawę z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, ustawę z dnia 16 marca 2001 r. o Biurze Ochrony Rządu, ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 28 lutego 2003 r. – Prawo upadłościowe i naprawcze, ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

[3)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82 poz. 556 oraz z 2008 r. Nr 17, poz. 101.

5) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
6) uzasadnienie;
7) pouczenie o karze, o której mowa w art. 209 ust. 1.

3. Prezes UKE może zastosować do pozyskania informacji, o których mowa w ust. 1, opracowane przez siebie formularze, dążąc do ujednolicenia i zapewnienia spójności pozyskanych danych.”;

3) art. 8 otrzymuje brzmienie:

„Art. 8. 1. Prezes UKE zapewnia dostęp do informacji otrzymanych od przedsiębiorców telekomunikacyjnych organom regulacyjnym innych państw członkowskich Unii Europejskiej oraz państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronom umowy o Europejskim Obszarze Gospodarczym, zwanych dalej „państwami członkowskimi”, i Komisji Europejskiej, z wyjątkiem przypadków określonych w ustawie.

2. Prezes UKE informuje przedsiębiorcę telekomunikacyjnego o udostępnieniu informacji dostarczonej uprzednio przez tego przedsiębiorcę na żądanie Prezesa UKE.”;

4) w art. 10:

a) ust. 1 otrzymuje brzmienie:

„1. Działalność telekomunikacyjna będąca działalnością gospodarczą jest działalnością regulowaną i podlega wpisowi do rejestru przedsiębiorców telekomunikacyjnych, zwanego dalej „rejestrem”. Wpisowi do rejestru podlega również działalność telekomunikacyjna prowadzona przez przedsiębiorcę telekomunikacyjnego z państwa członkowskiego albo państwa, które zawarło ze Wspólnotą Europejską i jej państwami członkowskimi umowę regulującą swobodę świadczenia usług, który czasowo świadczy na terytorium Rzeczypospolitej Polskiej usługi na zasadach określonych odpowiednio w przepisach Traktatu ustanawiającego Wspólnotę Europejską, umowy o Europejskim Obszarze Gospodarczym albo w przepisach innej umowy regulującej swobodę świadczenia usług.”,

b) w ust. 4 pkt 4 otrzymuje brzmienie:

„4) numer w rejestrze przedsiębiorców albo ewidencji działalności gospodarczej lub innym właściwym rejestrze w państwie członkowskim lub innym państwie określonym w ust. 1;”;

5) w art. 15 pkt 1 otrzymuje brzmienie:

„1) określenia rynku właściwego, o którym mowa w art. 22 ust. 1, a także jego analizy i wyznaczenia przedsiębiorcy telekomunikacyjnego o znaczącej pozycji rynkowej lub przedsiębiorców telekomunikacyjnych zajmujących kolektywną pozycję znaczącą, lub uchylenia decyzji w tej sprawie,”;

6) w art. 19 ust. 2 i 3 otrzymują brzmienie:

„2. Jeżeli w zakresie ustalenia znaczącej pozycji rynkowej oraz w zakresie zamiaru zdefiniowania rynku właściwego innego niż rynki określone w zaleceniu Komisji Europejskiej w sprawie właściwych rynków produktów i usług w sektorze łączności elektronicznej podlegających regulacji *ex ante,* zwanego dalej „zaleceniem Komisji”, Komisja Europejska stwierdzi, że proponowane rozstrzygnięcie może utrudnić rozwój jednolitego rynku lub mogłoby naruszyć prawo wspólnotowe, Prezes UKE po upływie terminu, o którym mowa w art. 16 ust. 2, zawiesza postępowanie na okres 2 miesięcy. W przypadku otrzymania w tym okresie wezwania Komisji Europejskiej do wycofania projektu rozstrzygnięcia, Prezes UKE uwzględnienia stanowisko Komisji Europejskiej i umarza postępowanie.

3. Prezes UKE uwzględnia przy stosowaniu ustawy w największym możliwie stopniu wytyczne Komisji Europejskiej w sprawie analizy rynku i ustalania znaczącej pozycji rynkowej oraz zalecenie Komisji w ich aktualnym brzmieniu, a w przypadku odstąpienia od ich stosowania powiadamia Komisję Europejską, uzasadniając swe stanowisko.”;

7) w dziale II rozdział 1 otrzymuje brzmienie:

„Rozdział 1

Analiza rynku, postępowanie w sprawie określania rynków właściwych, nakładania, zmiany i uchylenia obowiązków regulacyjnych

Art. 21. Prezes UKE przeprowadza analizę rynku w zakresie wyrobów i usług telekomunikacyjnych.

Art. 22. 1. Po przeprowadzeniu analizy, o której mowa w art. 21, nie rzadziej niż co 2 lata, a także niezwłocznie po wydaniu albo zmianie zalecenia Komisji Prezes UKE przeprowadza postępowanie w celu:

1) określenia rynku właściwego, zgodnie z prawem konkurencji, w zakresie wyrobów i usług telekomunikacyjnych, zwanego dalej „rynkiem właściwym”,

2) ustalenia, czy na rynku właściwym występuje przedsiębiorca telekomunikacyjny o znaczącej pozycji rynkowej lub przedsiębiorcy telekomunikacyjni zajmujący kolektywną pozycję znaczącą,
3) wyznaczenia przedsiębiorcy telekomunikacyjnego o znaczącej pozycji rynkowej lub przedsiębiorców telekomunikacyjnych zajmujących kolektywną pozycję znaczącą, w przypadku stwierdzenia, że na rynku właściwym nie występuje skuteczna konkurencja oraz
4) nałożenia, utrzymania, zmiany lub uchylenia obowiązków regulacyjnych na przedsiębiorcę telekomunikacyjnego o znaczącej pozycji rynkowej lub przedsiębiorców telekomunikacyjnych zajmujących kolektywną pozycję znaczącą.

2. Przez obowiązek regulacyjny rozumie się obowiązek, o którym mowa w art. 34, 36 – 40, 42, 44 – 47 lub art. 72 ust. 3.

Art. 23. 1. W przypadku ustalenia, że na rynku właściwym nie występuje przedsiębiorca telekomunikacyjny o znaczącej pozycji rynkowej lub przedsiębiorcy telekomunikacyjni zajmujący kolektywną pozycję znaczącą Prezes UKE, po przeprowadzeniu postępowania, o którym mowa w art. 22 ust. 1, wydaje postanowienie, w którym:
1) określa rynek właściwy, mając na uwadze poziom rozwoju krajowego rynku produktów i usług telekomunikacyjnych, zgodnie z prawem konkurencji;
2) stwierdza, że na tym rynku właściwym występuje skuteczna konkurencja.

2. Do projektu postanowienia, o którym mowa w ust. 1, stosuje się przepisy o postępowaniu konsultacyjnym.

Art. 24. W przypadku ustalenia, że na rynku właściwym występuje przedsiębiorca telekomunikacyjny o znaczącej pozycji rynkowej lub przedsiębiorcy telekomunikacyjni zajmujący kolektywną pozycję znaczącą Prezes UKE, po przeprowadzeniu postępowania, o którym mowa w art. 22 ust. 1, wydaje decyzję, w której:
1) określa rynek właściwy, mając na uwadze poziom rozwoju krajowego rynku produktów i usług telekomunikacyjnych, zgodnie z prawem konkurencji;
2) wyznacza przedsiębiorcę telekomunikacyjnego o znaczącej pozycji rynkowej lub przedsiębiorców telekomunikacyjnych zajmujących kolektywną pozycję znaczącą oraz:

a) nakłada obowiązki regulacyjne, biorąc pod uwagę adekwatność i proporcjonalność danego obowiązku do problemów rynkowych, których rozwiązanie służy realizacji celów określonych w art. 1 ust. 2, albo
b) utrzymuje nałożone obowiązki regulacyjne, jeżeli przedsiębiorca telekomunikacyjny lub przedsiębiorcy telekomunikacyjni nie utracili tej pozycji, albo
c) zmienia nałożone obowiązki regulacyjne, jeżeli przedsiębiorca telekomunikacyjny lub przedsiębiorcy telekomunikacyjni nie utracili tej pozycji, ale zmiany na rynku właściwym uzasadniają zmianę tych obowiązków.

Art. 24a. 1. Jeżeli przed wydaniem rozstrzygnięcia, o którym mowa w art. 23 ust. 1 albo w art. 24, na tym samym rynku właściwym występował przedsiębiorca telekomunikacyjny o znaczącej pozycji rynkowej lub przedsiębiorcy telekomunikacyjni zajmujący kolektywną pozycję znaczącą, którzy utracili tę pozycję, Prezes UKE, w drodze decyzji, określa termin uchylenia obowiązków regulacyjnych, tak aby uchylenie to uwzględniało sytuację przedsiębiorców telekomunikacyjnych działających na rynku objętych tą decyzją, nie dłuższy jednak niż przewidziane w umowach zawartych pomiędzy przedsiębiorcami okresy wypowiedzenia umowy.

2. Decyzję, o której mowa w ust. 1, ogłasza się na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej.

Art. 25. 1. Przedsiębiorca telekomunikacyjny zajmuje znaczącą pozycję rynkową, jeżeli na rynku właściwym samodzielnie posiada pozycję ekonomiczną odpowiadającą dominacji w rozumieniu przepisów prawa wspólnotowego.

2. Prezes UKE przy ocenie pozycji rynkowej przedsiębiorcy telekomunikacyjnego na rynku właściwym bierze pod uwagę kryteria wymienione w wytycznych Komisji, o których mowa w art. 19 ust. 3.

3. Dwóch lub więcej przedsiębiorców telekomunikacyjnych zajmuje kolektywną pozycję znaczącą, jeżeli nawet przy braku powiązań organizacyjnych lub innych związków między nimi posiadają na rynku właściwym pozycję ekonomiczną odpowiadającą dominacji w rozumieniu przepisów prawa wspólnotowego.

4. Prezes UKE przy ustalaniu, czy dwóch lub więcej przedsiębiorców telekomunikacyjnych zajmuje kolektywną znaczącą pozycję na rynku właściwym ocenia

cechy rynku właściwego, w szczególności udział przedsiębiorców w rynku oraz jego przejrzystość, a jeżeli ocena tych cech nie wskazuje na brak kolektywnej pozycji znaczącej dodatkowo stosuje w szczególności następujące kryteria:

1) dojrzałość rynku,
2) zastój albo umiarkowany wzrost popytu,
3) niską elastyczność popytu,
4) jednorodność produktów,
5) podobne struktury kosztów przedsiębiorców,
6) brak innowacji technologicznych, dojrzałość technologii,
7) brak możliwości zwiększenia produkcji lub świadczenia usług,
8) wysokie bariery dostępu do rynku,
9) brak równoważącej siły nabywczej,
10) brak potencjalnej konkurencji,
11) różnego rodzaju nieformalne lub inne powiązania pomiędzy danymi przedsiębiorcami,
12) brak albo ograniczenie konkurencji cenowej,
13) możliwość stosowania mechanizmów odwetowych

– które nie muszą być spełnione łącznie.

Art. 25a. W przypadku określenia rynku właściwego odbiegającego od zalecenia Komisji Prezes UKE poddaje projekt rozstrzygnięcia, o którym mowa w art. 23 ust. 1 albo w art. 24, postępowaniu konsolidacyjnemu.

Art. 25b. Rozstrzygnięcie, o którym mowa w art. 23 ust. 1 albo w art. 24:

1) wydaje się po zasięgnięciu opinii Prezesa UOKiK wydanej w formie postanowienia;
2) ogłasza się na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej.

Art. 25c. W przypadku rynku właściwego uznanego decyzją Komisji Europejskiej za rynek ponadnarodowy Prezes UKE przeprowadza jego analizę w porozumieniu z organami regulacyjnymi innych państw członkowskich. Przepis art. 23 lub 24 stosuje się odpowiednio.”;

8) w art. 34 w ust. 2 pkt 12 otrzymuje brzmienie:

„12) świadczeniu usług telekomunikacyjnych z uwzględnieniem pierwszeństwa zgodnie z art. 176a ust. 2 pkt 3.”;

9) art. 56 otrzymuje brzmienie:

„Art. 56. 1. Świadczenie usług telekomunikacyjnych odbywa się na podstawie umowy o świadczenie usług telekomunikacyjnych.

2. Umowę o świadczenie usług telekomunikacyjnych zawiera się w formie pisemnej. Wymóg formy pisemnej nie dotyczy umowy o świadczenie usług telekomunikacyjnych zawieranych przez dokonanie czynności faktycznych obejmujących w szczególności umowy o świadczenie usług telefonicznych za pomocą aparatu publicznego lub przez wybranie numeru dostępu do sieci dostawcy usług.

3. Umowa o świadczenie usług telekomunikacyjnych, z zastrzeżeniem ust. 5, powinna określać w szczególności:

1) strony umowy, w tym nazwę (firmę), adres i siedzibę dostawcy usług;
2) rodzaj świadczonych usług;
3) termin oczekiwania na przyłączenie do sieci lub termin rozpoczęcia świadczenia usług;
4) okres, na jaki została zawarta umowa;
5) pakiet taryfowy, jeżeli na świadczone usługi obowiązują różne pakiety taryfowe;
6) sposób składania zamówień na pakiety taryfowe oraz dodatkowe opcje usługi;
7) okres rozliczeniowy;
8) tryb i warunki dokonywania zmian umowy oraz warunki jej przedłużenia;
9) zakres świadczonych publicznie dostępnych usług telekomunikacyjnych, ze wskazaniem elementów składających się na opłatę abonamentową;
10) dane dotyczące jakości usług;
11) zakres obsługi serwisowej;
12) sposób i termin rozwiązania umowy;
13) zakres odpowiedzialności z tytułu niewykonania lub nienależytego wykonania umowy, wysokość odszkodowania oraz zasady i terminy jego wypłaty;
14) zasady, tryb i terminy składania oraz rozpatrywania reklamacji;
15) informację o polubownych sposobach rozwiązywania sporów;
16) sposób uzyskania informacji o aktualnym cenniku usług oraz kosztach usług serwisowych.

4. Umowa o zapewnienie przyłączenia do publicznej sieci telekomunikacyjnej poza elementami, o których mowa w ust. 3, powinna określać numer przydzielony abonentowi, a w przypadku przyłączenia do publicznej stacjonarnej sieci telefonicznej także adres zakończenia sieci.

5. Dane, o których mowa w ust. 3 pkt 9-16, na podstawie wyraźnego postanowienia umowy, mogą być zawarte w regulaminie świadczenia publicznie dostępnych usług telekomunikacyjnych.”;

10) w art. 57:

a) ust. 4 otrzymuje brzmienie:

„4. Przepisów ust. 2 i 3 nie stosuje się do umów o świadczenie usług telekomunikacyjnych zawieranych przez dokonanie czynności faktycznych, o których mowa w art. 56 ust. 2.”,

b) ust. 6 otrzymuje brzmienie:

„6. W przypadku zawarcia umowy o świadczenie usług telekomunikacyjnych, w tym o zapewnienie przyłączenia do publicznej sieci telekomunikacyjnej, związanego z ulgą przyznaną abonentowi, wysokość roszczenia z tytułu jednostronnego rozwiązania umowy przez abonenta lub przez dostawcę usług z winy abonenta przed upływem terminu ustalonego w umowie nie może przekroczyć wartości ulgi przyznanej abonentowi pomniejszonej o proporcjonalną jej wartość za okres od dnia zawarcia umowy do dnia jej rozwiązania.”;

11) w art. 59 ust. 2 otrzymuje brzmienie:

„2. Przepis ust. 1 stosuje się do użytkowników końcowych usługi przedpłaconej świadczonej w ruchomej publicznej sieci telefonicznej.”;

12) art. 60 otrzymuje brzmienie:

„Art. 60. Regulamin świadczenia usług dostawcy publicznie dostępnych usług telekomunikacyjnych dla użytkowników końcowych usługi przedpłaconej świadczonej w ruchomej publicznej sieci telefonicznej powinien określać w szczególności:

1) nazwę (firmę), adres i siedzibę dostawcy usług;
2) zakres świadczonych publicznie dostępnych usług telekomunikacyjnych, ze wskazaniem elementów składających się na opłatę za świadczenie usług;

3) standardowe warunki umowy, w tym wskazanie minimalnego czasu trwania umowy, jeżeli taki został określony;
4) zakres obsługi serwisowej;
5) zakres odpowiedzialności z tytułu niewykonania lub nienależytego wykonania umowy, wysokość odszkodowania oraz zasady i terminy jego wypłaty;
6) zasady, tryb i terminy składania oraz rozpatrywania reklamacji;
7) sposób uzyskania informacji o aktualnym cenniku usług oraz kosztach usług serwisowych.”;

13) po art. 60 dodaje się art. 60a w brzmieniu:

„Art. 60a. 1. Dostawca publicznie dostępnych usług telekomunikacyjnych:

1) doręcza abonentowi na piśmie treść każdej proponowanej zmiany warunków umowy, o której mowa w art. 56 ust. 3,
2) doręcza abonentowi na piśmie oraz podaje do publicznej wiadomości treść każdej proponowanej zmiany warunków umowy określonych w regulaminie, o którym mowa w art. 59 ust. 1, oraz
3) podaje do publicznej wiadomości treść każdej proponowanej zmiany warunków umowy określonych w regulaminie, o którym mowa w art. 60

– z wyprzedzeniem co najmniej jednego okresu rozliczeniowego przed wprowadzeniem tych zmian w życie. Jednocześnie abonent powinien zostać poinformowany o prawie wypowiedzenia umowy w przypadku braku akceptacji zmian w regulaminie.

2. W razie skorzystania z prawa wypowiedzenia umowy w przypadku braku akceptacji niekorzystnej dla abonenta zmiany w umowie lub regulaminie, dostawcy publicznie dostępnych usług telekomunikacyjnych nie przysługuje roszczenie odszkodowawcze, a także zwrot ulgi, o której mowa w art. 57 ust. 6, o czym abonent powinien zostać także poinformowany. Jeżeli proponowane zmiany dotyczą warunków umowy, o których mowa w art. 56 ust. 3, a abonent nie skorzystał z prawa wypowiedzenia umowy, warunki umowy pozostają bez zmian.

3. Przepisu ust. 2 nie stosuje się, jeżeli konieczność wprowadzenia zmian, o których mowa w ust. 1, następuje na skutek zmiany przepisów prawa.”;

14) w art. 61:

a) ust. 5 i 6 otrzymują brzmienie:

„5. Dostawca publicznie dostępnych usług telekomunikacyjnych doręcza abonentowi na piśmie oraz podaje do publicznej wiadomości treść każdej zmiany w cenniku, z wyprzedzeniem co najmniej jednego okresu rozliczeniowego przed wprowadzeniem tych zmian w życie. Jednocześnie abonent powinien zostać poinformowany o prawie wypowiedzenia umowy w przypadku braku akceptacji zmiany w cenniku.

6. W przypadku, o którym mowa w ust. 5, abonent powinien zostać poinformowany także o tym, że w razie skorzystania z prawa wypowiedzenia umowy w przypadku braku akceptacji podwyższenia cen dostawcy publicznie dostępnych usług telekomunikacyjnych nie przysługuje roszczenie odszkodowawcze, a także zwrot ulgi, o której mowa w art. 57 ust. 6.”,

b) po ust. 6 dodaje się ust. 6a w brzmieniu:

„6a. Przepisu ust. 6 nie stosuje się, jeżeli konieczność wprowadzenia zmiany, o której mowa w ust. 5, następuje na skutek zmiany przepisów prawa.”;

15) w art. 71 dodaje się ust. 4 i 5 w brzemieniu:

„4. Prezes UKE prowadzi bazę danych zawierającą przeniesione numery, o których mowa w ust. 1.

5. Operator publicznej sieci telefonicznej jest obowiązany połączyć tę sieć bezpośrednio lub za pośrednictwem publicznej sieci telefonicznej innego operatora z bazą danych, o której mowa w ust. 4. Operator publicznej sieci telefonicznej jest obowiązany dokonywać na bieżąco aktualizacji bazy danych, o której mowa w ust. 4.”;

16) w art. 153 w ust. 4 uchyla się pkt 5 – 7;

17) w art. 159 w ust. 1 pkt 5 otrzymuje brzmienie:

„5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawionych połączeń.”;

18) w art. 161 w ust. 2 pkt 6 otrzymuje brzmienie:

„6) nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numeru paszportu lub karty pobytu;”;

19) w art. 165:

a) uchyla się ust. 1,

b) ust. 5 otrzymuje brzmienie:

„5. Do przetwarzania danych transmisyjnych, zgodnie z ust. 2-4, uprawnione są podmioty działające z upoważnienia operatorów publicznych sieci telekomunikacyjnych i dostawców publicznie dostępnych usług telekomunikacyjnych, zajmujące się naliczaniem opłat, zarządzaniem ruchem w sieciach telekomunikacyjnych, obsługą klienta, systemem wykrywania nadużyć finansowych, marketingiem usług telekomunikacyjnych lub świadczeniem usług o wartości wzbogaconej. Podmioty te mogą przetwarzać dane transmisyjne wyłącznie dla celów niezbędnych przy wykonywaniu tych działań.”;

20) w art. 166 uchyla się ust. 5;

21) w art. 169 w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Dane osobowe posiadane przez przedsiębiorcę telekomunikacyjnego zawarte w publicznie dostępnym spisie abonentów, zwanym dalej „spisem”, wydawanym w formie książkowej lub elektronicznej, a także udostępniane za pośrednictwem służb informacyjnych przedsiębiorcy telekomunikacyjnego powinny być ograniczone do:”;

22) w art. 171:

a) ust. 2 i 3 otrzymują brzmienie:

„2. Dostawca usług świadczonych w publicznej sieci telefonicznej umożliwiającej prezentację identyfikacji linii wywołującej jest obowiązany zapewnić, za pomocą prostych środków:

1) użytkownikowi wywołującemu – możliwość jednorazowego wyeliminowania prezentacji identyfikacji linii wywołującej u użytkownika wywoływanego podczas wywołania i połączenia;
2) abonentowi wywołującemu – możliwość stałego wyeliminowania prezentacji identyfikacji linii wywołującej u użytkownika wywoływanego podczas wywołania

i połączenia, u operatora, do którego sieci jest przyłączony abonent będący stroną umowy z dostawcą usług;

3) abonentowi wywoływanemu – możliwość eliminacji dla połączeń przychodzących prezentacji identyfikacji linii wywołującej, a jeżeli taka prezentacja jest dostępna przed rozpoczęciem połączenia przychodzącego, także możliwość blokady połączeń przychodzących od abonenta lub użytkownika stosującego eliminację prezentacji identyfikacji linii wywołującej.

3. Dostawca usług świadczonych w publicznej sieci telefonicznej zapewniającej prezentację identyfikacji zakończenia sieci, do której zostało przekierowane połączenie, zwaną dalej „prezentacją identyfikacji linii wywoływanej", jest obowiązany zapewnić abonentowi wywoływanemu możliwość eliminacji, za pomocą prostych środków, prezentacji identyfikacji linii wywoływanej u użytkownika wywołującego.",

b) ust. 8 otrzymuje brzmienie:

„8. Przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia służbom ustawowo powołanym do niesienia pomocy dostępu do identyfikacji linii wywołującej oraz danych dotyczących lokalizacji, bez uprzedniej zgody zainteresowanych abonentów lub użytkowników, jeżeli jest to konieczne do umożliwienia tym służbom wykonywania ich zadań w możliwie najbardziej efektywny sposób.",

c) ust. 10 otrzymuje brzmienie:

„10. Dane, o których mowa w ust. 9, pozostają w dyspozycji przedsiębiorcy telekomunikacyjnego. Do ich udostępniania stosuje się art. 180d.";

23) art. 176 otrzymuje brzmienie:

„Art. 176. Przedsiębiorca telekomunikacyjny jest obowiązany do wykonywania zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie i na warunkach określonych w niniejszej ustawie oraz w przepisach odrębnych.";

24) po art. 176 dodaje się art. 176a w brzmieniu:

„Art. 176a. 1. Przedsiębiorca telekomunikacyjny, w celu zapewnienia ciągłości świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia:

1) sytuacji kryzysowych,
2) stanów nadzwyczajnych,
3) bezpośrednich zagrożeń dla infrastruktury przedsiębiorcy

– zwanych dalej „sytuacjami szczególnych zagrożeń”.

2. Przedsiębiorca telekomunikacyjny, z zastrzeżeniem ust. 5 pkt 2, jest obowiązany posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, zwane dalej „planami”, dotyczące w szczególności:

1) współpracy z innymi przedsiębiorcami telekomunikacyjnymi;
2) współpracy z zagranicznymi operatorami telekomunikacyjnymi, a w szczególności państw sąsiadujących;
3) współpracy z podmiotami i służbami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy ludności, a także zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego oraz z podmiotami właściwymi w sprawach zarządzania kryzysowego, wskazanymi w ramach uzgodnień planów, o których mowa w ust. 3, przez organy uzgadniające plany;
4) zabezpieczenia infrastruktury telekomunikacyjnej w sytuacjach szczególnych zagrożeń oraz przed nieuprawnionym dostępem;
5) utrzymania ciągłości, a w przypadku jej utraty, odtwarzania:
    a) świadczenia usług telekomunikacyjnych,
    b) dostarczania sieci telekomunikacyjnej
    – z uwzględnieniem pierwszeństwa dla podmiotów i służb, o których mowa w pkt 3;
6) technicznych i organizacyjnych przygotowań, w przypadku wprowadzenia ograniczeń w działalności telekomunikacyjnej przewidzianych ustawą;
7) sposobu udostępniania urządzeń telekomunikacyjnych, o którym mowa w art. 177 ust. 3, przez przedsiębiorców telekomunikacyjnych;
8) ewidencji i gromadzenia rezerw przedsiębiorcy lub współpracy z dostawcami sprzętu oraz usług serwisowych i naprawczych.

3. Z zastrzeżeniem ust. 5 pkt 1 lit. c, przedsiębiorca telekomunikacyjny sporządzający plany dokonuje uzgodnienia ich zawartości z organami, o których mowa w ust. 5 pkt 1 lit. b.

4. Po stwierdzeniu wystąpienia sytuacji szczególnych zagrożeń lub po uzyskaniu informacji o ich wystąpieniu od podmiotów lub służb, o których mowa w ust. 2 pkt 3, przedsiębiorca telekomunikacyjny podejmuje niezwłocznie działania określone w planach.

5. Rada Ministrów, mając na uwadze zakres i rodzaj wykonywanej działalności telekomunikacyjnej, wielkość przedsiębiorcy telekomunikacyjnego i jego znaczenie dla gospodarki, obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, a także wymagania, o których mowa w ust. 2, w drodze rozporządzenia:

1) określi:
   a) rodzaje planów, ich zawartość oraz tryb sporządzania i aktualizacji,
   b) organy uzgadniające plany oraz zakres tych uzgodnień,
   c) rodzaje przedsiębiorców telekomunikacyjnych obowiązanych do uzgadniania zawartości planów;
2) może określić rodzaje działalności telekomunikacyjnej lub rodzaje przedsiębiorców telekomunikacyjnych niepodlegających obowiązkowi sporządzania planu.”;

25) w art. 177:

a) uchyla się ust. 1 i 2,

b) ust. 3 – 5 otrzymują brzmienie:

„3. Przedsiębiorca telekomunikacyjny w sytuacjach szczególnych zagrożeń jest obowiązany do nieodpłatnego udostępniania urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej innemu przedsiębiorcy telekomunikacyjnemu, podmiotowi i służbie, o których mowa w art. 176a ust. 2 pkt 3, z zachowaniem zasady minimalizowania negatywnych skutków takiego udostępnienia tych urządzeń dla ciągłości wykonywania działalności telekomunikacyjnej przez przedsiębiorcę.

4. Podmioty, w tym niebędące przedsiębiorcami telekomunikacyjnymi, używające radiowe urządzenia nadawcze lub nadawczo-odbiorcze stosowane w służbach radiokomunikacyjnych, w sytuacjach szczególnych zagrożeń są obowiązane do nieodpłatnego udostępniania urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej podmiotom koordynującym działania ratownicze, podmiotom właściwym w sprawach zarządzania kryzysowego, służbom ustawowo powołanym do niesienia pomocy, a także innym podmiotom realizującym zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

5. Przepisy ust. 3 i 4 stosuje się odpowiednio podczas przeprowadzania akcji ratowniczej o zasięgu międzynarodowym, co najmniej w zakresie ustalonym umowami międzynarodowymi, których Rzeczpospolita Polska jest stroną.”,

c) dodaje się ust. 6 w brzmieniu:

„6. Rada Ministrów określi, w drodze rozporządzenia, tryb nieodpłatnego udostępniania radiowych urządzeń nadawczych lub nadawczo-odbiorczych stosowanych w służbach radiokomunikacyjnych przez podmioty niebędące przedsiębiorcami telekomunikacyjnymi, mając na uwadze konieczność zachowania zasady minimalizowania negatywnych skutków udostępniania tych urządzeń.”;

26) w art. 178:

a) w ust. 1 pkt 1 otrzymuje brzmienie:

„1) utrzymania ciągłości lub odtwarzania:

a) dostarczania sieci telekomunikacyjnej,

b) świadczenia usług telekomunikacyjnych

– z uwzględnieniem pierwszeństwa dla podmiotów i służb, o których mowa w ust. 2 pkt 1;”,

b) ust. 2 i 3 otrzymują brzmienie:

„2. Decyzja Prezesa UKE, o której mowa w ust. 1:

1) wydawana jest z urzędu lub na wniosek podmiotów koordynujących działania ratownicze, podmiotów właściwych w sprawach zarządzania kryzysowego, służb ustawowo powołanych do niesienia pomocy, a także innych podmiotów realizujących zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;
2) może być ogłoszona ustnie, bez uzasadnienia, w całości lub części, jeżeli wymagają tego względy obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

3. W przypadkach i na zasadach określonych w przepisach odrębnych Komendant Główny Policji, komendant wojewódzki Policji, Komendant Główny Straży Granicznej, komendant Oddziału Straży Granicznej, Komendant Główny Żandarmerii Wojskowej, komendant Oddziału Żandarmerii Wojskowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego oraz Szef Biura Ochrony Rządu mogą zarządzić o zastosowaniu urządzeń uniemożliwiających telekomunikację na określonym obszarze.”;

27) w art. 179:

a) uchyla się ust. 1,

b) ust. 3 otrzymuje brzmienie:

„3. Przedsiębiorca telekomunikacyjny, z zastrzeżeniem ust. 12 pkt 2, jest obowiązany do:

1) zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania, zwanych dalej „warunkami dostępu i utrwalania”, umożliwiających jednoczesne i wzajemnie niezależne:

a) uzyskiwanie przez Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i wywiad skarbowy, zwane dalej „uprawnionymi podmiotami”, w sposób określony w ust. 4b, dostępu do:

– treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych, zwanych dalej „przekazami telekomunikacyjnymi”, nadawanych lub odbieranych przez użytkownika końcowego lub urządzenie końcowe,

– posiadanych przez przedsiębiorcę danych związanych z przekazami telekomunikacyjnymi, o których mowa w ust. 9, art. 159 ust. 1 pkt 1 i pkt 3-5,

b) uzyskiwanie przez uprawnione podmioty danych związanych ze świadczoną usługą telekomunikacyjną i danych, o których mowa w art. 161,

c) utrwalanie przez uprawnione podmioty przekazów telekomunikacyjnych i danych, o których mowa w lit. a i b;

2) utrwalania na rzecz sądu i prokuratora przekazów telekomunikacyjnych i danych, o których mowa w pkt 1 lit. a i b.”,

c) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu:

„3a. Przedsiębiorca telekomunikacyjny zapewnia, na własny koszt, warunki dostępu i utrwalania w zakresie wszystkich świadczonych usług telekomunikacyjnych, począwszy od dnia rozpoczęcia działalności telekomunikacyjnej, a w przypadku rozpoczęcia świadczenia nowej usługi telekomunikacyjnej od dnia jej uruchomienia.

3b. Przedsiębiorca telekomunikacyjny zapewnia, na własny koszt, utrwalanie na rzecz sądu lub prokuratora przekazów telekomunikacyjnych i danych, o których mowa w ust. 3 pkt 1 lit. a i b.”,

d) ust. 4 otrzymuje brzmienie:

„4. Przedsiębiorca telekomunikacyjny zapewnia warunki dostępu i utrwalania z zachowaniem wymagań określonych w rozporządzeniu, o którym mowa w ust. 12.”,

e) po ust. 4 dodaje się ust. 4a – 4c w brzmieniu:

„4a. Warunki dostępu i utrwalania mogą być zapewniane za pomocą interfejsów zlokalizowanych w miejscach obejmowanych przez sieć przedsiębiorcy telekomunikacyjnego na zasadach określonych w umowach zawartych przez uprawnione podmioty z przedsiębiorcą telekomunikacyjnym. 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 telekomunikacyjnego, umożliwiające: techniczną realizację interfejsu, niezbędną ochronę tego miejsca wynikającą z przepisów odrębnych oraz minimalizację nakładów ponoszonych przez przedsiębiorcę telekomunikacyjnego i podmioty uprawnione.

4b. Zapewnienie warunków dostępu i utrwalania powinno umożliwiać uprawnionym podmiotom dostęp do przekazów telekomunikacyjnych i danych bez udziału pracowników przedsiębiorcy telekomunikacyjnego. Za zgodą uprawnianego podmiotu warunki dostępu i utrwalania mogą być zapewnione przy niezbędnym współudziale upoważnionych pracowników przedsiębiorcy telekomunikacyjnego gwarantujących prawidłową realizację przedmiotowych czynności w zakresie określonym przez uprawniony podmiot.

4c. Dopuszcza się możliwość zapewnienia warunków dostępu i utrwalania przez dwóch lub więcej przedsiębiorców telekomunikacyjnych za pomocą tych samych interfejsów. Szczegółowe zasady współpracy przedsiębiorców telekomunikacyjnych w tym zakresie regulują umowy zawarte pomiędzy nimi. Przed zawarciem umowy przedsiębiorcy telekomunikacyjni uzgadniają warunki techniczne i eksploatacyjne z uprawnionymi podmiotami. Zawarcie umowy nie zwalnia jej stron z indywidualnej odpowiedzialności za zapewnienie warunków dostępu i utrwalania.”,

f) uchyla się ust. 5,

g) ust. 6 otrzymuje brzmienie:

„6. Prezes UKE, na uzasadniony wniosek przedsiębiorcy telekomunikacyjnego, po uzyskaniu, w terminie określonym w art. 106 Kodeksu postępowania administracyjnego zgody uprawnionych podmiotów, może, w całości lub w części, w drodze decyzji, zawiesić na okres nie dłuższy niż 6 miesięcy, obowiązek zapewnienia warunków dostępu i utrwalania.

Wniosek składa się w terminie nie dłuższym niż 14 dni od dnia wystąpienia zdarzenia, o którym mowa w zdaniu pierwszym. Do wniosku dołącza się harmonogram osiągnięcia przez przedsiębiorcę telekomunikacyjnego pełnej zdolności do wykonywania obowiązku.” ,

h) po ust. 6 dodaje się ust. 6a i 6b w brzmieniu:

„6a. Przepisu ust. 6 nie stosuje się do przedsiębiorcy telekomunikacyjnego rozpoczynającego działalność telekomunikacyjną lub rozpoczynającego świadczenie nowej usługi telekomunikacyjnej.

6b. Złożenie wniosku lub zawieszenie obowiązku zapewnienia warunków dostępu i utrwalania nie zwalnia przedsiębiorcy telekomunikacyjnego z obowiązku zapewnienia warunków dostępu i utrwalania, w zakresie posiadanych możliwości technicznych, organizacyjnych i finansowych.”,

i) ust. 7 i 8 otrzymują brzmienie:

„7. Przedsiębiorca telekomunikacyjny może powierzyć, w drodze umowy, innemu przedsiębiorcy telekomunikacyjnemu zapewnienie warunków dostępu i utrwalania. Powierzenie to nie zwalnia powierzającego z odpowiedzialności za zapewnienie warunków dostępu i utrwalania.

8. Przedsiębiorca telekomunikacyjny jest obowiązany do wskazania Prezesowi UKE:

1) jednostki organizacyjnej lub osoby mającej siedzibę lub miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej uprawnionej do reprezentowania tego przedsiębiorcy w sprawach związanych z zapewnieniem warunków dostępu i utrwalania;
2) przedsiębiorcy telekomunikacyjnego, który będzie w jego imieniu zapewniał warunki dostępu i utrwalania;
3) przedsiębiorcy telekomunikacyjnego, wspólnie z którym będzie zapewniał warunki dostępu i utrwalania za pomocą tych samych interfejsów.”,

j) po ust. 8 dodaje się ust. 8a w brzmieniu:

„8a. W przypadku zmiany danych podmiotów, o których mowa w ust. 8, przedsiębiorca telekomunikacyjny jest obowiązany poinformować Prezesa UKE o tych zmianach.”,

k) ust. 10 otrzymuje brzmienie:

„10. Prezes UKE przekazuje niezwłocznie informacje, o których mowa w ust. 8 i 8a, Ministrowi Sprawiedliwości, Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw finansów publicznych, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Centralnego Biura Antykorupcyjnego, Szefowi Służby Kontrwywiadu Wojskowego, a także ministrowi, którego zakres zadań obejmuje koordynowanie działalności służb specjalnych – jeżeli został powołany.”,

l) uchyla się ust. 11,

m) dodaje się ust. 12 w brzmieniu:

„12. Rada Ministrów określi, w drodze rozporządzenia:

1) wymagania i sposób zapewnienia warunków dostępu i utrwalania, o których mowa w ust. 3 i art. 180d, z wyłączeniem spraw uregulowanych w art. 242 Kodeksu postępowania karnego, kierując się zasadą osiągania celu przy jak najniższych nakładach;
2) rodzaje działalności telekomunikacyjnej lub rodzaje przedsiębiorców telekomunikacyjnych niepodlegających obowiązkowi zapewnienia warunków dostępu i utrwalania, o których mowa w ust. 3 i art. 180d, kierując się zakresem i rodzajem świadczonych usług telekomunikacyjnych lub wielkością sieci telekomunikacyjnych przedsiębiorców.”;

28) po art. 180 dodaje się art. 180a – 180g w brzmieniu:

„Art. 180a. 1. Z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt:

1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć;
2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także sądowi i prokuratorowi, na zasadach i w trybie określonym w przepisach odrębnych;
3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym

przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami art. 159 – 175 i art. 180e.

2. Z zastrzeżeniem ust. 3, obowiązek, o którym mowa w ust. 1, uważa się za wykonany, jeżeli operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych w przypadku zaprzestania działalności telekomunikacyjnej, przekaże dane do dalszego przechowywania, udostępniania oraz ochrony innemu operatorowi publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych.

3. Jeżeli ogłoszono upadłość operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych, upadły operator lub dostawca ma obowiązek przekazania danych, o których mowa w ust. 1, do dalszego przechowywania, udostępniania oraz ochrony Prezesowi UKE.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób przekazywania Prezesowi UKE danych w przypadku, o którym mowa w ust. 3, oraz sposób udostępniania przez Prezesa UKE tych danych podmiotom, o których mowa w ust. 1 pkt 2, w celu zapewnienia realizacji zadań przez te podmioty.

5. Obowiązkowi, o którym mowa w ust. 1, podlegają dane dotyczące połączeń zrealizowanych i nieudanych prób połączeń, o których mowa w art. 159 ust. 1 pkt 5.

6. Obowiązek, o którym mowa w ust. 1, powinien być realizowany w sposób, który nie powoduje ujawniania przekazu telekomunikacyjnego.

7. Udostępnianie danych, o którym mowa w ust. 1 pkt 1, może nastąpić za pomocą sieci telekomunikacyjnej, chyba że przepisy odrębne stanowią inaczej.

Art. 180b. 1. Obowiązek, o którym mowa w art. 180a ust. 1, może być wykonywany wspólnie przez dwóch lub więcej operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych.

2. Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych może powierzyć realizację obowiązku, o którym mowa w art. 180a ust. 1, w drodze umowy, innemu przedsiębiorcy telekomunikacyjnemu. Powierzenie to nie zwalnia powierzającego z odpowiedzialności za realizację tego obowiązku.

Art. 180c. 1. Obowiązkiem, o którym mowa w art. 180a ust. 1, objęte są dane niezbędne do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego:
    a) inicjującego połączenie,
    b) do którego kierowane jest połączenie;
2) określenia:
    a) daty i godziny połączenia telefonicznego oraz czasu jego trwania,
    b) rodzaju połączenia telefonicznego,
    c) lokalizacji telekomunikacyjnego urządzenia końcowego używanego w ruchomej publicznej sieci telefonicznej, dotyczącej połączenia lub próby uzyskania połączenia.

2. Minister właściwy do spraw łączności w porozumieniu z ministrem właściwym do spraw wewnętrznych, mając na uwadze rodzaj wykonywanej działalności telekomunikacyjnej przez operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych, dane określone w ust. 1, koszty pozyskania i utrzymania danych oraz potrzebę unikania wielokrotnego zatrzymywania i przechowywania tych samych danych, określi, w drodze rozporządzenia:

1) szczegółowy wykaz danych, o których mowa w ust. 1;
2) rodzaje operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania tych danych.

Art. 180d. Przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom na własny koszt, a także sądowi i prokuratorowi, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i pkt 3-5, w art. 161 oraz w art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych.

Art. 180e. W celu ochrony danych, o której mowa w art. 180a ust. 1 pkt 3, przedsiębiorca telekomunikacyjny stosuje właściwe środki techniczne i organizacyjne oraz zapewnia dostęp do tych danych jedynie upoważnionym pracownikom.

Art. 180f. 1. Przedsiębiorca telekomunikacyjny jest obowiązany dostarczać Prezesowi UKE dane dotyczące infrastruktury telekomunikacyjnej eksploatowanej lub używanej przez

tego przedsiębiorcę, niezbędnej do przygotowania systemów łączności na potrzeby obronne państwa, w tym systemu kierowania bezpieczeństwem narodowym, i aktualizować niezwłocznie po każdej zmianie.

2. Dane, o których mowa w ust. 1, są gromadzone w bazie danych utworzonej i zarządzanej przez Prezesa UKE. Bazę aktualizuje się niezwłocznie po każdej zmianie danych.

3. Minister właściwy do spraw łączności określi, w drodze rozporządzenia, szczegółowy zakres danych, o których mowa w ust 1, formę i tryb ich dostarczania oraz aktualizacji, mając na uwadze warunki i sposób przygotowania oraz wykorzystania systemów łączności na potrzeby obronne państwa, bezpieczeństwo przekazywanych danych oraz zapewnienie ich jednorodnej postaci.

Art. 180g. 1. Przedsiębiorca telekomunikacyjny, w terminie do dnia 31 stycznia, składa Prezesowi UKE, za rok poprzedni informacje o:

1) liczbie przypadków, w których uprawnionym podmiotom, sądowi i prokuratorowi były udostępnione dane, o których mowa w art. 180a ust. 1;
2) czasie, jaki upłynął między datą zatrzymania danych a datą złożenia przez podmioty, o których mowa w pkt 1, wniosku lub ustnego żądania o ich udostępnienie;
3) przypadkach, w których wniosek lub ustne żądanie, o którym mowa w pkt 2, nie mógł być zrealizowany.

2. Prezes UKE przekazuje corocznie Komisji Europejskiej informacje, o których mowa w ust. 1.

3. Minister właściwy do spraw łączności określi, w drodze rozporządzenia, wzór formularza służącego do przekazywania informacji Prezesowi UKE, kierując się potrzebą przekazania Komisji Europejskiej pełnej i rzetelnej informacji.”;

29) uchyla się art. 181;

30) art. 182 otrzymuje brzmienie:

„Art. 182. Rada Ministrów określi, w drodze rozporządzenia, wymagania techniczne i eksploatacyjne dla interfejsów, o których mowa w art. 179 ust. 4a, umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, o których mowa w art. 179 ust. 3 i w art. 180d,

kierując się zasadą minimalizacji nakładów przedsiębiorcy telekomunikacyjnego i podmiotów uprawnionych.”;

31) tytuł działu X otrzymuje brzmienie:

„DZIAŁ X

Administracja łączności i postępowanie przed Prezesem UKE”;

32) w art. 190:

a) ust. 2 otrzymuje brzmienie:

„2. Prezes UKE składa ministrowi właściwemu do spraw łączności coroczne sprawozdanie ze swojej działalności regulacyjnej oraz realizacji polityki rządu i wspólnotowej polityki telekomunikacyjnej, za rok poprzedni, w terminie do dnia 30 kwietnia. Minister właściwy do spraw łączności opiniuje sprawozdanie w terminie 1 miesiąca od dnia jego przedstawienia przez Prezesa UKE i przekazuje sprawozdanie wraz z opinią Prezesowi Rady Ministrów. Negatywna opinia stanowi podstawę do złożenia przez Prezesa Rady Ministrów wniosku o odwołanie Prezesa UKE.”,

b) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Prezes UKE przekazuje ministrowi właściwemu do spraw łączności, na jego żądanie, informacje o swojej działalności.”,

c) ust. 4 otrzymuje brzmienie:

„4. Prezesa UKE powołuje i odwołuje Sejm za zgodą Senatu na wniosek Prezesa Rady Ministrów. Kadencja Prezesa UKE trwa 5 lat. Po upływie kadencji Prezes UKE pełni swoją funkcję do czasu powołania następcy.”,

d) po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. Prezes UKE może być odwołany przed upływem kadencji, na którą został powołany, wyłącznie w przypadku:

1) rażącego naruszenia prawa;
2) skazania prawomocnym wyrokiem sądu za popełnione umyślnie przestępstwo lub przestępstwo skarbowe;
3) orzeczenia zakazu zajmowania kierowniczych stanowisk lub pełnienia funkcji związanych ze szczególną odpowiedzialnością w organach państwa;
4) choroby trwale uniemożliwiającej wykonywanie zadań;
5) złożenia rezygnacji;
6) nierealizowania przez Prezesa UKE celów, o których mowa w art. 1 ust. 2.”;

33) w art. 192 w ust. 1 po pkt 5 dodaje się pkt 5a – 5c w brzmieniu:

„5a) kontrolowanie realizacji obowiązków wynikających z przepisów rozporządzenia WE nr 717/2007 Parlamentu Europejskiego i Rady z dnia 27 czerwca 2007 r. w sprawie roamingu w publicznych sieciach telefonii ruchomej wewnątrz Wspólnoty oraz zmieniającego dyrektywę 2002/21/WE (Dz. Urz. WE L 171 z 29.06.2007, str. 32);

5b) wykonywanie kontroli nad operatorami publicznej sieci telekomunikacyjnej i dostawcami publicznie dostępnych usług telekomunikacyjnych w zakresie realizacji obowiązków, o których mowa w art. 180a ust. 1, z wyjątkiem realizacji obowiązków dotyczących danych osobowych chronionych zgodnie z przepisami o ochronie danych osobowych;

5c) prowadzenie baz danych, o których mowa w art. 71 ust. 4 oraz w art. 180f ust. 2;”;

34) w art. 206 ust. 2 – 2b otrzymują brzmienie:

„2. Od decyzji w sprawach o ustalenie znaczącej pozycji rynkowej, nałożenia, zniesienia lub zmiany obowiązków regulacyjnych, nałożenia kar oraz od decyzji wydawanych w sprawach spornych, z wyjątkiem decyzji w sprawie rezerwacji częstotliwości po przeprowadzeniu przetargu albo konkursu oraz od decyzji o uznaniu przetargu albo konkursu za nierozstrzygnięty, przysługuje odwołanie do Sądu Okręgowego w Warszawie – sądu ochrony konkurencji i konsumentów.

2a. Decyzje, o których mowa w ust. 2, z wyjątkiem decyzji w sprawie nałożenia kar i zniesienia obowiązków regulacyjnych, podlegają natychmiastowemu wykonaniu.

2b. Na postanowienie, o którym mowa w art. 23, przysługuje zażalenie do Sądu Okręgowego w Warszawie – sądu ochrony konkurencji i konsumentów.”;

35) w art. 209 w ust. 1:

a) po pkt 13 dodaje się punkt 13a w brzmieniu:

„13a) nie wypełnia lub nienależycie wypełnia obowiązki określone w art. 56 ust. 5, art. 57 ust. 6, art. 60, art. 60a ust. 2 i art. 61 ust. 6,”,

b) dodaje się pkt 28 i 29 w brzmieniu:

„28) nie wypełnia obowiązków wynikających z art. 180g,

29) nie wypełnia obowiązków określonych w art. 3-6 rozporządzenia WE nr 717/2007 Parlamentu Europejskiego i Rady z dnia 27 czerwca 2007 r. w sprawie roamingu w publicznych sieciach telefonii ruchomej wewnątrz Wspólnoty oraz zmieniającego dyrektywę 2002/21/WE”;

36) użyte w art. 34 ust. 1, art. 36, art. 37 ust. 1, art. 38 ust. 1, art. 39 ust. 1, art. 40 ust. 1, art. 42 ust. 1 oraz art. 43 ust. 3 wyrazy „art. 25 ust. 4" zastępuje się wyrazami „art. 24 pkt 2 lit. a";

37) użyte w art. 46 ust. 1, art. 72 ust. 3, art. 134, art. 192 ust. 1 pkt 18, art. 206 ust. 2b wyrazy „art. 23" zastępuje się wyrazami „art. 23 i 24".

Art. 2. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277, z późn. zm.[4)]) wprowadza się następujące zmiany:

1) po art. 18b dodaje się art. 18c w brzmieniu:

„Art. 18c. 1. W przypadkach, o których mowa w art. 18 ust. 1, Komendant Główny Policji lub komendant wojewódzki Policji może zarządzić zastosowanie przez Policję urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

2. O zastosowaniu urządzeń, o których mowa w ust. 1, Komendant Główny Policji lub komendant wojewódzki Policji niezwłocznie informuje Prezesa Urzędu Komunikacji Elektronicznej.";

2) w art. 20c:

a) ust. 1 i 2 otrzymują brzmienie:

„1. W celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]), zwane dalej „danymi telekomunikacyjnymi", oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną udostępnia nieodpłatnie dane telekomunikacyjne:

1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;

[4)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. Nr 57, poz. 390, Nr 120, poz. 818, Nr 140, poz. 981 i Nr 165, poz. 1170 oraz z 2008 r. Nr 86, poz. 521 i Nr 171, poz. 1065.

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.”,

b) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.”,

c) uchyla się ust. 3 i 4,

d) ust. 5 otrzymuje brzmienie:

„5. Udostępnienie Policji danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej jeżeli:

1) wykorzystywane sieci telekomunikacyjne zapewniają:
   a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
   b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;
2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności.”,

e) uchyla się ust. 8.

Art. 3. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997, z późn. zm.[5)]) wprowadza się następujące zmiany:

1) w art. 10b ust. 1 – 4 otrzymują brzmienie:

„1. W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]), zwane dalej „danymi telekomunikacyjnymi", w trybie:

1) pisemnego wniosku Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej albo osoby przez nich upoważnionej,
2) ustnego żądania funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1,
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1,

oraz może przetwarzać te dane.

2. W przypadku, o którym mowa w ust. 1 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Komendantem Głównym Straży Granicznej a tym podmiotem.

3. Podmiot wykonujący działalność telekomunikacyjną udostępnia nieodpłatnie dane telekomunikacyjne, funkcjonariuszowi wskazanemu we wniosku właściwego organu Straży Granicznej lub funkcjonariuszowi, o którym mowa w ust. 1 pkt 2 i 3.

4. Udostępnienie Straży Granicznej danych telekomunikacyjnych może nastąpić przy pomocy sieci, jeżeli:

1) wykorzystywane sieci telekomunikacyjne zapewniają:

   a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,

   b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;

[5)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 90, poz. 757, z 2006 r. Nr 104 poz. 708 i 711 i Nr 170, poz. 1218, z 2007 r. Nr 57, poz. 390 i Nr 82, poz. 558 oraz z 2008 r. Nr 86, poz. 521.

2) jest to uzasadnione specyfiką lub zakresem wykonywanych przez jednostki organizacyjne Straży Granicznej zadań albo prowadzonych przez nie czynności.”;

2) po art. 10c dodaje się art. 10d w brzmieniu:

„Art. 10d. 1. W celu realizacji zadań, o których mowa w art. 1 ust. 2 pkt 1, 2, 4-5d i 10 Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej może zarządzić o zastosowaniu urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez Straż Graniczną, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

2. O zastosowaniu urządzeń, o których mowa w ust. 1, Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej niezwłocznie informuje Prezesa Urzędu Komunikacji Elektronicznej.”.

Art. 4. W ustawie z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65, z późn. zm.[6)]) wprowadza się następujące zmiany:

1) art. 36b otrzymuje brzmienie:

„1. W celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 3 pkt 4 i 5, wywiad skarbowy może mieć udostępniane dane:

1) o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]), zwane dalej „danymi telekomunikacyjnymi”,
2) identyfikujące podmiot korzystający z usług pocztowych oraz dotyczące faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług

oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną lub operator świadczący usługi pocztowe udostępnia nieodpłatnie dane, o których mowa w ust. 1:

1) na pisemny wniosek Generalnego Inspektora Kontroli Skarbowej;
2) na pisemny wniosek pracownika wywiadu skarbowego posiadającego pisemne upoważnienie Generalnego Inspektora Kontroli Skarbowej do występowania w jego imieniu o udostępnienie danych, o których mowa w ust. 1;

[6)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 64, poz. 594, Nr 91, poz. 868, Nr 171, poz. 1800 i Nr 173, poz. 1808, z 2005 r. Nr 132, poz. 1110 i Nr 183, poz. 1537, z 2006 r. Nr 66, poz. 470, Nr 104, poz. 708 i 711, Nr 157, poz. 1119, Nr 191, poz. 1413 i Nr 217, poz. 1590, z 2007 r. Nr 171, poz. 1207 oraz z 2008 r. Nr 110, poz. 707.

3) za pośrednictwem sieci telekomunikacyjnej pracownikowi wywiadu skarbowego posiadającemu pisemne upoważnienie, o którym mowa w pkt 2.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Generalnym Inspektorem Kontroli Skarbowej a tym podmiotem.

4. Podmiot występujący z wnioskiem, o którym mowa w ust. 2, informację o wystąpieniu z wnioskiem przekazuje niezwłocznie ministrowi właściwemu do spraw finansów publicznych. Minister właściwy do spraw finansów publicznych w każdej chwili może zażądać od Generalnego Inspektora Kontroli Skarbowej informacji o przyczynach uzasadniających wystąpienie z wnioskiem, a także o sposobie wykorzystania danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe.

5. Minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, w przypadku gdy uzna wystąpienie z wnioskiem, o którym mowa w ust. 2, za nieuzasadnione.

6. Udostępnienie wywiadowi skarbowemu danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia:

1) możliwość ustalenia pracownika wywiadu skarbowego uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane;
2) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych.

7. Udostępnianie wywiadowi skarbowemu danych, o których mowa w ust. 1, następuje na koszt podmiotu prowadzącego działalność telekomunikacyjną i operatora świadczącego usługi pocztowe.”;

2) w art. 36c ust. 10 otrzymuje brzmienie:

„10. Operator publicznej sieci telekomunikacyjnej, dostawca publicznie dostępnych usług telekomunikacyjnych oraz operator świadczący usługi pocztowe są obowiązani do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez wywiad skarbowy kontroli operacyjnej.”.

Art. 5. W ustawie z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.[7)]) wprowadza się następujące zmiany:

1) w art. 218 § 1 otrzymuje brzmienie:

„§ 1. Urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celne oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]), jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie.”;

2) art. 218b otrzymuje brzmienie:

„Art. 218b. Minister Sprawiedliwości w porozumieniu z ministrem właściwym do spraw łączności, Ministrem Obrony Narodowej oraz ministrem właściwym do spraw wewnętrznych określi, w drodze rozporządzenia, sposób technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia danych, o których mowa w art. 218 § 1, niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji, a także sposoby zabezpieczania danych informatycznych w urządzeniach zawierających te dane oraz w systemach i na informatycznych nośnikach danych, mając na uwadze konieczność zabezpieczenia tych danych przed ich utratą, zniekształceniem lub nieuprawnionym ujawnieniem.”.

Art. 6. W ustawie z dnia 16 marca 2001 r. o Biurze Ochrony Rządu (Dz. U. z 2004 r. Nr 163, poz. 1712, z późń. zm.[8)]) po art. 7 dodaje się art. 7a w brzmieniu:

„Art. 7a. 1. Szef BOR, w celu realizacji zadań BOR, określonych w art. 2 ust. 1, może zarządzić o zastosowaniu urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez BOR, z uwzględnieniem

---

[7)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 50, poz. 580, Nr 62, poz. 717, Nr 73, poz. 852 i Nr 93, poz. 1027, z 2001 r. Nr 98, poz. 1071 i Nr 106, poz. 1149, z 2002 r. Nr 74, poz. 676, z 2003 r. Nr 17, poz. 155, Nr 111, poz. 1061 i Nr 130, poz. 1188, z 2004 r. Nr 51, poz. 514, Nr 69, poz. 626, Nr 93, poz. 889, Nr 240, poz. 2405 i Nr 264, poz. 2641, z 2005 r. Nr 10, poz. 70, Nr 48, poz. 461, Nr 77, poz. 680, Nr 96, poz. 821, Nr 141, poz. 1181, Nr 143, poz. 1203, Nr 163, poz. 1363, Nr 169, poz. 1416 i Nr 178, poz. 1479, z 2006 r. Nr 15, poz. 118, Nr 66, poz. 467, Nr 95, poz. 659, Nr 104, poz. 708 i 711, Nr 141, poz. 1009 i 1013, Nr 167, poz. 1192 i Nr 226, poz. 1647 i 1648, z 2007 r. Nr 20, poz. 116, Nr 64, poz. 432, Nr 80, poz. 539, Nr 89, poz. 589, Nr 99, poz. 664, Nr 112, poz. 766 i Nr 123, poz. 849 oraz z 2008 r. Nr 100, poz. 648 i Nr 107, poz. 686.

[8)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 210, poz. 2135, z 2006 r. Nr 1054, poz. 708 i 711 oraz z 2008 r. Nr 66, poz. 402.

konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

2. O zastosowaniu urządzeń, o których mowa w ust. 1, Szef BOR niezwłocznie informuje Prezesa Urzędu Komunikacji Elektronicznej.”.

Art. 7. W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353, z późn. zm.[9)]) wprowadza się następujące zmiany:

1) w art. 30:

a) ust. 1 i 2 otrzymują brzmienie:

„1. W celu zapobiegania lub wykrywania przestępstw, w tym skarbowych, Żandarmeria Wojskowa, może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]), zwane dalej „danymi telekomunikacyjnymi”, oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną udostępnia nieodpłatnie dane telekomunikacyjne:

1) żołnierzowi Żandarmerii Wojskowej wskazanemu w pisemnym wniosku Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej albo osoby przez nich upoważnionej,
2) na ustne żądanie żołnierza Żandarmerii Wojskowej posiadającego pisemne upoważnienie osób, o których mowa w pkt 1,
3) za pośrednictwem sieci telekomunikacyjnej żołnierzowi Żandarmerii Wojskowej posiadającemu pisemne upoważnienie, osób o których mowa w pkt 1.”,

b) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Komendantem Głównym Żandarmerii Wojskowej a tym podmiotem.”,

---

[9)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 154, poz. 1800, z 2002 r. Nr 74, poz. 676 i Nr 89, poz. 804, z 2003 r. Nr 113, poz. 1070 i Nr 139, poz. 1326, z 2004 r. Nr 116, poz. 1203, Nr 171, poz. 1800 i Nr 273, poz. 2703, z 2006 r. Nr 104, poz. 711 oraz z 2007 r. Nr 176, poz. 1242.

c) uchyla się ust. 3,

d) ust. 4 otrzymuje brzmienie:

„4. Udostępnienie Żandarmerii Wojskowej danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:

1) wykorzystywane sieci i system teleinformatyczny zapewniają:
   a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
   b) zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostępu do danych,
2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Żandarmerii Wojskowej albo prowadzonych przez nie czynności.";

2) po art. 30 dodaje się art. 30a w brzmieniu:

„Art. 30a. 1. W celu realizacji zadań, o których mowa w art. 4 ust. 1 pkt 2-4, 5 i 8, Komendant Główny Żandarmerii Wojskowej lub – po uzyskaniu zgody Komendanta Głównego Żandarmerii Wojskowej – komendant oddziału Żandarmerii Wojskowej mogą zarządzić zastosowanie urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez Żandarmerię Wojskową, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

2. O zastosowaniu urządzeń, o których mowa w ust. 1, Komendant Główny Żandarmerii Wojskowej niezwłocznie informuje Prezesa Urzędu Komunikacji Elektronicznej.".

Art. 8. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. Nr 74, poz. 676, z późn. zm.[10)]) wprowadza się następujące zmiany:

1) po art. 26 dodaje się art. 26a w brzmieniu:

„Art. 26a. 1. W celu realizacji zadań, o których mowa w art. 5 ust. 1 pkt 1 i 2, Szef ABW może zarządzić o zastosowaniu przez ABW urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności

[10)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 90, poz. 844, Nr 113, poz. 1070, Nr 130, poz. 1188 i Nr 166, poz. 1609, z 2004 r. Nr 109, poz. 1159, Nr 171, poz. 1800, Nr 267, poz. 2647 i Nr 273, poz. 2703, z 2006 r. Nr 104, poz. 708 i 711 i Nr 218, poz. 1592 oraz z 2008 r. Nr 11, poz. 59.

przez ABW, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

2. O zastosowaniu urządzeń, o których mowa w ust. 1, Szef ABW niezwłocznie informuje Prezesa UKE.";

2) art. 28 otrzymuje brzmienie:

„Art. 28. 1. Obowiązek uzyskania zgody sądu, o której mowa w art. 27 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez ABW zadań, o których mowa w art. 5 ust. 1, w postaci danych:

1) o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]),
2) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

2. Podmiot wykonujący działalność telekomunikacyjną lub operator świadczący usługi pocztowe udostępnia nieodpłatnie dane, o których mowa w ust. 1, odpowiednio:

1) funkcjonariuszowi ABW wskazanemu w pisemnym wniosku Szefa ABW lub osoby upoważnionej przez ten organ,
2) na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW,
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi ABW posiadającemu upoważnienie, o którym mowa w pkt 2.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu wykonującego działalność telekomunikacyjną lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem ABW a tym podmiotem.

4. Udostępnienie ABW danych, o których mowa w ust. 1 pkt 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia:

1) możliwość ustalenia funkcjonariusza ABW uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
2) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do tych danych.";

Art. 9. W ustawie z dnia 28 lutego 2003 r. – Prawo upadłościowe i naprawcze (Dz. U. Nr 60, poz. 535, z późn. zm.[11)]) w art. 53 dodaje się ust. 6 w brzmieniu:

„6. Jeżeli upadły jest operatorem publicznej sieci telekomunikacyjnej lub dostawcą publicznie dostępnych usług telekomunikacyjnych w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]), o ogłoszeniu upadłości powiadamia się Prezesa Urzędu Komunikacji Elektronicznej. Powiadomienie następuje w dniu ogłoszenia upadłości i dokonuje się go przy zastosowaniu środków bezpośredniego przekazu informacji, takich jak telefon, faks, poczta elektroniczna.”.

Art. 10. W ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708, Nr 158, poz. 1122 i Nr 218, poz. 1592 oraz z 2008 r. Nr 171, poz. 1056) art. 18 otrzymuje brzmienie:

„Art. 18. 1. Obowiązek uzyskania zgody sądu, o której mowa w art. 17, nie dotyczy informacji niezbędnych do realizacji przez CBA zadań określonych w art. 2, w postaci danych:

1) o których mowa w art. 180c oraz 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]), zwanych dalej „danymi telekomunikacyjnymi”;
2) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

2. Podmiot wykonujący działalność telekomunikacyjną lub podmiot uprawniony do wykonywania działalności pocztowej udostępnia nieodpłatnie dane, o których mowa w ust. 1:

1) na pisemny wniosek Szefa CBA lub osoby przez niego upoważnionej;
2) na ustne żądanie funkcjonariusza CBA, posiadającego pisemne upoważnienie Szefa CBA lub osoby przez niego upoważnionej;
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi CBA posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem CBA a tym podmiotem.

[11)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 217, poz. 2125, z 2004 r. Nr 91, poz. 870 i 871, Nr 96, poz. 959, Nr 121, poz. 1264, Nr 146, poz. 1546, Nr 173, poz. 1808 i Nr 210, poz. 2135, z 2005 r. Nr 94, poz. 785, Nr 183, poz. 1538 i Nr 184, poz. 1539, z 2006 r. Nr 47, poz. 347, Nr 133, poz. 935 i Nr 157, poz. 1119, z 2007 r. Nr 123, poz. 85 i Nr 179, poz. 1279 oraz z 2008 r. Nr 96, poz. 606 i Nr 116, poz. 731.

4. Udostępnienie CBA danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:

1) sieć ta zapewnia:
   a) możliwość ustalenia funkcjonariusza CBA uzyskującego te dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
   b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do uzyskiwanych danych;
2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne CBA albo prowadzonych przez nie czynności.”.

Art. 11. W ustawie z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 i Nr 218, poz. 1592) wprowadza się następujące zmiany:

1) po art. 29 dodaje się art. 29a w brzmieniu:

„Art. 29a. 1. W celu realizacji zadań, o których mowa w art. 5 ust. 1 pkt 1 lit. a-c, f, g oraz art. 39 ust. 1, Szef SKW może zarządzić o zastosowaniu urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez SKW, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

2. W związku z wykonywaniem zadań, o których mowa w art. 6 ust. 1 w związku z ust. 3 i art. 39 ust. 1, Szef SWW może zarządzić o zastosowaniu przez SWW urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

3. O zastosowaniu urządzeń, o których mowa w ust. 1 i 2, Szef SKW niezwłocznie informuje Prezesa Urzędu Komunikacji Elektronicznej.”;

2) w art. 31 ust. 11 otrzymuje brzmienie:

„11. Operator publicznej sieci telekomunikacyjnej, dostawca publicznie dostępnych usług lub operator świadczący usługi pocztowe są obowiązani do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez SKW kontroli operacyjnej.”;

3) art. 32 otrzymuje brzmienie:

„Art. 32. 1. Obowiązek uzyskania zgody sądu, o której mowa w art. 31 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez SKW zadań określonych w art. 5 i 6, w postaci danych:

1) o których mowa w art. 180c oraz 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[3)]), zwanych dalej „danymi telekomunikacyjnymi”;
2) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

2. Udostępnienie przez przedsiębiorcę telekomunikacyjnego lub operatora świadczącego usługi pocztowe danych, o których mowa w ust. 1, następuje nieodpłatnie:

1) na pisemny wniosek Szefa SKW lub osoby przez niego upoważnionej;
2) na ustne żądanie funkcjonariusza SKW, posiadającego pisemne upoważnienie Szefa SKW;
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi SKW posiadającemu pisemne upoważnienie Szefa SKW.

3. O udostępnieniu danych w trybie określonym w ust. 2 pkt 2 przedsiębiorca telekomunikacyjny lub operator świadczący usługi pocztowe informuje Szefa SKW.

4. Przedsiębiorca telekomunikacyjny oraz operator świadczący usługi pocztowe są obowiązani udostępnić dane, o których mowa w ust. 1, funkcjonariuszom wskazanym we wniosku.

5. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacych odbywa się bez udziału pracowników podmiotu wykonującego działalność telekomunikacyjną lub przy niezbędnym ich współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem SKW a tym podmiotem.

6. Udostępnienie SKW danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:

1) wykorzystywane sieci i system teleinformatyczny zapewniają:
    a) możliwość ustalenia osoby uzyskującej te dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
    b) zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostęp do tych danych;
2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez SKW albo prowadzonych przez nią czynności.”.

Art. 12. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590) po art. 11 dodaje się art. 11a w brzmieniu:

„Art. 11a. Centrum informuje Komisję Europejską i państwa członkowskie Unii Europejskiej o środkach zastosowanych w sytuacji kryzysowej w celu zabezpieczenia prawidłowego działania publicznej sieci telekomunikacyjnej oraz stacji nadawczych i odbiorczych używanych do zapewnienia bezpieczeństwa, w zakresie dotyczącym systemu łączności i sieci teleinformatycznych.”.

Art. 13. 1. Do spraw wszczętych i niezakończonych przed dniem wejścia w życie ustawy stosuje się przepisy dotychczasowe, z zastrzeżeniem ust. 2.

2. Sprawy wszczęte na podstawie art. 179 ust. 6 i art. 222 ust. 2 ustawy, o której mowa w art. 1, niezakończone przed dniem wejścia w życie ustawy, umarza się.

Art. 14. 1. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 176 ust. 4 i art. 181 ustawy, o której mowa w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 176a ust. 5 i art. 179 ust. 12 tej ustawy w brzmieniu nadanym niniejszą ustawą.

2. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 218b ustawy, o której mowa w art. 5, zachowują moc do czasu wydania przepisów wykonawczych wydanych na podstawie art. 218b tej ustawy w brzmieniu nadanym niniejszą ustawą.

Art. 15. Prezes UKE powołany na podstawie ustawy, o której mowa w art. 1, pełni swoją funkcję do czasu powołania Prezesa UKE zgodnie z przepisami niniejszej ustawy.

Art. 16. Operator publicznej sieci telekomunikacyjnej i dostawca publicznie dostępnych usług telekomunikacyjnych przechowują dane, o których mowa w art. 165 ust. 1 i art. 166 ust. 5 ustawy, o której mowa w art. 1, w zakresie danych związanych z dostępem do sieci Internet, telefonii internetowej i poczty elektronicznej, na zasadach dotychczasowych.

Art. 17. Bazy danych, o których mowa w art. 71 ust. 4 oraz w art. 180f ust. 2 ustawy, o której mowa w art. 1, tworzy się nie później niż po upływie 24 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 18. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia, z wyjątkiem art. 180a ust. 3, który wchodzi w życie z dniem 1 stycznia 2010 r.

27/10/BS

UZASADNIENIE

Niemal czteroletni okres obowiązywania ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne wskazał na potrzebę usprawnienia niektórych mechanizmów i instytucji, w tym pełniejsze dostosowanie przepisów ustawy do prawa Unii Europejskiej – obowiązek implementacji nowej 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, zmieniającej dyrektywę 2002/58/WE.

Wśród przepisów projektu należy wymienić również propozycje zmian innych ustaw w zakresie realizacji przez przedsiębiorców telekomunikacyjnych obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Uzasadnienie szczegółowe

Art. 2 pkt 48 – zmiana definicji usługi telekomunikacyjnej

Zmiana w definicji usługi telekomunikacyjnej ma na celu objęcie regulacjami telekomunikacyjnymi tych aspektów poczty elektronicznej, które polegają na przekazywaniu sygnałów w sieci telekomunikacyjnej. W tym celu wykreślono zapis, iż usługa poczty elektronicznej nie stanowi usługi telekomunikacyjnej. Jest to zgodne z dyrektywami 2002/58/WE i 2002/21/WE, a także pozwoli na wyeliminowanie wątpliwości interpretacyjnych co do pojęcia poczty elektronicznej.

Istniejący dotychczas przepis mógł budzić wątpliwości interpretacyjne co do zakresu pojęcia przekazywania poczty elektronicznej i usługi poczty elektronicznej. Tymczasem nie są to pojęcia tożsame, co wynika jednoznacznie z dyrektyw.

Dyrektywa 2002/58/WE nie definiuje wprost usługi poczty elektronicznej, definiuje jedynie pocztę elektroniczną, jako wszelkiego rodzaju wiadomości tekstowe, głosowe, dźwiękowe lub wizualne przesyłane przez publiczną sieć telekomunikacyjną, które mogą być przechowywane w sieci lub w urządzeniu końcowym odbiorcy, dopóki nie zostaną przez niego odebrane. Poczta elektroniczna jest jednym z rodzajów przekazu, który podlega ochronie zgodnie z przepisami omawianej dyrektywy.

Z kolei pojęcie usługi przekazywania poczty elektronicznej jest wyraźnie objęte dyrektywą ramową, co statuuje pkt 10 motywów tej dyrektywy. Powyższe potwierdza również art. 2c tej dyrektywy w definicji usługi łączności elektronicznej, tj. usługi polegającej całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej, w zakres której wchodzą usługi telekomunikacyjne i usługi transmisyjne świadczone przez sieci nadawcze. Definicja ta jest tożsama z definicją usługi telekomunikacyjnej w polskim Prawie telekomunikacyjnym. Obie te definicje obejmują swoim zakresem usługę przekazywania poczty elektronicznej.

Sama usługa poczty elektronicznej nie jest usługą telekomunikacyjną, gdyż jej zasadniczymi elementami są: udostępnienie indywidualnego konta pocztowego, zapewnienie możliwości odbierania poczty elektronicznej kierowanej na konto pocztowe, zapewnienie możliwości

wysyłania poczty elektronicznej z konta pocztowego, zapewnienie możliwości przechowywania poczty elektronicznej. W związku z powyższym należy uznać, iż usługa ta jest usługą społeczeństwa informacyjnego, wyłączoną mocą art. 2c dyrektywy ramowej z zakresu usług łączności elektronicznej.

Jedynie drugie z powyższych pojęć, czyli pojęcie „usługa przekazywania poczty elektronicznej", jest usługą telekomunikacyjną i zmieniona nowelizacją treść przepisu art. 2 ust. 48 jest skutkiem przyjętej powyżej interpretacji definicji związanych z pocztą elektroniczną.

Art. 6

Wprowadzenie tej zmiany spowodowane jest koniecznością zbierania informacji niezbędnych do prowadzenia analiz rynku telekomunikacyjnego, prowadzenia statystyk oraz przekazywania danych organom regulacyjnym innych państw członkowskich Unii Europejskiej i Komisji Europejskiej. Dodatkowo Prezes UKE będzie miał prawo żądania tych informacji w terminie nie krótszym niż 7 dni i w określonym zakresie, uzasadnionym celem żądania. Zgodnie z projektowanym brzmieniem ust. 3 żądanie powinno być proporcjonalne do celu, jakiemu ma służyć. Zbieranie informacji nie dotyczy osób fizycznych oraz podmiotów, o których mowa w art. 4.

Art. 8 i art. 161 ust. 2 pkt 6

Rozszerzono zakres obowiązku zapewnienia dostępu do informacji w związku z zobowiązaniami międzynarodowymi Rzeczypospolitej Polskiej wobec krajów EFTA.

W ust. 2 art. 8 uregulowany został obowiązek informowania o przekazaniu Komisji Europejskiej i organom regulacyjnym innych państw członkowskich informacji, otrzymanych od przedsiębiorcy telekomunikacyjnego. Przepis ten wynika z brzmienia art. 5 ust. 2 dyrektywy ramowej, zgodnie z którym (...) Jeżeli dostarczona informacja odnosi się do informacji dostarczonej uprzednio przez przedsiębiorstwo na wniosek krajowego organu regulacyjnego, przedsiębiorstwa takie winne zostać o tym poinformowane. (...). Regulacja art. 8 ust. 2 tym różni się od przepisów art. 6, iż dotyczy sytuacji, kiedy Prezes UKE posiada już informacje od przedsiębiorcy (uzyskał je wcześniej, dla innych celów niż przekazanie Komisji Europejskiej) i przekazuje te informacje KE lub organom regulacyjnym innych państw członkowskich, a następnie informuje o tym przedsiębiorcę. Art. 6 dotyczy zaś sytuacji, kiedy Prezes UKE nie posiada określonych informacji i zwraca się z żądaniem informacji, wskazując przy tym cel, jakim może być np. konieczność przekazania informacji KE lub organom państw członkowskich.

Art. 10

Zmiana art. 10 ust. 1 ma na celu umożliwienie wpisania do rejestru, w związku z art. 49 TWE, przedsiębiorcy telekomunikacyjnego nieposiadającego siedziby na terytorium Rzeczypospolitej Polskiej, jeżeli zamierza świadczyć na terytorium Rzeczypospolitej Polskiej usługi.

Zmiana art. 10 ust. 4 pkt 4 spowodowana jest zmianą ust. 1 oraz tym, że obowiązek przedstawienia numeru rejestracji powinien mieć zastosowanie jedynie wobec tych podmiotów, które numer taki posiadają, nie powinien zaś stanowić bariery dla podmiotów, które działają w państwie pochodzenia bez konieczności rejestracji. Również takie podmioty

powinny mieć bowiem możliwość uzyskania wpisu do polskiego rejestru przedsiębiorców telekomunikacyjnych.

Art. 15

Zaproponowana zmiana jest związana ze zmianą art. 21 – 25c określających postępowanie w sprawie określania rynków właściwych, nakładanie, zmiana i znoszenie obowiązków regulacyjnych.

Zmiana służy stworzeniu w ustawie jednoznacznych, w odniesieniu do procedury konsultowania, rozstrzygnięć Prezesa UKE z zainteresowanymi podmiotami.

Art. 21 – 25c

Zmiany w art. 21 – 25c są związane z zarzutami Komisji Europejskiej, która wielokrotnie podnosiła brak możliwości skutecznego odwołania się od rozstrzygnięcia w przedmiocie wyznaczenia, zdefiniowania rynku właściwego, gdyż rozporządzenie ministra właściwego do spraw łączności w sprawie określenia rynków właściwych jako akt powszechnie obowiązujący nie daje możliwości zakwestionowania rozstrzygnięć przez przedsiębiorców telekomunikacyjnych w normalnym trybie odwoławczym.

Proces analizy rynków rozpoczyna się od ich określenia przez regulatora (zdefiniowania) przez analizę danych, którymi UKE dysponuje, aż po stwierdzenie, czy występuje na nich skuteczna konkurencja czy też nie występuje, a co za tym idzie wyznaczenie przedsiębiorcy zajmującego znaczącą pozycję i nałożenie obowiązków regulacyjnych.

Wprowadzone zmiany mają umożliwić Prezesowi UKE wyznaczanie rynków właściwych zgodnie z Zaleceniem Komisji. Prezes UKE będzie wydawał decyzje, w których w pierwszej kolejności określi rynek właściwy, dokona analizy tego rynku pod kątem występujących na nim problemów, a następnie wyznaczy przedsiębiorcę lub przedsiębiorców o znaczącej pozycji (co oznacza, że rynek nie jest skutecznie konkurencyjny) i nałoży obowiązki regulacyjne. W ten sposób strony postępowania będą miały możliwość zaskarżenia decyzji także w części dotyczącej wyznaczenia rynku właściwego.

W przypadku ustalenia, że na danym rynku właściwym istnieje konkurencja, tzn. nie występuje przedsiębiorca o znaczącej pozycji rynkowej, Prezes UKE wydaje rozstrzygnięcie w formie postanowienia, na które podmiotom zainteresowanym przysługuje tryb odwoławczy – zażalenie.

Należy tu podkreślić, iż w ten sposób ujęta zostanie dodatkowa regulacja – dotychczas nieokreślona w ustawie – Prawo telekomunikacyjne – określająca konsekwencje stwierdzenia, że operator utracił pozycję rynkową. W decyzji o zniesieniu obowiązków Prezes UKE oznacza termin ich uchylenia w taki sposób, aby uchylenie uwzględniało sytuację przedsiębiorców działających na rynku objętych tą decyzją.

Zainteresowane strony zostaną zawiadomione przez Prezesa UKE o podjętym przez niego rozstrzygnięciu również na stronie Biuletynu Informacji Publicznej UKE.

Zgodnie z przepisem art. 15(3) zdanie ostatnie dyrektywy ramowej: Krajowe organy regulacyjne będą postępować zgodnie z procedurami, o których mowa w art. 6 i 7

(konsultacje i konsolidacje), zanim zdefiniują rynki różne od tych, które zostały zdefiniowane w zaleceniach. Regulacje te pozwalają na konsolidowanie projektów rozstrzygnięcia, które definiuje rynek inny niż wskazany w zaleceniach i jednocześnie wyznacza SMP i nakłada obowiązki.

Proponowane rozwiązanie usprawni również proces określania rynków właściwych.

Art. 34 ust. 2 pkt 12

Zmiana ma charakter porządkowy w związku ze zmianą przepisów działu VIII.

Art. 56

Wprowadzone zmiany w art. 56 ustawy służą wyeliminowaniu dotychczasowych powtórzeń w zakresie informacji i danych, które powinny być określone w umowie i w regulaminie, przy jednoczesnym spełnieniu wymogów określonych w art. 20 dyrektywy o usłudze powszechnej oraz Załączniku II dyrektywy.

Dodatkowo wyraźnie wskazano, które z obligatoryjnych elementów umowy mogą zostać określone w regulaminie przez dostawcę publicznie dostępnych usług telekomunikacyjnych.

Art. 57 ust. 4 i 6

Proponowany przepis zwiększa ochronę konsumentów, gdyż wysokość kary w przypadku zawarcia umowy o świadczenie usług telekomunikacyjnych, w tym o zapewnienie przyłączenia do sieci, związanego z ulgą przyznaną abonentowi, stanowi równowartość przyznanej ulgi na dzień rozwiązania umowy, a nie jak dotychczas na dzień jej podpisania.

W przypadku jednostronnego rozwiązania umowy przez abonenta lub przez dostawcę usług z winy abonenta przed upływem terminu ustalonego w umowie abonent powinien zwrócić ulgę przyznaną mu przy podpisywaniu umowy. Dotychczas abonent zwracał ulgę w pełnej wysokości, bez względu na to, czy rozwiązanie umowy miało miejsce zaraz po podpisaniu umowy czy tuż przed jej rozwiązaniem. Aktualne rozwiązanie określa, że wysokość zwracanej przez abonenta ulgi nie może przekroczyć wartości ulgi pomniejszonej o proporcjonalną jej wartość za okres od dnia zawarcia umowy do dnia jej rozwiązania. Przedmiotowa zmiana jest prokonsumencka.

Art. 59 ust. 2

Przepis dotyczący przypadków zmiany regulaminu przez dostawcę usług telekomunikacyjnych został przeniesiony do nowo projektowanego art. 60a, z uwagi na fakt, iż reguluje szczególną sytuację zmian warunków umownych. W związku z powyższym oraz koniecznością prawidłowej implementacji art. 20 ust. 4 dyrektywy o usłudze powszechnej, przepis został odpowiednio zmodyfikowany oraz wydzielony w ramach nowej jednostki redakcyjnej art. 60a.

Z uwagi na fakt, iż ust. 1 określa zawartość regulaminu i definiuje obowiązek jego dostarczania przez dostawcę usług abonentom, nowo projektowany ust. 2 statuuje, iż dostawca usług ma takie same obowiązki wobec użytkowników usług przedpłaconych, którzy w świetle definicji ustawowych abonentami nie są.

W konsekwencji przepis ust. 1 znajdzie również zastosowanie w relacjach z użytkownikami usług przedpłaconych, którzy zawierają umowę o świadczenie usług w drodze kupna tzw. „startera".

Art. 60

Dotychczasowa treść art. 60 wprowadzająca niezamknięty katalog informacji, jakie powinny znaleźć się w regulaminie świadczenia usług telekomunikacyjnych, pozostawała w niespójności z treścią art. 56 i powodowała nieuzasadnioną konieczność powtarzania tych samych informacji zarówno w umowie, jak i w regulaminie świadczenia usług. Z tego względu wyraźnie wskazano, iż art. 60 dotyczy regulaminu świadczenia usług przedpłaconych, których odbiorcami są użytkownicy nieposiadający umowy pisemnej.

Art. 60a

Projektowana zmiana jest konsekwencją uchylenia art. 59 ust. 2.

Pierwsza zmiana polega na określeniu zakresu informacji, do podania których dostawca usług jest zobowiązany w przypadku zamiaru dokonania zmian warunków umownych. Z uwagi na fakt, iż dotychczas dostawca usług miał obowiązek informowania wyłącznie o zmianach w regulaminie bez podawania ich treści, w wyniku zmiany dostawca usług będzie zobowiązany do podawania ich treści, a abonenci lub użytkownicy nie będą zmuszeni do samodzielnego ustalania dokonanych przez dostawcę zmian.

Kolejna zmiana dotyczy dookreślenia obowiązków informacyjnych dostawcy usług w przypadku zmiany warunków umownych z uwagi na fakt, iż warunki te mogą zostać zawarte w umowie lub stosowanych przez dostawcę regulaminach.

Dodatkowo ust. 1 lit. c określa obowiązek dostawcy usług przedpłaconych do informowania swoich użytkowników o zmianach w regulaminie przez podanie go do publicznej wiadomości.

Ponadto, z uwagi na zidentyfikowanie przez KE nieprawidłowej implementacji ww. przepisu dyrektywy oraz niezgodne z intencją ustawodawcy stosowanie przepisów przez urząd regulacyjny, wyraźnie wskazano, iż abonent nie nabywa określonego w ust. 2 uprawnienia do odstąpienia od umowy, w przypadku gdy dostawca usług dokonuje zmian warunków umownych z przyczyn od siebie niezależnych na skutek zmiany przepisów prawa (ust. 3). W tym samym celu w ust. 1 zastosowano termin „proponowana zmiana", wskazując, iż w zakresie ust. 1 intencja wprowadzenia zmian leży wyłącznie po stronie dostawcy usług, nie wynika zaś z konieczności dostosowania określonych warunków umownych w związku z faktem zmiany przepisów prawa (sytuacji określonej w ust. 3).

Biorąc również pod uwagę wątpliwości interpretacyjne dotyczące dwóch analogicznych sytuacji, w wyniku zaistnienia których abonent nabywa określone uprawnienia, tj. sytuacji podwyższenia przez dostawcę cen usług (art. 61 ust. 6) oraz sytuacji zmiany warunków umownych określonej w niniejszej jednostce redakcyjnej, doprecyzowano, iż w przypadku braku akceptacji przez abonenta proponowanych zmian, które w ocenie abonenta są dla niego niekorzystne, dostawcy usług, oprócz roszczenia odszkodowawczego, nie będzie również przysługiwał zwrot ulgi, o której mowa w art. 57 ust. 6.

Art. 61

Przepis ma na celu zapewnienie jednolitych reguł i zasad dokonywania zmian w cennikach świadczenia usług telekomunikacyjnych, analogicznie jak ma to miejsce w przypadku zmiany warunków umownych. Wyraźnie wskazano również, iż uprawnienie do wypowiedzenia umowy bez obowiązku zapłaty kary umownej w związku ze zmianą cennika przez dostawcę usług abonent nabywa wyłącznie w przypadku podwyższenia cen usług. Ponadto,

analogicznie do zmian w art. 60, czyli przypadków zmiany regulaminu lub warunków umownych, wprowadzono wyjątek od powyższej zasady, w myśl którego wspomniane uprawnienie abonentowi nie przysługuje, jeśli konieczność podwyższenia cen wynika ze zmiany przepisów prawa.

Art. 71

W celu sprawnej realizacji przedsięwzięć związanych z obsługą numerów przeniesionych proponuje się, aby Prezes UKE prowadził centralną bazę numerów przeniesionych. Obowiązkiem operatorów publicznych sieci telefonicznych byłoby połączenie swojej sieci bezpośrednio lub za pomocą sieci innego operatora z tą bazą w celu jej aktualizacji.

Art. 153 ust. 4

Zmiany w art. 153 ust. 4 pkt 5 i 6 wynikają z rozporządzenia (WE) nr 552/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. (Dz. Urz. WE L 096 z 31.03.2004, str. 26), na podstawie którego urządzenia zarządzania ruchem lotniczym podlegają ocenie zgodności z zasadniczymi wymaganiami określonymi na podstawie tego rozporządzenia.

Zmiana pkt 7 jest konsekwencją zmian wprowadzonych ustawą z dnia 17 listopada 2006 r. o systemie oceny zgodności wyrobów przeznaczonych na potrzeby obronności i bezpieczeństwa państwa. Ustawa ta wprowadza do ustawy – Prawo telekomunikacyjne art. 152a, zgodnie z którym do wymagań aparatury, w tym telekomunikacyjnych urządzeń końcowych i urządzeń radiowych przeznaczonych na powyższe cele, stosuje się przepisy ww. ustawy. Telekomunikacyjne urządzenia końcowe i urządzenia radiowe nieprzeznaczone na potrzeby obronności i bezpieczeństwa państwa powinny spełniać zasadnicze wymagania i podlegać obowiązkowej ocenie zgodności z nimi. Wyjątkiem są urządzenia wymienione w ust. 4 pkt 1 – 5, zwolnione z takich wymagań przepisami unijnymi.

Art. 159 ust. 1 pkt 5

Zmianę w art. 159 ust. 1 pkt 5 ustawy – Prawo telekomunikacyjne wynika z implementacji do krajowego porządku prawnego 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 zmieniającej dyrektywę 2002/58/WE (Dz. Urz. UE L 105 z 13.04.2006, str. 54). Polska ma obowiązek jej implementacji do przepisów krajowych w terminie 18 (telefonia) i 36 miesięcy (usługi internetowe). W tym przypadku proponowana zmiana ma za zadanie zastąpienie niejasnego pojęcia „próba uzyskania połączenia", określonym w przepisach dyrektywy pojęciem „nieudanej próby połączenia". Pojęcie to jest zdecydowanie bardziej jednoznaczne, a jego wprowadzenie do ustawy niezbędne w związku z procesem transpozycji przepisów dyrektywy do regulacji krajowych.

Art. 161

Zmiana art. 161 ust. 2 pkt 6 polega na rozszerzeniu kręgu osób o obywateli Konfederacji Szwajcarskiej, a związana jest z koniecznością wdrożenia decyzji Rady nr 2006/245/WE.

Art. 165 i 166

Uchylenie art. 165 ust. 1 oraz art. 166 ust. 5 ustawy – Prawo telekomunikacyjne jest konsekwencją wprowadzenia przepisów art. 180a wprost związanych z implementacją dyrektywy 2006/24/WE. W istocie przepisy art. 180a zastępują uchylone przepisy w sposób zgodny z przepisami dyrektywy.

Art. 169

Doprecyzowano, iż dane osobowe udostępniane są ograniczone do danych posiadanych przez przedsiębiorcę telekomunikacyjnego.

Art. 171

Zmiany wprowadzone w art. 171 mają charakter zmian porządkujących w związku ze zmianą przepisów działu VIII ustawy. Wynikają również z konieczności dostosowania tego przepisu do przepisów dyrektywy o prywatności i łączności elektronicznej, w szczególności w zakresie używanej terminologii. W art. 171 ust. 8 i 10 wprowadzono pojęcie „przedsiębiorca telekomunikacyjny". Określone obowiązki powinny ciążyć na wszystkich przedsiębiorcach telekomunikacyjnych, a nie tylko na operatorach sieci czy też na dostawcach publicznie dostępnych usług telekomunikacyjnych. Ponadto w ust. 10 wprowadzono przepis, iż do udostępniania danych ust. 9, stosuje się art. 180d.

Art. 176 – 182

Obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego

Zmiany proponowane w art. 176 – 182 ustawy – Prawo telekomunikacyjne są zmianami, których wprowadzenie ma za zadanie dopasowanie siatki pojęciowej stosowanej w ustawie – Prawo telekomunikacyjne i w ustawach kompetencyjnych precyzujących zadania organów państwowych posiadających uprawnienia do prowadzenia działań operacyjnych z wykorzystaniem telekomunikacji, a także w innych przepisach ustawowych dotyczących sytuacji szczególnych zagrożeń i powinności przedsiębiorców związanych z wykonywaniem obowiązków związanych z obronnością państwa. Wprowadzone zmiany mają za zadanie wyraźne odróżnienie, przez wydzielenie odrębnych tematycznie jednostek redakcyjnych ustawy, obowiązków związanych z działaniami przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń, wprowadzania dodatkowych ograniczeń i obowiązków w funkcjonowaniu sieci telekomunikacyjnych i świadczeniu usług oraz utrzymywaniu i odtwarzaniu zdolności usługowych przedsiębiorców na zasadach preferencyjnych, współpracy z uprawnionymi organami państwowymi prowadzącymi działania operacyjne oraz obowiązków w zakresie zachowywania danych związanych z połączeniami telekomunikacyjnymi, obligatoryjnie zatrzymywanych przez przedsiębiorcę na potrzeby ścigania sprawców przestępstw i prowadzenia w tym względzie postępowań sądowych. Dotychczasowy kształt przepisów działu VIII powodował powstawanie trudności interpretacyjnych, w szczególności dotyczących zakresu zobowiązań oraz organów państwowych, na rzecz których realizowane były obowiązki związane z obronnością, bezpieczeństwem państwa oraz bezpieczeństwem i porządkiem publicznym. Proponowane zmiany mają na celu uniknięcie wymienionych wyżej problemów interpretacyjnych.

Przepisy znowelizowanego działu VIII ustawy określają warunki dostępu i utrwalania oraz rodzaje danych podlegających retencji, których jednoznaczne i szczegółowe określenie nastąpi w drodze rozporządzenia. Przepisy te określają jako podstawowy sposób realizacji obowiązków w zakresie zapewnienia warunków dostępu i utrwalania z zachowaniem wymagań określonych w rozporządzeniu, o którym mowa w art. 179 ust. 12.

Ponadto przewidziano fakultatywną możliwość zapewnienia warunków dostępu i utrwalania za pomocą interfejsów na zasadach określonych w umowach zawartych przez uprawnione podmioty z przedsiębiorcą telekomunikacyjnym. Umowa może określać współudział stron w kosztach zastosowania interfejsów. Proponowane przepisy nie zawierają rozwiązań szczegółowych, w zakresie ochrony danych, wykraczających poza ochronę tajemnicy telekomunikacyjnej, gdyż wymogi szczegółowe w zakresie niezbędnym do zastosowania przy wykonywaniu obowiązków określonych w dziale VIII, a w szczególności w art. 179 i 180a zależą od przyjętego sposobu realizacji ww. zadań i są określone przepisami odrębnymi, w tym w szczególności przepisami ustawy o ochronie informacji niejawnych i ustawy o ochronie danych osobowych. Przepisy tych ustaw mają zastosowanie niezależnie od minimalnego standardu zabezpieczenia danych telekomunikacyjnych, określonego w dziale VII ustawy.

Art. 176 otrzymał brzmienie, które w swojej treści zawiera obecnie obowiązujący art. 179 ust. 1.

Dodany został nowy artykuł art. 176a, który wprowadza definicję sytuacji szczególnych zagrożeń, której wprowadzenie postulowało środowisko przedsiębiorców telekomunikacyjnych. Zaproponowana definicja jest oparta na siatce pojęciowej zaczerpniętej z ustawy o zarządzaniu kryzysowym oraz z ustaw o stanach nadzwyczajnych i uwzględnia również sytuacje związane z awariami technicznymi i uszkodzeniami infrastruktury telekomunikacyjnej przedsiębiorcy. W ust. 2 ograniczono zakres zawartości planów wykluczając z niego obszary tematyczne określone w poprzednich przepisach w art. 176 ust. 2 pkt 4 oraz częściowo art. 176 ust. 2 pkt 7 (priorytety). W znowelizowanych przepisach ujęto, poza aspektami związanymi ze świadczeniem usług telekomunikacyjnych, także problematykę dostarczania sieci z uwzględnieniem pierwszeństwa dla podmiotów koordynujących, podmiotów zarządzania kryzysowego, służb ustawowo powołanych do niesienia pomocy, podmiotów realizujących zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, bardzo istotną, a niestety pominiętą w przepisach dotychczasowych.

W art. 176a ust. 3 wskazano organy, z którymi przedsiębiorca telekomunikacyjny uzgadnia zawartość planu działań w sytuacjach szczególnych zagrożeń.

Nowy przepis art. 176a ust. 4 określa, w którym momencie przedsiębiorca praktycznie podejmuje działania określone w planie i od jakich organów uzyskuje ewentualną informację o wystąpieniu sytuacji szczególnych zagrożeń. Wprowadzenie przepisu było postulowane przez środowisko przedsiębiorców.

W art. 176a ust. 5 rozszerzono delegację do wydania rozporządzenia o określenie organów dokonujących uzgodnień planów przedsiębiorców. Zmieniono także delegację w zakresie określenia przedsiębiorców i rodzajów działalności telekomunikacyjnej niepodlegających obowiązkowi sporządzenia planu. Uchylenie art. 177 ust. 1 i 2 spowodowane jest małą czytelnością i brakiem jednoznaczności przepisów dotychczasowych, rezygnacją z wprowadzania do przepisów ustawowych obowiązków z zakresu świadczenia usług o określonych priorytetach, spowodowaną brakiem technicznej standaryzacji w tym zakresie

oraz praktycznym brakiem możliwości wydania rozporządzenia, delegacja do wydania którego znajdowała się w art. 177 ust. 2. Najistotniejszy przepis dotychczasowego art. 177 ust. 1 znajduje swoje odzwierciedlenie w nowym art. 176a ust. 5, w którym łącznie z przepisem art. 176a ust. 2 pkt 3 określa, jakie podmioty i służby oraz w jaki sposób wskazane, będą podmiotami i służbami, dla których realizowane jest świadczenie usług i dostarczania sieci, a także utrzymania ciągłości i ich odtwarzanie, z uwzględnieniem pierwszeństwa.

W art. 177 dokonano zmian redakcyjnych w związku z uchyleniem ust. 1 i 2.

W art. 177 ust. 6 została zawarta delegacja do wydania rozporządzenia przez Radę Ministrów, które ureguluje tryb nieodpłatnego udostępniania w sytuacji szczególnego zagrożenia przedsiębiorcom telekomunikacyjnym oraz podmiotom i służbom wykonującym zadania w zakresie ratownictwa, niesienia pomocy ludności, zarządzania kryzysowego, a także zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, urządzeń nadawczych lub nadawczo-odbiorczych przez podmioty niebędące przedsiębiorcami telekomunikacyjnymi.

Zmiana art. 178 ust. 1 pkt 1 jest konsekwencją zmian w art. 176 i 177.

Nowe brzmienie art. 178 ust. 2 jest podyktowane tym, że w przepisach dotychczasowych określono zbyt wąski i zamknięty katalog podmiotów mogących występować z wnioskiem do Prezesa UKE o wydanie decyzji określonych w art. 178 ust. 1. W sytuacjach szczególnych zagrożeń podmiotami takimi mogą być także podmioty koordynujące działania ratownicze, podmioty właściwe w sprawach zarządzania kryzysowego oraz służby ustawowo powołane do niesienia pomocy.

W art. 178 ust. 2 został zaprojektowany nowy przepis, który umożliwia ogłoszenie decyzji Prezesa UKE w formie ustnej oraz odstąpienie od uzasadnienia decyzji. Stosownie do art. 14 § 2 K.p.a. sprawy mogą być załatwiane ustnie, gdy przemawia za tym interes strony, a przepis prawa nie stoi temu na przeszkodzie – zdaniem autorów komentarzy do K.p.a. wyrażenie: „gdy przemawia za tym interes strony" należałoby uważać za równoznaczne pod względem swojego sensu z wyrażeniem: „gdy strona na to się zgadza". Treść „oświadczenia" strony co do zgody musi mieć charakter wyraźny. Wyrażenia zgody nie można domniemywać. W sytuacji istnienia jakichkolwiek wątpliwości a zwłaszcza, gdy w ocenie organu za ustnym załatwieniem sprawy przemawia interes strony, organ jest obowiązany zwrócić się do strony o jej stanowisko. Brak zgody nakłada na organ administracji publicznej obowiązek zastosowania formy pisemnej. W przypadku ustnego załatwienia sprawy treść oraz istotne motywy takiego załatwienia powinny być utrwalone w aktach w formie protokołu lub podpisanej przez stronę adnotacji. W uchwale sędziów NSA z dnia 13 października 1997 r. (FPK 13/97, ONSA 1998, nr 1, poz. 70) stwierdzono, że „ogłoszenie ustne decyzji administracyjnej, jako wyjątek od zasady pisemności, wymaga utrwalenia tej czynności na piśmie w drodze sporządzenia protokołu (art. 67 § 2 pkt 5 K.p.a.), który powinien odpowiadać wymaganiom art. 68 i 107 K.p.a. w zakresie koniecznych elementów decyzji". Składniki decyzji administracyjnej określa art. 107 § 1 K.p.a. Wobec braku wyraźnego postanowienia w tej kwestii należy przyjąć, że powyższy przepis ma zastosowanie do decyzji pisemnych i decyzji ogłoszonych ustnie, z tym że w odniesieniu do decyzji ustnych niektóre wymagania określone w art. 107 § 1 z natury rzeczy nie będą mogły być spełnione, np. podpis osoby upoważnionej do wydania decyzji. Art. 107 § 1 K.p.a. do niezbędnych elementów decyzji zalicza uzasadnienie faktyczne i prawne. Od uzasadnienia decyzji można odstąpić w dwóch przypadkach – gdy decyzja uwzględnia w całości żądanie strony (nie dotyczy to jednak decyzji rozstrzygających sporne interesy stron oraz decyzji wydanych na skutek

odwołania) oraz gdy z dotychczasowych przepisów ustawowych wynikała możliwość zaniechania lub ograniczenia uzasadnienia ze względu na interes bezpieczeństwa państwa lub porządek publiczny. Niestety w przypadku decyzji wydawanych przez Prezesa UKE na podstawie art. 178 ustawy – Prawo telekomunikacyjne nie ma możliwości rezygnacji z uzasadnienia. Aby takie rozwiązanie było możliwe został wprowadzony do projektu przepis zezwalający na odstąpienie od uzasadnienia. W projektowanym art. 178 ust. 2 dopuszczono odstąpienie od uzasadnienia decyzji w całości lub w części, jeżeli wymagają tego względy obronności lub bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

W art. 178 ust. 3 zawarto zamknięty katalog organów, które mogą dysponować urządzeniami, których zastosowanie ma na celu uniemożliwienie na określonym obszarze telekomunikacji z zastrzeżeniem, że przypadki i zasady ich użycia zostaną określone w przepisach odrębnych.

W ustawach kompetencyjnych uprawnionych podmiotów zostały zawarte przepisy materialne sankcjonujące używanie urządzeń uniemożliwiających telekomunikację, przypadki i zasady ich zastosowania, a także obowiązek poinformowania o ich użyciu Prezesa Urzędu Komunikacji Elektronicznej.

Jednocześnie przepis dotychczasowy mówiący jedynie o uniemożliwieniu połączeń telefonicznych nie był możliwy do wykonania z powodów technicznych.

Uchylenie ust. 1 w art. 179 jest związane z przebudową całego rozdziału VIII. Uchylenie ust. 1 jest podyktowane zbędnością tego przepisu. Przepis ten w istocie wskazywał jedynie na obowiązek wykonywania zadań w zakresie obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, określonych w ustawie i przepisach odrębnych.

Przepis art. 179 ust. 1 został przeniesiony z niewielkimi zmianami do oddzielnej jednostki redakcyjnej, tj. art. 176.

Zmiany wprowadzone w art. 179 ust. 3 mają na celu ujednolicenie siatki pojęciowej stosowanej w ustawie – Prawo telekomunikacyjne i w ustawach kompetencyjnych precyzujących zadania organów państwowych posiadających uprawnienia do prowadzenia kontroli operacyjnej w telekomunikacji. W tym względzie wprowadzono w ust. 3 pojęcie „warunków dostępu i utrwalania" oraz „przekazów telekomunikacyjnych", zdefiniowane na podstawie pojęć użytych w ustawach kompetencyjnych. Dodatkowo dokonano zmiany przez ukierunkowanie wskazania przez uprawnione podmioty „użytkownika końcowego" w miejsce występującego w poprzedniej redakcji art. 179 ust. 3 wskazania „treści i danych", co było organizacyjnie i technicznie niemożliwe. W związku z niejasnością, którą powodowało poprzednie określenie podmiotów uprawnionych, szczególnie w kontekście jednoczesnego i wzajemnie niezależnego dostępu, przyjęto rozwiązanie definiujące jako „uprawnione podmioty" Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i wywiad skarbowy. Dodano również wyrazy „urządzenia końcowego", które mają na celu ujednolicenie i doprecyzowanie zasad współpracy uprawnionych podmiotów z przedsiębiorcami telekomunikacyjnymi, które wynikają zarówno z przepisów ustawy – Prawo telekomunikacyjne, jak i ustaw kompetencyjnych uprawnionych podmiotów.

Nowy art. 179 ust. 3a zastępuje uchylony art. 179 ust. 5.

Został wprowadzony nowy art. 179 ust. 3b, który ze względów legislacyjnych został wyodrębniony z art. 179 ust. 3.

W art. 179 ust. 4 wprowadzono jako podstawowy sposób realizacji obowiązków przez przedsiębiorcę telekomunikacyjnego przez zapewnienie warunków dostępu i utrwalania z zachowaniem wymagań określonych w rozporządzeniu, o którym mowa w art. 179 ust. 12.

W art. 179 ust. 4a wprowadzono jako fakultatywny sposób realizacji przedmiotowych obowiązków – sposób oparty na interfejsach przygotowywanych przez przedsiębiorcę – zlokalizowanych w miejscach obejmowanych przez sieć przedsiębiorcy telekomunikacyjnego i wskazanych przez uprawnione podmioty, na zasadach określonych w umowach zawartych przez uprawnione podmioty z przedsiębiorcą telekomunikacyjnym. Umowa może określać współudział stron w kosztach zastosowania interfejsów.

Zgodnie z art. 179 ust. 4b interfejsy powinny umożliwić uprawnionym podmiotom dostęp do przekazów telekomunikacyjnych i danych bez udziału pracowników przedsiębiorcy telekomunikacyjnego.

Przepis art. 179 ust. 4c dopuszcza wspólne przygotowanie interfejsu przez kilku przedsiębiorców. Szczegół wspólnego przygotowania interfejsów zostaną zawarte w umowach. Przed zawarciem umowy przedsiębiorcy telekomunikacyjni uzgadniają warunki techniczne i eksploatacyjne z uprawnionymi podmiotami.

Został uchylony art. 179 ust. 5 ze względu na zmianę terminologii użytej w dziale VIII i dostosowanie do pozostałych przepisów z tej jednostki redakcyjnej.

W art. 179 ust. 6 zawarto znowelizowany przepis dotyczący zawieszenia obowiązku zapewnienia warunków dostępu i utrwalania treści przekazów telekomunikacyjnych i danych związanych z tymi przekazami, określonych w ustawie, po wyrażeniu zgody podmiotów uprawnionych. W związku z niejasnościami interpretacyjnymi zrezygnowano z pojęcia „odroczenia terminu", natomiast wprowadzono możliwość czasowego zawieszenia, w całości lub w części, obowiązku zapewnienia warunków dostępu i utrwalania, które będzie mogło być zastosowane wyłącznie na czas określony, nie dłuższy niż 6 miesięcy, w szczególnie uzasadnionych przypadkach, na wniosek zainteresowanego przedsiębiorcy telekomunikacyjnego. Istotą rozwiązania wprowadzającego cezurę czasową, w przypadku wydawania przez Prezesa UKE decyzji zawieszających wykonanie przez przedsiębiorców telekomunikacyjnych obowiązków na rzecz obronności i bezpieczeństwa państwa, jest konieczność ograniczenia działań przedsiębiorców polegających na stałym odraczaniu i faktycznym braku wykonywania nałożonych na nich – już w 2004 r. – przez ustawodawcę obowiązków. Zgodnie z zaproponowaną zmianą, Prezes UKE zostałby wyposażony w harmonogram osiągnięcia przez przedsiębiorcę telekomunikacyjnego pełnej zdolności do wykonywania obowiązku i mógłby na tej podstawie w sposób bardziej efektywny, przy pomocy instrumentów ustawowych, egzekwować jego wykonanie.

W art. 179 ust. 6a zostało przewidziane wyłączenie, które powoduje że zapisów art. 179 ust. 6 nie stosuje się do przedsiębiorcy telekomunikacyjnego rozpoczynającego działalność telekomunikacyjną lub rozpoczynającego świadczenie nowej usługi telekomunikacyjnej.

W art. 179 ust. 6b został określony przypadek gdy przedsiębiorca telekomunikacyjny złożył wniosek lub został zawieszony obowiązek zapewnienia warunków dostępu i utrwalania, jednakże jest zobowiązany do realizacji ww. obowiązków w zakresie posiadanych możliwości technicznych, organizacyjnych i finansowych.

W art. 179 ust. 7 zostało wprowadzone rozwiązanie, które minimalizuje koszty po stronie przedsiębiorcy telekomunikacyjnego, polegającego na umożliwieniu outsourcingu obowiązku z art. 179 ust. 3 na podmiot wyspecjalizowany w świadczeniu tego typu usług, którym jest

przedsiębiorca telekomunikacyjny, przy zachowaniu odpowiedzialności przedsiębiorcy telekomunikacyjnego (powierzającego).

Zmiana w art. 179 ust. 8 pkt 1 i 2 polega na usunięciu niejasnego odwołania do wymogów przepisów odrębnych, które powinny spełniać osoby reprezentujące przedsiębiorcę telekomunikacyjnego w zakresie przewidzianym przepisami art. 179. Dodatkowy pkt 3 obliguje przedsiębiorców do podania Prezesowi UKE informacji uzupełniającej, w przypadku skorzystania kilku z nich z możliwości przygotowania i wspólnego eksploatowania interfejsów.

W dodanym ust. 8a został zawarty obowiązek informowania Prezesa UKE przez przedsiębiorcę telekomunikacyjnego w przypadku zmiany danych, o których mowa w art. 179 ust. 8.

Zmiany w art. 179 ust. 10 mają charakter porządkujący.

Uchylony przepis art. 179 ust. 11, po wprowadzeniu stosownych korekt związanych ze zmianą terminologii, znajduje się w proponowanej nowelizacji w art. 179 ust. 3a.

Art. 179 ust. 12 precyzuje delegację do wydania rozporządzeń. Delegacja zawarta w art. 179 ust. 12 zastępuje uchylony przepis delegujący zawarty w art. 181 w poprzednich przepisach ustawy. Nowy przepis uwzględnia nowelizację siatki pojęciowej oraz konsekwencje zmian wprowadzonych w całym art. 179.

Nowy art. 180a stanowi pierwszą część implementacji do krajowego porządku prawnego dyrektywy UE w sprawie retencji danych telekomunikacyjnych. W artykule tym wskazano, że retencja danych będzie służyła szczególnie wykrywaniu przestępstw skierowanych przeciwko obronności, bezpieczeństwu państwa, bezpieczeństwu i porządkowi publicznemu oraz przestępstw skarbowych. Przepis art. 180a ust. 1 pkt 2 nakłada na operatora publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych obowiązek zatrzymywania i przechowywania danych przez 24 miesiące. Wprowadzenie maksymalnego terminu zatrzymywania danych przez 24 miesiące wynika z okoliczności, że Polska jest lub może być wykorzystywana jako zaplecze logistyczne lub punkt tranzytowy dla ugrupowań terrorystycznych. Z uwagi na położenie geograficzne Polski, na szlakach wschód – zachód i północ – południe, istnieje bardzo duże prawdopodobieństwo wykorzystania terytorium naszego państwa właśnie w ten sposób. Dotyczy to zarówno islamistów, jak i innych grup terrorystycznych. Pomijając oczywiste zagrożenia związane z nielegalną działalnością (przemyt broni, materiałów wybuchowych i innych niebezpiecznych materiałów, przemyt ludzi, prowadzenie działalności szkoleniowej, rekrutacyjnej i propagandowej), które mają charakter pośredni dla społeczeństwa, istnieje także zagrożenie bezpośrednie w momencie ujawnienia faktu prowadzenia takiej działalności. Może to być stawianie oporu w celu udaremnienia wykonania czynności służbowych przez funkcjonariuszy (w tym z użyciem broni i ładunków wybuchowych), branie zakładników w celu umożliwienia sobie ucieczki, także poza terytorium Rzeczypospolitej Polskiej, dokonywanie zamachów terrorystycznych w celu wymuszenia na władzach uwolnienia aresztowanych osób, jak również odstąpienia od czynności wobec sprawców tych działań, także organizowanie ucieczek i buntów w zakładach karnych i aresztach śledczych. Podobny charakter mogą mieć sytuacje, w których terroryści będą próbować wykorzystać terytorium Polski jako drogę ucieczki. Z uwagi na wspomniane położenie geograficzne, członkostwo Rzeczypospolitej Polskiej w Unii Europejskiej (łatwiejsze podróżowanie w kierunku zachodnim i północnym), bliskość Bałkanów, państw postradzieckich, rozwiniętą infrastrukturę transportową i telekomunikacyjną, a także czynniki społeczne i ekonomiczne (kontakty handlowe z krajami bliskowschodnimi, przeszłą obecność wielu obywateli tych państw) należy uznać, że istnieje wysokie ryzyko wykorzystania terytorium Polski do

opisanej działalności (być może już taka działalność jest prowadzona). Wbrew powszechnemu przekonaniu o trudności z „wtopieniem się" w otoczenie, nie stanowi to problemu w dużych miastach. Jakkolwiek obecnie centrum logistycznym i werbunkowym islamistów w Europie są państwa zachodnie, to wraz ze zwiększaniem skuteczności działań policji i służb specjalnych w tych państwach, terroryści mogą zostać zmuszeni do znalezienia sobie innego miejsca, z mniej skuteczną i mniej doświadczoną w ich zwalczaniu policją. Ponadto należy zakładać, że wzrost imigracji do krajów UE dotknie także Polskę, co stworzy nowe uwarunkowania do aktywności środowisk radykalnych. Poważnym problemem może być też działalność rekrutacyjna prowadzona przez islamistów wśród rdzennych mieszkańców krajów europejskich, co przełoży się na zagrożenie wyżej opisanymi sytuacjami kryzysowymi, które również należy ocenić jako duże.

Kolejnym ważnym problemem, który dotknie bezpośrednio bezpieczeństwa Polski, może być utworzenie nowego szlaku przerzutu heroiny do Europy przez terytorium Polski za pośrednictwem żołnierzy służących w Afganistanie. Sprzedaż heroiny to jedno ze źródeł finansowania al-Kaidy. W sytuacji uczestnictwa polskich żołnierzy w przemycie narkotyków mogłaby zostać zagrożona sojusznicza wiarygodność Polski. Polscy żołnierze pomagaliby bowiem pośrednio, nie wiedząc o tym, finansować działalność al-Kaidy oraz talibów.

Warto również przypomnieć, że na terytorium Polski ma swoją siedzibę Europejska Agencja Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej (FRONTEX). Do jej zadań należy m.in.: przeprowadzanie analizy ryzyka, śledzenie rozwoju badań mających znaczenie dla kontroli i ochrony granic zewnętrznych, wspomaganie państw członkowskich w sytuacjach wymagających zwiększonej pomocy technicznej i operacyjnej na granicach zewnętrznych.

Drugą częścią tej implementacji będzie wydanie szczegółowych rozporządzeń, zgodnie z delegacją zawartą w art. 180c ust. 2.

Przepisy art. 180a ust. 1 określają obowiązek wynikający z dyrektywy, a w art. 180c zawierają ogólną klasyfikację danych podlegających retencji.

Art. 180a ust. 3 i 4 reguluje istotną kwestię przejęcia danych telekomunikacyjnych od upadłego operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych. Dane mogą stanowić bardzo ważny materiał dowodowy w postępowaniach karnych, dlatego powinny być one w dalszym ciągu przechowywane przez operatora – następcę prawnego operatora, który zaprzestał działalności. Dane takie byłyby przejęte przez Prezesa UKE na zasadach określonych w rozporządzeniu Prezesa Rady Ministrów. Konsekwencją tych propozycji jest zmiana w ustawie – Prawo upadłościowe i naprawcze (nowy ust. 6 w art. 53).

W art. 180b ust. 1 dopuszczono możliwość wykonywania obowiązków, o których mowa w art. 180a, (zatrzymywania, przechowywania i udostępniania oraz chronienia danych) wspólnie przez kilku operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych.

W art. 180b ust. 2 zostało wprowadzone rozwiązanie, które minimalizuje koszty po stronie operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych, polegające na umożliwieniu outsourcingu obowiązku z art. 180a ust. 1 na podmiot wyspecjalizowany w świadczeniu tego typu usług, którym jest przedsiębiorca telekomunikacyjny, przy zachowaniu odpowiedzialności przedsiębiorcy telekomunikacyjnego (powierzającego).

W art. 180c zostały określone kategorie danych dostępnych operatorowi publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych, które podlegają obowiązkowi z art. 180a ust. 1.

Art. 180c ust. 2 stanowi delegację dla ministra właściwego do spraw łączności w porozumieniu z ministrem właściwym do spraw wewnętrznych do wydania rozporządzenia określającego szczegółowy wykaz danych podlegających retencji oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych zobowiązanych do zatrzymywania i przechowywania określonych rodzajów danych telekomunikacyjnych. Zważywszy na dwustopniowy proces wdrożenia dyrektywy retencyjnej, odrębnie dla danych związanych z dostępem do Internetu, telefonii internetowej i internetowej poczty elektronicznej, delegacja powyższa będzie wymagała wydania dwóch odrębnych rozporządzeń.

W art. 180d zostały określone organy państwowe, którym przedsiębiorcy telekomunikacyjni, są zobowiązani zapewnić warunki dostępu i utrwalania oraz udostępnić zgromadzone dane na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych. Zapewnienie warunków dostępu i utrwalania, o których mowa w art. 180d, jest możliwe na trzy sposoby:
– przez wykorzystanie interfejsu, o którym mowa w art. 179 ust. 4a. Zgodnie z zawartą w art. 182 delegacją do wydania przez Radę Ministrów rozporządzenia, będzie możliwe takie określenie warunków technicznych i eksploatacyjnych dla interfejsów, aby były to interfejsy tożsame,
– przez budowę oddzielnego interfejsu, w oparciu o wymagania zawarte w rozporządzeniu Rady Ministrów wydanym na podstawie art. 182 projektu,
– przez wykorzystanie obecnie posiadanych przez przedsiębiorców telekomunikacyjnych rozwiązań technicznych oraz rozwiązań planowanych w związku z koniecznością udostępniania danych retencyjnych.
W każdym z wyżej wymienionych przypadków skorzystanie z udostępnienia danych przez interfejs będzie możliwe tylko w przypadku zawarcia porozumienia między przedsiębiorcą telekomunikacyjnym a uprawnionym podmiotem, co minimalizuje koszty zarówno po stronie przedsiębiorcy, jak i podmiotu uprawnionego.

Art. 180e ogranicza dostęp do danych podlegających retencji jedynie do upoważnionych pracowników przedsiębiorców telekomunikacyjnych.

Przepis art. 180f umożliwia uzyskiwanie danych niezbędnych do realizacji przez Prezesa UKE przepisów rozporządzenia Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa (Dz. U. Nr 180, poz. 1855), nakładających na Prezesa UKE obowiązek dokonywania analizy możliwości przedsiębiorców telekomunikacyjnych w zakresie ich wykorzystania na potrzeby obronne państwa oraz utworzenia bazy danych o przedsiębiorcach telekomunikacyjnych niezbędnej do przygotowania i wykorzystania obronnych systemów łączności.

Proponowany przepis umożliwi pozyskiwanie danych niezbędnych do tworzenia takiej bazy oraz aktualizacji centralnej bazy danych o systemach łączności na potrzeby obronne państwa zarządzanej przez Ministra Obrony Narodowej. Dotychczas nie było narzędzia prawnego pozwalającego skutecznie pozyskiwać ww. danych. Wprowadzenie tego przepisu umożliwi Prezesowi UKE właściwe wykonywanie zadań w zakresie obronności.

Art. 180g ust. 3 zawiera delegację do wydania rozporządzenia, którego przepisy określą wzór formularza służącego do przekazywania informacji Prezesowi UKE .

Uchylenie przepisu art. 181 ustawy – Prawo telekomunikacyjne jest konsekwencją przebudowy działu VIII ustawy, przeniesienia delegacji z art. 181 do nowego art. 179 ust. 12.

Art. 182 otrzymał nowe brzmienie; zostały wykreślone wytyczne dotyczące wymagań europejskich organizacji normalizacyjnych i wymagań innych międzynarodowych organizacji normalizacyjnych, których Rzeczpospolita Polska jest członkiem.

Art. 190 ust. 4 i 4a

Przywrócono kadencyjność Prezesa UKE oraz uzupełniono przesłanki odwołania Prezesa UKE o możliwość jego odwołania z powodu nierealizowania przez niego celów ustawy – Prawo telekomunikacyjne. Propozycja ta wychodzi naprzeciw dążeniom Komisji Europejskiej do zwiększenia niezależności krajowego organu regulacyjnego m.in. przez określenie przejrzystych przesłanek odwołania jego szefa. W ramach przeglądu ram regulacyjnych łączności elektronicznej jest proponowany następujący przepis art. 3 ust. 3 dyrektywy ramowej 2002/21/WE: „…Państwa członkowskie zapewniają, by zwolnienie szefów krajowych organów regulacyjnych lub ich zastępców było możliwe wyłącznie wówczas, gdy nie będą oni spełniać warunków wymaganych do wykonywania ich obowiązków określonych wcześniej w prawie krajowym lub jeżeli dopuszczą się poważnego uchybienia. Decyzja o zwolnieniu szefa krajowego organu regulacyjnego zawiera uzasadnienie i jest opublikowana w chwili tego zwolnienia…”.

Art. 192

W art. 192 ust. 5a został rozszerzony katalog zakresu działania Prezesa UKE przez dodanie kompetencji do kontrolowania realizacji obowiązków wynikających z przepisów rozporządzenia Parlamentu Europejskiego i Rady nr 717/2007/WE z dnia 27 czerwca 2007 r. w sprawie roamingu w publicznych sieciach telefonii ruchomej wewnątrz Wspólnoty oraz zmieniającego dyrektywę 2002/21/WE (Dz. Urz. WE L 171/32 z 29.06.2007, str. 32).

W art. 192 ust. 5b została dodana kompetencja dotycząca wykonywania kontroli nad operatorami publicznej sieci telekomunikacyjnej i dostawcami publicznie dostępnych usług telekomunikacyjnych w zakresie realizacji obowiązków, o których mowa w art. 180a ust. 1. Przechowywanie danych retencyjnych ma być podporządkowane podstawowym zasadom dotyczącym prawidłowej ochrony i bezpieczeństwa danych. W prawie polskim kontrola przestrzegania owych zasad może być prowadzona przez Generalnego Inspektora Ochrony Danych Osobowych jedynie pośrednio i w zakresie ograniczonym do danych osobowych, według zasad wynikających z ustawy o ochronie danych osobowych. Ww. nadzór będzie wykonywany przez Prezesa UKE z wyłączeniem danych osobowych chronionych zgodnie z przepisami o ochronie danych osobowych.

W art. 192 ust. 5c dodano kompetencję Prezesa UKE do prowadzenia centralnej bazy numerów przeniesionych oraz bazy zawierającej dane dotyczące infrastruktury telekomunikacyjnej eksploatowanej lub używanej przez tego przedsiębiorcę niezbędnej do przygotowania systemów łączności na potrzeby obronne państwa, w tym systemu kierowania bezpieczeństwem narodowym.

Art. 206 ust. 2, 2a i 2b

W art. 206 został rozszerzony katalog roztrzygnięć, od których przedsiębiorcom telekomunikacyjnym służy odwołanie. Został uwzględniony tryb odwoławczy od

postanowienia o uznaniu rynku właściwego za rynek konkurencyjny oraz od decyzji w sprawie zniesienia lub zmiany obowiązków regulacyjnych.

Art. 209 ust. 1 pkt 28 i 29

Zaproponowane przepisy powstały w związku z:

- niewykonywaniem przez przedsiębiorców telekomunikacyjnych obowiązku rejestrowania przypadków udostępniania danych, o których mowa w art. 180c ust. 1 pkt 3 oraz w art. 180d,
- wejściem w życie dnia 30 czerwca 2007 r. rozporządzenia (WE) nr 717/2007 Parlamentu Europejskiego i Rady z dnia 27 czerwca 2007 r. w sprawie roamingu w publicznych sieciach telefonii ruchomej wewnątrz Wspólnoty oraz zmieniającego dyrektywę 2002/21/WE, które nakłada na państwa członkowskie Unii Europejskiej obowiązek wprowadzenia przepisów określających kary stosowane w przypadku naruszenia ww. rozporządzenia.

Zmiany w ustawach:

- o Policji,
- o Straży Granicznej,
- o Biurze Ochrony Rządu,
- o kontroli skarbowej,
- Kodeks postępowania karnego,
- o Żandarmerii Wojskowej i wojskowych organach porządkowych,
- o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
- o Centralnym Biurze Antykorupcyjnym,
- o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

Przepisy zmieniające ustawy kompetencyjne zawarte w odpowiednich art. 2 – 11 ustawy mają na celu dostosowanie siatki pojęciowej stosowanej w ustawach kompetencyjnych precyzujących uprawnienia podmiotów uprawnionych i nowych przepisów art. 180a ustawy dotyczących retencji danych telekomunikacyjnych. W ustawach kompetencyjnych Policji, Straży Granicznej, wywiadu skarbowego, Żandarmerii Wojskowej, Biura Ochrony Rządu, Agencji Bezpieczeństwa Wewnętrznego, a także Służby Kontrwywiadu Skarbowego, dodane zostały przepisy, które pozwalają na zastosowanie urządzeń uniemożliwiających telekomunikację na określonym obszarze. Ponadto przewidziano obowiązek informowania Prezesa UKE o zastosowaniu tych urządzeń, a także wskazano, że przy ich zastosowaniu będzie istnieć konieczność minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych. W ustawach kompetencyjnych zostały wprowadzone przepisy umożliwiające przekazywanie danych retencyjnych za pomocą sieci telekomunikacyjnych przedstawicielom upoważnionych podmiotów. Rozwiązanie takie w znacznym stopniu skróci czas oczekiwania na uzyskanie danych retencyjnych od podmiotu prowadzącego działalność telekomunikacyjną oraz zmniejszy jego koszty. Zostały także

wprowadzone przepisy pozwalające na udostępnianie danych retencyjnych za pośrednictwem sieci telekomunikacyjnej bez udziału pracowników podmiotu prowadzącego działalność.

Zmiany w ustawie – Prawo upadłościowe i naprawcze

Dodanie ust. 6 w art. 53 ustawy – Prawo upadłościowe i naprawcze jest konsekwencją propozycji polegającej na przejęciu danych telekomunikacyjnych od upadłego operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych. Dane takie byłyby przejęte przez Prezesa UKE w przypadku ogłoszenia upadłości lub braku następcy prawnego podmiotu, który zakończył działalność telekomunikacyjną, na zasadach określonych w rozporządzeniu Prezesa Rady Ministrów.

Zmiana w ustawie o zarządzaniu kryzysowym

W toku prac prowadzonych nad projektem ustawy o kompatybilności elektromagnetycznej, wdrażającej do krajowego systemu prawnego dyrektywę 2004/108/WE – „Dyrektywa 2004/108/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 2004 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej oraz uchylająca dyrektywę 89/336/EWG" – wystąpiła kwestia właściwej implementacji art. 4 ust. 2 lit. b ww. dyrektywy, dotyczącego zastosowania przez państwa członkowskie środków specjalnych w zakresie oddawania do użytku lub użytkowania urządzeń i środków specjalnych podejmowanych ze względów bezpieczeństwa, w celu ochrony publicznej sieci telekomunikacyjnej lub stacji odbiorczych lub nadawczych, użytkowanych w celach zapewnienia bezpieczeństwa w wyraźnie określonym spektrum sytuacji.

Środki te nie mają związku z kwestiami kompatybilności elektromagnetycznej, ale ich ewentualne wprowadzenie może mieć wpływ na swobodny przepływ urządzeń, które muszą, na podstawie przepisów ustawy o kompatybilności elektromagnetycznej, spełniać zasadnicze wymagania dotyczące kompatybilności elektromagnetycznej zarówno na etapie wprowadzania ich do obrotu, jak również w fazie używania tych urządzeń przez operatorów telekomunikacyjnych i innych użytkowników. Ponieważ „środki podejmowane ze względów bezpieczeństwa" byłyby wprowadzane z przyczyn innych, niż brak zgodności z zasadniczymi wymaganiami w zakresie kompatybilności elektromagnetycznej, wydaje się właściwe wdrożenie ww. przepisu dyrektywy 2004/108/WE w ustawie o zarządzaniu kryzysowym.

Proponowane umiejscowienie ww. zmiany jako art. 11a ustawy o zarządzaniu kryzysowym wiąże się z treścią art. 11, w którym w ust. 2 dotyczącym zadań Rządowego Centrum Bezpieczeństwa w pkt 6 jest wymieniona współpraca ze strukturami Paktu Północnoatlantyckiego i Unii Europejskiej.

Proponowana zmiana do ustawy o zarządzaniu kryzysowym była wnoszona na etapie prac parlamentarnych nad tą ustawą, jednak propozycja ta nie znalazła swojego finału w ostatecznym tekście ustawy.

Przepisy przejściowe

Art. 13

Przepis przejściowy dotyczący umorzenia postępowań administracyjnych wszczętych na podstawie przepisów dotychczasowych związanych z odroczeniem terminu wykonywania przez przedsiębiorców obowiązków związanych z przygotowaniem warunków do prowadzenia kontroli operacyjnej przez podmioty uprawnione.

Aktualnie w UKE są prowadzone dwie grupy postępowań administracyjnych (łącznie 332) z wniosków przedsiębiorców telekomunikacyjnych:

- o odroczenie terminu zapewnienia uprawnionym podmiotom technicznych i organizacyjnych możliwości realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, złożonych na podstawie przepisów art. 40 ust. 2 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (249 postępowań),
- o odroczenie terminu wykonywania przedmiotowych zadań i obowiązków, złożonych na podstawie przepisów art. 179 ust. 6 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (83 postępowania).

Postępowania pierwszej grupy są prowadzone od marca 2003 r., zaś drugiej grupy od kwietnia 2005 r. W sprawie tych postępowań Prezes URTiP wielokrotnie wydawał postanowienia informujące o niemożliwości rozpatrzenia sprawy w terminie ustawowym i wyznaczające nowy termin załatwienia sprawy. Wydawane postanowienia były uzasadniane przede wszystkim brakiem możliwości załatwienia sprawy z uwagi na niewydanie (do dnia wydania postanowienia) aktu wykonawczego będącego wypełnieniem delegacji do art. 182 Prawa telekomunikacyjnego, tj. określającego wymagania techniczne i eksploatacyjne dla interfejsów umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

W proponowanej nowelizacji odchodzi się od instytucji „odraczania terminu", natomiast wprowadza się możliwość zwolnienia przedsiębiorcy telekomunikacyjnego z zapewnienia warunków dostępu i utrwalania treści przekazów telekomunikacyjnych i danych związanych z tymi przekazami. Zwolnienia te są przewidziane wyłącznie w szczególnie uzasadnionych przypadkach i nie mogą być realizowane masowo, tak jak to umożliwiają przepisy dotyczące odroczenia terminu. Ponadto przepisy rozporządzenia Rady Ministrów z dnia 13 września 2005 r. w sprawie wypełniania przez przedsiębiorców telekomunikacyjnych zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, niezależnie od możliwości 6-miesięcznego odroczenia terminu, przewidują 12-miesięczny termin dostosowania się przedsiębiorcy telekomunikacyjnego do wymagań wynikających z rozporządzenia, tj. do dnia 11 października 2006 r. Tak więc w obecnie obowiązującym stanie prawnym wszyscy przedsiębiorcy telekomunikacyjni, bez względu na konieczność wystąpienia szczególnie uzasadnionych okoliczności, korzystają z mocy prawa z 12-miesięcznego okresu przejściowego, w którym nie muszą spełniać wymagań określonych w przepisach. Stąd też prowadzone postępowania administracyjne stały się w istocie bezzasadne, jednak istniejące przepisy prawa nie pozwalają Prezesowi UKE na ich umorzenie.

Art. 15

W związku z proponowanymi zmianami w art. 190 w zakresie możliwości odwoływania Prezesa UKE i przywrócenia jego kadencyjności, które przyczyniają się do niezależności organu, rozwiązanie takie wydaje się najwłaściwsze.

Art. 16

Przepis przejściowy dotyczący retencji danych internetowych, których nie dotyczy przedmiotowa nowelizacja (w odniesieniu do tej kategorii danych Polska skorzystała z odroczenia stosowania postanowień dyrektywy 2006/24/WE, zgodnie z art. 15 ust. 3 ww. dyrektywy). W związku z powyższym, do czasu uregulowania kwestii retencji danych

internetowych, jest konieczne zachowanie dotychczasowych zasad przechowywania tych danych.
Art. 165 ust. 1 i art. 166 ust. 5 Prawa telekomunikacyjnego w obecnym brzmieniu nakładają na operatorów publicznych sieci telekomunikacyjnych i dostawców publicznie dostępnych usług telekomunikacyjnych obowiązek przechowywania przez okres 2 lat danych transmisyjnych dotyczących abonentów i użytkowników końcowych i ich udostępniania „z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego". Rozwiązanie to jest oparte na przewidzianej w art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej możliwości odstępstwa od tajemnicy telekomunikacyjnej. W związku z przyjęciem 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 zmieniającej dyrektywę 2005/58/WE, reżim przechwytywania danych związanych z przekazami telekomunikacyjnymi uległ daleko idącym zmianom. Dyrektywa 2006/24/WE wprowadziła szczegółowe regulacje w zakresie zatrzymywania i przechowywania określonych kategorii danych telekomunikacyjnych, stanowiąc w tym zakresie lex specialis wobec dyrektywy 2002/58/WE (wyraźnie podkreśla to art. 11 dyrektywy 2006/24/WE). Oznacza to, że retencja danych we Wspólnocie będzie odtąd regulowana w dwojaki sposób:
– dane telekomunikacyjne, o których mowa w art. 5 dyrektywy 2006/24/WE, będą zatrzymywane i przechowywane zgodnie ze standardami określonymi w tej dyrektywie,
– pozostałe dane – będą zatrzymywane i przechowywane w sposób określony w art. 15 ust. 1 dyrektywy 2002/58/WE (wyraźnie podkreśla to motyw 12 preambuły do dyrektywy 2006/24/WE).
Prawo krajowe powinno uwzględniać różnice wynikające ze wspólnotowej regulacji retencji danych telekomunikacyjnych w zależności od ich kategorii. Oznacza to konieczność uchylenia bądź zmiany art. 165 ust. 1 Prawa telekomunikacyjnego w jego obecnym kształcie. Przepis ten ustanawia, w zakresie retencji danych telekomunikacyjnych, ten sam reżim prawny dla wszystkich danych transmisyjnych obejmujących również dane objęte postanowieniami dyrektywy 2006/24/WE.

Art. 17
Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia, z wyjątkiem art. 180a ust. 3, który wchodzi w życie z dniem 1 stycznia 2010 r. Art. 180a ust. 3 reguluje kwestie przejęcia danych telekomunikacyjnych od upadłego operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych przez Prezesa UKE. Biorąc pod uwagę konieczność podjęcia wszystkich działań logistycznych i organizacyjnych związanych z utworzeniem systemu związanego z przechowywaniem, udostępnianiem oraz ochroną przejętych przez Prezesa UKE od upadłego operatora danych planuje się, że uruchomienie systemu nastąpi na początku 2010 r. Warto podkreślić, że aktualnie nie są znane przypadki prowadzenia postępowań upadłościowych wobec operatorów publicznej sieci telekomunikacyjnej i dostawców publicznie dostępnych usług telekomunikacyjnych. Ze względu na długotrwałość postępowania upadłościowego, przesunięcie w czasie uruchomienia funkcjonowania systemu nie nastąpi ze szkodą ani dla operatorów publicznej sieci telekomunikacyjnej i dostawców publicznie dostępnych usług telekomunikacyjnych, ani dla podmiotów uprawnionych.

Projekt ustawy nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej Ministerstwa Infrastruktury. Organizacje o charakterze lobbingowym wymienione w rejestrze podmiotów wykonujących zawodową działalność lobbingową (bip.mswia.gov.pl) nie zgłosiły zainteresowania pracami nad projektem ustawy.

OCENA SKUTKÓW REGULACJI

1. Podmioty, na które oddziałują projektowane regulacje

Do podmiotów, na które oddziałują projektowane regulacje należą przedsiębiorcy telekomunikacyjni wpisani do rejestru prowadzonego przez Prezesa UKE, których jest obecnie około siedmiu tysięcy, podmioty posiadające rezerwację częstotliwości, pozwolenia radiowe, konsumenci, użytkownicy końcowi, organy administracji rządowej.

Przepisy art. 176 – 178 dotyczące obowiązków przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń, w tym planowania procedur uruchamianych w przypadku zagrożeń, wprowadzania specyficznych ograniczeń w prowadzonej działalności telekomunikacyjnej oraz udostępniania urządzeń w przypadku ich niezbędności przy prowadzeniu akcji ratowniczej, są przepisami uporządkowanymi pod względem pojęciowym i terminologicznym w stosunku do obecnych przepisów ustawy – Prawo telekomunikacyjne. Zakładają one m.in. złagodzenie obowiązków przez określenie katalogu przedsiębiorców i rodzajów działalności telekomunikacyjnej niepodlegających obowiązkowi wykonywania planów działań w sytuacjach szczególnych zagrożeń. Został ograniczony także zakres przedmiotowy zawartości planów przedsiębiorców. Wprowadzono postulowane przez przedsiębiorców określenie sytuacji szczególnych zagrożeń oraz skonkretyzowano przepisy określające, w którym momencie należy przystąpić do realizacji procedur zawartych w planach. W treści przepisów zrezygnowano ze świadczenia usług na zasadach priorytetowych, gdyż jak wskazały techniczne analizy i badania, realizacja tak sformułowanego obowiązku jest, wobec braku jednoznacznych standardów technicznych możliwych do zaimplementowania w urządzeniach telekomunikacyjnych, niemożliwa do realizacji w sposób jednolity i obejmujący wszystkie rodzaje urządzeń komutacyjnych użytkowanych i eksploatowanych na krajowym rynku telekomunikacyjnym. Ocenia się, że przepisy art. 176 – 178 projektu łagodzą i konkretyzują obowiązki narzucone na przedsiębiorców aktualnie obowiązującymi w tym zakresie przepisami ustawy – Prawo telekomunikacyjne i nie spowodują żadnych skutków negatywnych do prowadzenia przez przedsiębiorców działalności telekomunikacyjnej. Przepisy te, a w szczególności przepisy art. 176, przy merytorycznym podejściu do ich wykonania powinny wpłynąć na większą wiarygodność przedsiębiorców, przez określenie specyficznych mechanizmów i procedur pozwalających na kontynuowanie działalności także w sytuacjach szczególnych zagrożeń.

Podobnie należy ocenić nowe przepisy art. 179 i częściowo związane z nimi przepisy art. 180a – g. W projekcie, dokonano przede wszystkim konkretyzacji zapisów i ujednolicenia pojęć stosowanych nie tylko w ustawie nowelizowanej, ale także przepisach ustaw kompetencyjnych. Powinno się to przyczynić do jednoznaczności i usunięcia szeregu wątpliwości formułowanych przez środowisko telekomunikacyjne do obecnie funkcjonujących przepisów precyzujących obowiązki przedsiębiorców w zakresie wspierania działań operacyjnych prowadzonych przez uprawnione organy państwa.

Dokonano m.in. konkretyzacji zakresu przedmiotowego danych podlegających utrwalaniu włącznie z treściami korespondencji podlegającej kontroli.

W zakresie nowych przepisów dotyczących obowiązków w zakresie zatrzymywania danych telekomunikacyjnych, sformułowanych w art. 180a – 180f oraz 180i, dokonano pierwszego etapu (poziom ustawowy) implementacji dyrektywy UE w sprawie retencji danych telekomunikacyjnych.

Koszty związane z przystosowaniem się przedsiębiorców do realizacji obowiązków w zakresie zatrzymywania danych są pochodną obowiązku zatrzymywania pewnych kategorii

danych, z punktu widzenia przedsiębiorców zbędnych, a uznanych za istotne i objętych obowiązkiem zgodnie z dyrektywą UE, takich jak np. dane o nieudanych próbach połączeń, a także silnie zależą od okresu, z którego dane należy przechowywać.

Skonkretyzowanie szacunkowych kosztów pełnego wdrożenia przedmiotowych przepisów jest w chwili obecnej niemożliwe, gdyż brak jest na dzień dzisiejszy gotowych do zastosowania technicznych rozwiązań, jak również nie istnieją specyfikacje i standardy międzynarodowe precyzujące sposób realizacji przepisów dyrektywy w zakresie zatrzymywania danych dotyczących usług związanych z siecią Internet, w tym poczty elektronicznej.

2. Konsultacje

W ramach konsultacji społecznych projekt ustawy został przesłany do: Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, Polskiej Izby Komunikacji Elektronicznej, Polskiej Izby Informatyki i Telekomunikacji, Konfederacji Pracodawców Polskich, Polskiej Konfederacji Pracodawców Prywatnych, Stowarzyszenia Budowniczych Telekomunikacji, Krajowej Izby Gospodarczej Budownictwa Telekomunikacyjnego, Federacji Związków Pracowników Telekomunikacji, Stowarzyszenia Inżynierów Telekomunikacji oraz Stowarzyszenia Elektryków Polskich . Uwagi zgłoszone przez zainteresowane podmioty były dokładnie analizowane i zostały częściowo uwzględnione w ostatecznej wersji projektu. Uwzględniono m.in. uwagę PIIT, PKPP i FZZPT, aby art. 6 dotyczył obowiązku przekazywania przez przedsiębiorców telekomunikacyjnych tylko informacji a nie dokumentów – co w konsekwencji spowodowało zdjęcie z tych przedsiębiorców obowiązku tłumaczenia niektórych dokumentów przez tłumaczy przysięgłych i ponoszenia przez nich kosztów z tym związanych (uwaga KIGEiT). Uwzględniono, ze względu na duże koszty, jak i trudności w realizacji przez przedsiębiorców, wniosek PIIT, PKPP, KIGEiT i FZZPT o wykreślenie art. 80a, który przewidywał możliwość nieodpłatnego ograniczenia przez abonenta wysokości maksymalnej miesięcznej kwoty za połączenia telefoniczne, po przekroczeniu której świadczenie usług miało być zawieszone.

W projekcie uwzględniono częściowo uwagi zgłoszone w trakcie konsultacji środowiskowych do przepisów regulujących obowiązki przedsiębiorców telekomunikacyjnych na rzecz obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego.

Obowiązki określone w art. 171 ust. 8 i 10 zostały nałożone na wszystkich przedsiębiorców telekomunikacyjnych.

W art. 179 ust. 7 zostało wprowadzone rozwiązanie, które minimalizuje koszty po stronie przedsiębiorcy telekomunikacyjnego, polegające na umożliwieniu outsourcingu obowiązku z art. 179 ust. 3 na podmiot wyspecjalizowany w świadczeniu tego typu usług, którym jest przedsiębiorca telekomunikacyjny, przy zachowaniu odpowiedzialności przedsiębiorcy telekomunikacyjnego (powierzającego).

W art. 180b ust. 2 zostało wprowadzone rozwiązanie, które minimalizuje koszty po stronie operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych, polegające na umożliwieniu outsourcingu obowiązku z art. 180a ust. 1 na podmiot wyspecjalizowany w świadczeniu tego typu usług, którym jest przedsiębiorca telekomunikacyjny, przy zachowaniu odpowiedzialności przedsiębiorcy telekomunikacyjnego (powierzającego).

Natomiast w art. 180b ust. 2 odstąpiono od obowiązku przekazywania w terminie 30 dni od dnia zawarcia przez operatorów publicznej sieci telekomunikacyjnej lub dostawców

publicznie dostępnych usług telekomunikacyjnych Prezesowi UKE umów zawartych między nimi, które regulują realizację obowiązku, o którym mowa w art. 180a ust. 1.

W art. 180c ust. 1 zostały wprowadzone poprawki polegające na wprowadzeniu pojęć zgodnych z Prawem telekomunikacyjnym.

3. Wpływ regulacji na sektor finansów publicznych

1) wejście w życie projektowanych zmian ustawy spowoduje skutki finansowe dla budżetu państwa związane z rozszerzeniem katalogu naruszeń skutkujących nałożeniem kar pieniężnych nakładanych przez Prezesa UKE, co może spowodować dodatkowe wpływy do budżetu państwa,

2) w związku z propozycją Ministra Sprawiedliwości, aby po ogłoszeniu upadłości przez operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych dalsze przechowywanie, udostępnianie oraz ochronę danych telekomunikacyjnych powierza się Prezesowi UKE. Przewiduje się, zgodnie z wyliczeniami Prezesa UKE, że wstępne koszty związane z zapewnieniem przejmowania i udostępnienia przez Prezesa UKE danych „retencyjnych" od podmiotu, wobec którego ogłoszono upadłość, wyniosą:

    a) zakup sprzętu informatycznego i oprogramowania – ok. 7 mln zł,

    b) budowa systemu zabezpieczenia zasilania oraz klimatyzacji – ok. 2 mln zł,

    c) koszty utrzymania systemu informatycznego i oprogramowania – eksploatacja, aktualizacja oprogramowania, zabezpieczenie informatyczne (bez zapewnienia ochrony fizycznej) – ok. 1 mln zł (rocznie),

    d) określenie wymagań, standardów dla interfejsu importowego do systemu informatycznego prowadzonego przez Prezesa UKE (koszt ekspertyzy) – ok. 100 tys. zł,

    e) opracowanie SIWZ do systemu informatycznego i jego oprogramowania (koszt ekspertyzy) – ok. 500 tys. zł,

    f) zatrudnienie 10 osób * śr. wynagr. 5000 zł – 600 tys. zł.

    Wstępny, całkowity koszt szacuje się na ok. 11 mln zł (bez kosztów pozyskania budynku, w którym miałby być prowadzony system; w chwili obecnej nie można oszacować tego kosztu z uwagi na to, że Prezes UKE wystąpił do Ministra Obrony Narodowej o przekazanie informacji nt. możliwości udostępnienia budynku). Źródłem finansowania będą środki finansowe zaplanowane w budżecie państwa, w części której dysponentem jest Prezes UKE.

    Koszty przechowywania danych retencyjnych w przypadku zaprzestania działalności przez przedsiębiorcę telekomunikacyjnego są generowane głównie przez ilość przedsiębiorców, którzy zaprzestali prowadzenia działalności telekomunikacyjnej, przygotowanie warunków do przechowywania, wyboru i udostępniania właściwych danych na żądanie uprawnionych podmiotów oraz zapewnienia warunków bezpieczeństwa.

    Szacuje się, że tylko w niewielkim stopniu koszty te będą uzależnione od okresu przechowywania danych transmisyjnych.

4. Wpływ regulacji na rynek pracy

Przyjęcie projektowanej regulacji nie będzie oddziaływać na rynek pracy.

5. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość

Proponowane regulacje mogą mieć wpływ na konkurencyjność w zakresie rynku telekomunikacyjnego.

Celem proponowanych regulacji jest zapewnienie i zwiększenie skutecznej konkurencji na rynku telekomunikacyjnym. W związku z powyższym ceny dostępu do sieci Internet oraz ceny usługi powszechnej powinny ulegać stopniowemu zmniejszeniu.

Zgodnie z dyrektywą ramową organy regulacyjne poszczególnych krajów są zobowiązane do przeprowadzania analiz rynkowych w celu zidentyfikowania problemów na nich występujących, określenia czy dany rynek jest konkurencyjny. W przypadku stwierdzenia, że dany rynek nie jest w pełni konkurencyjny organ regulacyjny wyznacza na tym rynku przedsiębiorcę (lub przedsiębiorców) o znaczącej pozycji rynkowej i nakłada na niego (na nich) obowiązki regulacyjne. Obowiązki nałożone w decyzji organu regulacyjnego na przedsiębiorcę (lub przedsiębiorców) o znaczącej pozycji rynkowej mają na celu zwiększenie konkurencyjności panującej na danym rynku. Wśród przykładowych obowiązków jakie mogą zostać nałożone przez organ regulacyjny można wskazać:

- obowiązek zapewnienia przedsiębiorcom telekomunikacyjnym dostępu do sieci przedsiębiorcy posiadającego pozycję SMP, w tym użytkowania elementów infrastruktury lub sieci oraz udogodnień towarzyszących, w celu świadczenia usługi,
- obowiązek równego traktowania przedsiębiorców telekomunikacyjnych w zakresie dostępu telekomunikacyjnego, w szczególności przez oferowanie jednakowych warunków w porównywalnych okolicznościach, a także oferowaniu usług oraz udostępnianiu informacji na warunkach niegorszych od stosowanych w ramach własnego przedsiębiorstwa lub w stosunkach z podmiotami zależnymi,
- obowiązek ogłaszania informacji w sprawach zapewnienia dostępu telekomunikacyjnego dotyczących specyfikacji technicznych sieci i urządzeń telekomunikacyjnych, charakterystyki sieci, zasad i warunków świadczenia usług oraz korzystania z sieci, a także opłat,
- obowiązek polegający na prowadzeniu rachunkowości regulacyjnej w sposób umożliwiający identyfikację przepływów transferów wewnętrznych związanych z działalnością w zakresie dostępu telekomunikacyjnego w celu uniknięcia zawyżania opłat lub stosowania innych rodzajów dyskryminacji cenowej,
- obowiązek polegający na ustalaniu opłat z tytułu dostępu telekomunikacyjnego w celu świadczenia dostępu telekomunikacyjnego w oparciu o ponoszone koszty operatora i przedstawienia organowi regulacyjnemu uzasadnienia ich wysokości w określonym terminie od dnia doręczenia decyzji,
- obowiązek polegający na przygotowaniu i przedstawieniu w określonym terminie od dnia doręczenia decyzji oferty ramowej o dostępie telekomunikacyjnym,
- oferowanie usług na warunkach hurtowych w celu ich dalszej odsprzedaży przez innego przedsiębiorcę.

6. Wpływ regulacji na sytuację i rozwój regionów

Zapisy projektu mogą wpłynąć na sytuację przedsiębiorców telekomunikacyjnych, a przez to również na rozwój regionów.

7. Wstępna ocena zgodności regulacji z prawem Unii Europejskiej

Projekt jest zgodny z prawem UE. Dostosowuje obowiązujące zapisy do regulacji unijnych.

28/10/BS

URZĄD
KOMITETU INTEGRACJI EUROPEJSKIEJ
SEKRETARZ
KOMITETU INTEGRACJI EUROPEJSKIEJ
SEKRETARZ STANU
Mikołaj Dowgielewicz

Min.MD-2330 /08/DP/db

Warszawa, dnia 2 października 2008 r.

Pan
Maciej Berek
Sekretarz Rady Ministrów

Opinia o zgodności z prawem Unii Europejskiej ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (pismo z dnia 24 września 2008; nr RM-10-162-08) sporządzona na podstawie art. 9 pkt 3 w zw. z art. 2 ust. 1 pkt 2 i ust. 2 pkt 2a ustawy z dnia 8 sierpnia 1996 r. o Komitecie Integracji Europejskiej (Dz. U. Nr 106, poz. 494) oraz art. 42 ust 4 Regulaminu Sejmu przez Sekretarza Komitetu Integracji Europejskiej Mikołaja Dowgielewicza

Szanowny Panie Ministrze,

W związku z przedłożonym do rozpatrzenia przez Radę Ministrów projektem *ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw* (pismo nr RM-10-162-08) pozwalam sobie wyrazić następującą opinię:

I. **Projekt w obecnym brzmieniu jest zgodny z prawem Unii Europejskiej.**

II. W projekcie zmiany ustawy Prawo telekomunikacyjne Minister Infrastruktury zaproponował, aby w ustawie o zarządzaniu kryzysowym dodać art. 11a, zgodnie z którym Rządowe Centrum Bezpieczeństwa (dalej Centrum) *informuje Komisję Europejską i państwa członkowskie Unii Europejskiej o środkach zastosowanych w sytuacji kryzysowej, w celu zabezpieczenia prawidłowego działania publicznej sieci telekomunikacyjnej oraz stacji nadawczych i odbiorczych używanych do zapewnienia bezpieczeństwa, w zakresie dotyczącym systemu łączności i sieci teleinformatycznych.*

Minister Spraw Wewnętrznych i Administracji zakwestionował nałożenie na Centrum obowiązku informowania Komisji o stosowaniu wyżej wymienionych środków, jak również podniósł wątpliwości co do kompetencji Centrum w tym zakresie.

Art. 11a ma na celu implementację dyrektywy 2004/108/WE w sprawie zbliżania ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej oraz uchylającej dyrektywę 89/336/EWG[1] (dalej dyrektywa). Dyrektywa reguluje kompatybilność elektromagnetycznych urządzeń na rynkach wewnętrznych.

[1] Dz.Urz. WE L 309 z 31.12.2004, str. 22.

PROJEKT

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia .....

w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń

(Dz. U. z dnia .....)

Na podstawie art. 176a ust. 5 ustawy z dnia …….. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa:
1) zawartość oraz tryb sporządzania i aktualizacji przez przedsiębiorcę telekomunikacyjnego, zwanego dalej "przedsiębiorcą", planu działań w sytuacjach szczególnych zagrożeń, zwanego dalej "planem";
2) zakres uzgodnień planu z organami, o których mowa w § 8;
3) rodzaje przedsiębiorców obowiązanych do uzgadniania zawartości planów;
4) rodzaje przedsiębiorców nie podlegających obowiązkowi sporządzania planu.

§ 2. Obowiązkowi sporządzenia planu nie podlega przedsiębiorca, który wykonuje działalność gospodarczą:
1) polegającą wyłącznie na dostarczaniu udogodnień towarzyszących;
2) wyłącznie na obszarze nie przekraczającym granic administracyjnych gminy.

§ 3. 1. Przedsiębiorca, z zastrzeżeniem ust. 2, sporządza plan dla obszaru wykonywania działalności telekomunikacyjnej, określonego we wniosku o wpis do rejestru przedsiębiorców telekomunikacyjnych.

2. Przedsiębiorca sporządza plan dla faktycznego obszaru wykonywanej działalności w przypadku, gdy obszar ten jest mniejszy od określonego we wniosku, o którym mowa w ust. 1.

3. Przedsiębiorca wykonujący działalność telekomunikacyjną na jednym lub kilku obszarach, które nie przekraczają granic administracyjnych powiatu, sporządza plan dla całości lub części powiatu, na obszarze którego wykonuje działalność, zwany dalej "planem lokalnym".

4. Przedsiębiorca wykonujący działalność telekomunikacyjną na jednym lub kilku obszarach, które przekraczają granice administracyjne powiatu, sporządza plan dla części lub całości każdego województwa, na obszarze którego wykonuje działalność, zwany dalej "planem rejonowym".

5. Przedsiębiorca, o którym mowa w wykazie stanowiącym załącznik do rozporządzenia Rady Ministrów z dnia 9 listopada 2007 r. w sprawie wykazu przedsiębiorców o szczególnym

---

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i numer 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331, Nr 82, poz. 556 oraz z 2008 Nr 17, poz. 101.

znaczeniu gospodarczo-obronnym (Dz. U. Nr 214, poz. 1571), sporządza plan dla obszaru całego kraju, zwany dalej "planem ogólnym", oraz plan rejonowy odrębnie dla obszaru każdego województwa, na obszarze którego wykonuje działalność.

§ 4. 1. Przedsiębiorca sporządzający plan dokonuje:

1) analizy potencjalnych, szczególnych zagrożeń na obszarze, na którym wykonuje działalność telekomunikacyjną;
2) oceny wpływu szczególnych zagrożeń na własną infrastrukturę telekomunikacyjną oraz zdolność do zachowania ciągłości prowadzonej przez siebie działalności telekomunikacyjnej;
3) analizy potrzeb w zakresie świadczenia, utrzymania i odtwarzania usług telekomunikacyjnych oraz dostępu telekomunikacyjnego do współpracy z:
   a) podmiotami koordynującymi działania ratownicze,
   b) podmiotami zarządzania kryzysowego,
   c) służbami ustawowo powołanymi do niesienia pomocy,
   d) podmiotami realizującymi zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, wskazanymi przez organy, o których mowa w § 8;

2. Analizy i oceny, o których mowa w ust. 1 pkt 1 i 3, na potrzeby sporządzania planów rejonowych i lokalnych, przedsiębiorca dokonuje na podstawie danych uzyskanych, po wystąpieniu o ich udostępnienie, od właściwych terytorialnie wojewodów lub starostów.

3. Analizy i oceny, o których mowa w ust. 1 pkt 1 i 3, na potrzeby sporządzania planów ogólnych, przedsiębiorca dokonuje na podstawie danych uzyskanych, po wystąpieniu o ich udostępnienie, od organów, o których mowa w § 8 ust. 1 pkt 1 i 2, lub wskazanych przez nie centralnych organów administracji rządowej, odpowiednio do ich kompetencji.

§ 5. Plan ogólny powinien zawierać w szczególności:

1) podstawowe dane identyfikujące przedsiębiorcę określone w art. 10 ust. 4 pkt 1, 2, 5 i 6 ustawy z dnia 16 lipca - Prawo telekomunikacyjne, zwanej dalej "ustawą";
2) imiona, nazwiska, adresy i numery telefonów osób odpowiedzialnych za sporządzenie planu, wraz z określeniem zakresu ich kompetencji;
3) wykaz przeprowadzonych uzgodnień, wraz z potwierdzeniem ich dokonania przez podmioty, o których mowa w § 8;
4) ogólną charakterystykę prowadzonej działalności telekomunikacyjnej, w tym charakterystykę świadczonych usług oraz wykaz obiektów infrastruktury telekomunikacyjnej o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy i obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa ustalonych zgodnie z przepisami rozporządzenia Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Dz. U. Nr 116, poz. 1090);
5) wyniki analiz i oceny, o których mowa w § 4 ust. 1;
6) procedury współpracy przedsiębiorcy w sytuacjach szczególnych zagrożeń z innymi przedsiębiorcami, dotyczące zapewnienia dostępu telekomunikacyjnego, w tym w szczególności współpracy z zagranicznymi przedsiębiorcami telekomunikacyjnymi;
7) procedury współpracy przedsiębiorcy z podmiotami, o których mowa w art. 4 pkt 1, 2, 4, 5, 7 i 8 ustawy, w zakresie świadczenia, utrzymania i odtwarzania usług telekomunikacyjnych oraz zapewnienia i odtwarzania dostępu telekomunikacyjnego, w tym na zasadach pierwszeństwa, po dokonaniu oceny, o której mowa w § 4 ust. 1 pkt 3;

8) procedury, warunki i sposób zapewnienia połączeń telekomunikacyjnych na zasadach pierwszeństwa dla właściwych organów i służb, innych niż określone w pkt 7, ustalone na podstawie oceny, o której mowa w § 4 ust. 1 pkt 3, wraz z ich wykazem;
9) wykaz elementów sieci telekomunikacyjnych oraz sposób ich przygotowania do zapewnienia telekomunikacji na potrzeby podmiotów i służb wymienionych w § 4, ust. 1, pkt 3 wraz z procedurami uruchomienia tych elementów zgodnie z art. 176a, ust. 2 pkt 4 ustawy;
10) procedury współpracy z ministrem właściwym do spraw łączności, Prezesem Urzędu Komunikacji Elektronicznej, zwanym dalej "Prezesem UKE", oraz właściwymi organami i służbami w zakresie sposobów wzajemnego przekazywania informacji, alarmowania i ostrzegania, dotyczących sytuacji szczególnych zagrożeń, a także powiadamiania o konieczności podjęcia lub zaprzestania działań określonych w planie, wraz z wykazem imion i nazwisk osób lub nazw służb, właściwych w sprawach zarządzania kryzysowego, adresów lub siedzib, numerów telefonów i innych danych kontaktowych oraz zakresem ich kompetencji;
11) opis struktur organizacyjnych przedsiębiorcy obowiązujących w przypadku wystąpienia sytuacji szczególnych zagrożeń wraz z wykazem imion i nazwisk osób lub nazw służb, właściwych w sprawach zarządzania kryzysowego, adresów lub siedzib, numerów telefonów i innych danych kontaktowych oraz zakresem ich kompetencji;
12) opis wdrożonych systemów zabezpieczeń przed zakłóceniami, skutkami katastrof, klęsk żywiołowych i nieuprawnionym dostępem oraz procedur działania i środków wdrażanych w sytuacjach szczególnych zagrożeń dla zabezpieczenia własnej infrastruktury telekomunikacyjnej przedsiębiorcy;
13) wykaz obiektów i elementów infrastruktury telekomunikacyjnej dostosowanych do współpracy z ruchomymi urządzeniami telekomunikacyjnymi używanymi przez podmioty, o których mowa w art. 4 pkt 1 ustawy, wraz z procedurami ich użycia;
14) wykaz zrealizowanych inwestycji, o których mowa w § 11 ust. 1 pkt 1 lit. d rozporządzenia Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa (Dz. U. Nr 180, poz. 1855) zgodnie z art. 176a, ust. 2 pkt 3 i pkt 4 ustawy.

§ 6. Plan rejonowy powinien zawierać w szczególności:
1) treści określone w § 5 pkt 1-6, 8 i 10-14;
2) procedury współpracy przedsiębiorcy z właściwymi organami i służbami w zakresie zachowania ciągłości świadczenia usług oraz ich odtwarzania na zasadach pierwszeństwa w sytuacjach szczególnych zagrożeń;
3) wykaz urządzeń telekomunikacyjnych przeznaczonych lub możliwych do udostępnienia przez przedsiębiorcę innym przedsiębiorcom telekomunikacyjnym lub właściwym organom i służbom, niezbędnych do przeprowadzenia akcji ratowniczych oraz procedury udostępniania tych urządzeń;
4) charakterystykę asortymentową i ilościową zgromadzonych przez przedsiębiorcę rezerw przeznaczonych na utrzymanie ciągłości świadczenia usług oraz ich odtwarzanie w sytuacjach szczególnych zagrożeń wraz z procedurami ich użycia lub charakterystykę warunków zapewnienia dostawy urządzeń i podzespołów rezerwowych oraz usług zgodnie z umowami zawartymi z dostawcami;
5) wykaz właściwych organów i służb, dla których przedsiębiorca zapewnia dostęp telekomunikacyjny lub świadczy usługi wraz z określeniem ich rodzajów oraz procedur, warunków i sposobów świadczenia, utrzymania i odtwarzania tych usług lub dostępu,

realizowanych po dokonaniu oceny, o której mowa w § 4 ust. 1 pkt 3.

§ 7. Plan lokalny powinien zawierać w szczególności:
1) treści określone w § 5 pkt 1-6, 8, 11, 12 oraz § 6 pkt 2-5;
2) procedury współpracy z Prezesem UKE oraz właściwymi organami i służbami w zakresie sposobów wzajemnego przekazywania informacji, alarmowania i ostrzegania, dotyczących sytuacji szczególnych zagrożeń, a także powiadamiania o konieczności podjęcia lub zaprzestania działań określonych w planie, wraz z wykazem imion i nazwisk osób lub nazw służb, właściwych w sprawach zarządzania kryzysowego, adresów lub siedzib, numerów telefonów i innych danych kontaktowych oraz zakresem ich kompetencji.

§ 8. 1. Każdy przedsiębiorca sporządzający plan ogólny dokonuje jego uzgodnień z:
1) Ministrem Obrony Narodowej, ministrem właściwym do spraw wewnętrznych - w zakresie określonym w § 5 pkt 7-10 i 13;
2) ministrem właściwym do spraw zagranicznych, ministrem właściwym do spraw finansów publicznych, Ministrem Sprawiedliwości, Szefem Agencji Bezpieczeństwa Wewnętrznego oraz Szefem Agencji Wywiadu - w zakresie określonym w § 5 pkt 7 i 8;
3) ministrem właściwym do spraw łączności - w zakresie określonym w § 5 pkt 9, 10 i 14;
4) Prezesem UKE - w zakresie określonym w § 5 pkt 10, 13 i 14.

2. Każdy przedsiębiorca sporządzający plan rejonowy (z zastrzeżeniem ust. 4) dokonuje jego uzgodnień z:
1) ministrem właściwym do spraw łączności - w zakresie określonym w § 5 pkt 10 i 14;
2) Prezesem UKE - w zakresie określonym w § 5 pkt 10, 13 i 14;
3) właściwym terytorialnie wojewodą - w zakresie określonym w § 5 pkt 8 i 10 oraz w § 6 pkt 2 i 5.

3. Każdy przedsiębiorca sporządzający plan lokalny (z zastrzeżeniem ust. 4) dokonuje jego uzgodnień z:
1) Prezesem UKE - w zakresie określonym w § 7 pkt 2;
2) właściwym terytorialnie starostą - w zakresie określonym w § 5 pkt 8, § 6 pkt 2 i 5 oraz § 7 pkt 2.

4. Obowiązkowi uzgadniania planu nie podlega przedsiębiorca, którego jedyną formą działalności telekomunikacyjnej jest tylko i wyłącznie:
1) Świadczenie usług telefonii komórkowej jako operator wirtualnej sieci ruchomej MVNO (Mobile Virtual Network Operator) lub;
2) Świadczenie usług transmisji programów radiofonicznych lub telewizyjnych.

§ 9. Po dokonaniu uzgodnień, o których mowa w § 8, przedsiębiorca wprowadza plan do stosowania, co potwierdza podpisem osoba uprawniona do prowadzenia spraw przedsiębiorcy w zakresie określonym w rozporządzeniu.

§ 10. 1. Po zatwierdzeniu planu przedsiębiorca przekazuje:
1) po jednym egzemplarzu planu, o którym mowa w § 3 ust. 4 i 5, ministrowi właściwemu do spraw łączności oraz Prezesowi UKE;
2) jeden egzemplarz planu, o którym mowa w § 3 ust. 3, Prezesowi UKE.

2. W przypadku stwierdzenia braku kompletności planu, Prezes UKE zwraca go przedsiębiorcy, wyznaczając termin jego uzupełnienia.

3. Przedsiębiorca sporządza i przekazuje nieodpłatnie wyciąg z planu, sporządzony w

zakresie zagadnień podlegających uzgodnieniom, organom uzgadniającym plan, na ich wniosek.

4. Obowiązkowi przekazania planu osobom wymienionym w ust. 1 nie podlega przedsiębiorca wymieniony w § 8 ust. 4.

§ 11. 1. Plan podlega okresowej aktualizacji - nie rzadziej niż raz na 3 lata, w trybie określonym w § 4-10.

2. Plan podlega bieżącej aktualizacji w przypadku wystąpienia okoliczności wpływających na jego zawartość, a w szczególności:

1) w przypadku zmian w infrastrukturze telekomunikacyjnej oraz zakresie wykonywanej działalności telekomunikacyjnej, wpływających na zmianę sposobu i formę realizacji planu;
2) w przypadku zmiany danych identyfikujących przedsiębiorcę, warunków lub procedur współpracy z organami uzgadniającymi zawartość planu;
3) na wniosek właściwych organów administracji publicznej uzgadniających zawartość planu, uzasadniony zmianami potrzeb, o których mowa w § 4 ust. 1 pkt 3;
4) w przypadku zmiany danych dotyczących szczególnych zagrożeń.

3. Zmiana treści planu, o których mowa w § 5 pkt 7-10, 13 i 14, § 6 pkt 2 i 5 oraz § 7 pkt 2, wymaga uzgodnienia z organami, o których mowa w § 8, w zakresie ich właściwości.

4. Treść każdej zmiany planu ogólnego i rejonowego przedsiębiorca przekazuje odpowiednio ministrowi właściwemu do spraw łączności oraz Prezesowi UKE.

5. Treść każdej zmiany planu lokalnego przedsiębiorca przekazuje tylko Prezesowi UKE.

6. Do zmiany planu stosuje się przepisy § 10.

§ 12. 1. Przedsiębiorca sporządza plan zgodnie z przepisami rozporządzenia w terminie dwunastu miesięcy od dnia rozpoczęcia świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej albo od dnia wejścia w życie rozporządzenia, w zależności od tego, który z tych terminów nastąpi później.

2. Plany przedsiębiorców sporządzone na podstawie przepisów dotychczasowych zachowują moc do czasu sporządzenia planów na podstawie rozporządzenia.

§ 13. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

UZASADNIENIE

Projekt rozporządzenia Rady Ministrów **w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń** jest wykonaniem delegacji zawartej w art. 176a ust. 5 ustawy z dnia ..... - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.)

Niniejszy projekt rozporządzenia był poprzedzony rozporządzeniem Ministra Infrastruktury z dnia 16 czerwca 2005 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz. U. Nr 122, poz. 1029) wydanym na podstawie art. 176 ust. 4 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne.

Zgodnie z treścią znowelizowanej delegacji ustawowej nie zmienił się cel wydania regulacji, a jedynie jego zakres i jest w nim określenie:

1) zawartość oraz tryb sporządzania i aktualizacji przez przedsiębiorcę telekomunikacyjnego, zwanego dalej "przedsiębiorcą", planu działań w sytuacjach szczególnych zagrożeń, zwanego dalej "planem";
2) zakres uzgodnień planu z organami, o których mowa w § 8;
3) rodzaje przedsiębiorców obowiązanych do uzgadniania zawartości planów;
4) rodzaje przedsiębiorców nie podlegających obowiązkowi sporządzania planu.

W niniejszym rozporządzeniu doprecyzowano rodzaje przedsiębiorców telekomunikacyjnych obowiązanych do uzgadniania zawartości planów z „właściwymi organami”.

W poprzednim rozporządzeniu taki obowiązek spoczywał na wszystkich przedsiębiorcach telekomunikacyjnych wykonujących plany. A więc zmniejszono liczbę przedsiębiorców dokonujących uzgodnień oraz dokładniej określono jaki przedsiębiorca telekomunikacyjny nie dokonuje uzgodnień.

Z powyższego obowiązku wyłączono operatorów wirtualnej sieci ruchomej MVNO oraz przedsiębiorców telekomunikacyjnych świadczących usługi transmisji programów radiofonicznych lub telewizyjnych, jeśli jest to jedyna forma ich działalności telekomunikacyjnej.

OCENA SKUTKÓW REGULACJI

I. Podmioty, na które oddziałuje rozporządzenie.

Podmiotami, do których adresowane jest rozporządzenie są przedsiębiorcy telekomunikacyjni oraz uprawnione organy państwowe realizujące zadania na rzecz obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego.

II. Konsultacje społeczne.

Wobec faktu, że rozporządzenie zastępuje rozporządzenie Ministra Infrastruktury z dnia 16 czerwca 2005 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz. U. Nr 122, poz. 1029), nie zmieniając zakresu obowiązków nakładanych na przedsiębiorców telekomunikacyjnych, projektu nie skierowano do konsultacji społecznych.

III Wpływ na sektor finansów publicznych, w tym na budżet państwa i budżet jednostek samorządu terytorialnego oraz przychody i wydatki przedsiębiorców.

Wejście w życie rozporządzenia nie będzie miało wpływu na budżet państwa ani budżet samorządu terytorialnego oraz przychody i wydatki przedsiębiorców.

IV Wpływ regulacji na rynek pracy.

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

V Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość.

Wejście w życie rozporządzenia nie będzie miało wpływu na konkurencyjność gospodarki.

VI Wpływ regulacji na sytuację i rozwój regionów.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na sytuację i rozwój regionalny.

VII Zgodność z prawem Unii Europejskiej.

Przedmiot projektowanego aktu prawnego nie jest objęty zakresem prawa Unii Europejskiej.

13-10-tg

Projekt

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia

w sprawie określenia wymagań i sposobu zapewnienia przez przedsiębiorców telekomunikacyjnych, uprawnionym podmiotom, warunków dostępu i utrwalania w odniesieniu do niektórych danych będących w posiadaniu przedsiębiorców telekomunikacyjnych

Na podstawie art. 179 ust. 12 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. 1. Rozporządzenie określa:

1) wymagania i sposób zapewnienia, przez przedsiębiorców telekomunikacyjnych, uprawnionym podmiotom warunków dostępu i utrwalania, o których mowa w art. 179 ust. 3 ustawy, z wyłączeniem spraw uregulowanych w art. 242 Kodeksu postępowania karnego;
2) rodzaje działalności telekomunikacyjnej oraz rodzaje przedsiębiorców telekomunikacyjnych niepodlegających obowiązkowi zapewnienia warunków dostępu i utrwalania, o którym mowa w art. 179 ust. 3 ustawy.

2. Ilekroć w rozporządzeniu jest mowa o "ustawie", rozumie się przez to ustawę z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne.

§ 2. Z zastrzeżeniem § 11, przedsiębiorca telekomunikacyjny nie korzystający z rozwiązania interfejsowego zapewnia uprawnionym podmiotom warunki dostępu i utrwalania, o których mowa w art. 179 ust. 3 ustawy, poprzez stworzenie możliwości technicznych i organizacyjnych włączenia urządzeń będących na wyposażeniu uprawnionych podmiotów w punkcie styku lub w miejscu zapewniającym:

1) zapoznanie się z treścią i danymi w sposób umożliwiający dostęp:
   a) do treści komunikatu i innych danych, o których mowa w art. 159 ust. 1 ustawy, przekazywanych w sieci telekomunikacyjnej przedsiębiorcy, wysyłanych lub odbieranych w zakończeniach tej sieci uprawnione podmioty,
   b) do posiadanych lub przetwarzanych przez przedsiębiorcę danych:
      - określonych w art. 159 ust. 1 pkt 3 i 5 ustawy, dotyczących wskazanego przez uprawnione podmioty zakończenia sieci tego przedsiębiorcy,
      - określających zakończenia sieci, użytkownika lub abonenta, w przypadku zastosowania środków służących przekierowywaniu połączeń do sieci innych przedsiębiorców lub innych zakończeń sieci,
      - określonych w art. 159 ust. 1 pkt 4 ustawy, dotyczących wskazanych przez uprawnione podmioty zakończeń sieci tego przedsiębiorcy,
      - dotyczących rodzajów usług telekomunikacyjnych, z których korzysta wskazany przez uprawnione podmioty użytkownik lub abonent,
      - określonych w art. 161 ust. 2 i 3 ustawy lub zgromadzonych w wykazie, o którym mowa w art. 179 ust. 9 ustawy, dotyczących zakończeń sieci, użytkownika lub abonenta,
   c) do dokonania utrwalania przez uprawnione podmioty:
      - treści komunikatu i danych, o których mowa w pkt 1 lit. a,
      - danych, o których mowa w pkt 1 lit. b tiret pierwsze i drugie,
      - danych, o których mowa w pkt 1 lit. b tiret trzecie, wraz z czasem ich zaistnienia;

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834 oraz z 2007 r Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556.

2) stały dostęp uprawnionym podmiotom do punktu styku i miejsca jego lokalizacji poprzez takie zorganizowanie przez przedsiębiorcę pracy podległych mu pracowników aby dostęp ten był możliwy na każde żądanie uprawnionego podmiotu.

§ 3. Z zastrzeżeniem § 11, przedsiębiorca telekomunikacyjny eksploatujący sieć telekomunikacyjną obsługującą więcej niż 50.000 zakończeń sieci zapewnia warunki dostępu i utrwalania za pomocą interfejsu, o którym mowa w art. 179 ust. 4 ustawy. Przepis § 2 i 4 stosuje się odpowiednio.

§ 4. Warunki, o których mowa w § 2, zapewnia się w sposób umożliwiający:
1) rozpoczęcie dostępu, o którym mowa w § 2 pkt 1 lit a i b, lub utrwalania, o którym mowa w pkt. 1 lit c, niezwłocznie po wskazaniu przez uprawnione podmioty zakończeń sieci;
2) całodobowy, równoczesny z wysyłaniem lub odbiorem komunikatu, dostęp i utrwalanie treści komunikatu i danych, o których mowa w § 2 pkt 1 lit. a, natomiast jeżeli dostęp równoczesny nie jest możliwy - niezwłoczne dostarczenie treści komunikatu lub danych, które nie mogły być dostarczone;
3) dostęp i utrwalanie treści komunikatu lub danych w sposób pozwalający na ich odtworzenie przy pomocy standardowych urządzeń odtwarzających lub powszechnie stosowanego sprzętu komputerowego, w postaci:
   a) wysyłanej lub odbieranej we wskazanych zakończeniach sieci przedsiębiorcy - w przypadku treści komunikatu, o którym mowa w § 2 pkt 1 lit. a,
   b) występującej w sieci telekomunikacyjnej, jak również przetwarzanej przez przedsiębiorcę, a jeżeli ich nie przetwarza - w postaci, w jakiej występują w sieci telekomunikacyjnej - w przypadku danych, o których mowa w § 2 pkt 1 lit. b;
4) dostęp i utrwalanie treści komunikatu lub danych, tak aby na skutek zastosowania systemu jakość oraz zakres usługi telekomunikacyjnej świadczonej kontrolowanemu abonentowi lub użytkownikowi nie uległy zmianie.

§ 5. 1. Przedsiębiorca w ramach realizacji warunków dostępu i utrwalania powinien stosować się do wymagań ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, zpóźn. zm.[2)]).

2. Przedsiębiorca zapewniający warunki dostępu i utrwalania za pomocą interfejsu, o którym mowa w art. 179 ust. 4 ustawy, powinien zapewniać warunki do ochrony informacji niejawnych oznaczonych klauzulą "ściśle tajne", potwierdzone świadectwem bezpieczeństwa przemysłowego - pierwszego stopnia.

3. Przedsiębiorca nie wymieniony w ust. 2 oraz w przypadku:
1) eksploatowania sieci telekomunikacyjnej obsługującej od 5.000 do 50.000 zakończeń sieci -powinien zapewniać warunki do ochrony informacji niejawnych oznaczonych klauzulą "ściśle tajne", potwierdzone świadectwem bezpieczeństwa przemysłowego - drugiego stopnia;
2) eksploatowania sieci telekomunikacyjnej obsługującą od 500 do 5000 zakończeń sieci- powinien zapewniać warunki do ochrony informacji niejawnych oznaczonych klauzulą "ściśle tajne", potwierdzone świadectwem bezpieczeństwa przemysłowego - trzeciego stopnia.

4. Do dostępu do informacji niejawnych przez przedsiębiorcę eksploatującego sieć telekomunikacyjną obsługującą do 500 zakończeń sieci lub świadczącego usługi dostępu do sieci Internet za pośrednictwem sieci telekomunikacyjnej obsługującej do 500 zakończeń sieci posiadających własny adres IP, który nie posiada świadectwa bezpieczeństwa przemysłowego, mają zastosowanie przepisy art. 49 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.

§ 6. 1. Przedsiębiorca przekazuje:
1) informacje wskazujące miejsce realizacji dostępu i utrwalania treści komunikatu i danych;

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708 i 711, Nr 149, poz. 1078, Nr 218, poz. 1592 i Nr 220, poz. 1600.

2) specyfikację techniczną punktów styku, o których mowa w § 2, następującym podmiotom: Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw finansów publicznych, Szefowi Agencji Bezpieczeństwa Wewnętrznego i Szefowi Agencji Wywiadu.

§ 7. Udział pracowników przedsiębiorcy w zapewnieniu warunków dostępu i utrwalania powinien być ograniczony do niezbędnego minimum.

§ 8. W przypadku wystąpienia okoliczności uniemożliwiających dostęp lub utrwalanie treści komunikatu i danych przedsiębiorca składa, na pisemny wniosek uprawnionego podmiotu, pisemne wyjaśnienie zawierające opis okoliczności uniemożliwiających realizację zadań.

§ 9. 1. Miejsce dostępu i punkt styku, o którym mowa w § 2, przedsiębiorca przygotowuje w sposób zapewniający uprawnionym podmiotom jednoczesny i wzajemnie niezależny dostęp lub utrwalanie treści komunikatu i danych.

2. Maksymalna liczba zakończeń sieci, które mogą być wskazane przez uprawnione podmioty w celu zapewnienia warunków dostępu i utrwalania jest uzgadniana, w drodze odrębnych pisemnych porozumień zawartych przez przedsiębiorcę z Ministrem Obrony Narodowej, ministrem właściwym do spraw wewnętrznych, ministrem właściwym do spraw finansów publicznych, Szefem Agencji Bezpieczeństwa Wewnętrznego i Szefem Agencji Wywiadu.

3. W przypadku braku uzgodnienia, liczba zakończeń sieci dla każdego z organów, o których mowa w ust. 2, powinna wynosić co najmniej:

1) 0,05 % pojemności każdej centrali wchodzącej w skład sieci przedsiębiorcy lub
2) 0,03 % zakończeń sieci przedsiębiorcy zapewniającego warunki dostępu i utrwalania - z tym że nie może być mniejsza niż dwa.

§ 10. 1. Warunkami udzielenia zawieszenia, o którym mowa w art. 179 ust. 6 ustawy, są:

1) wystąpienie, niezależnych od przedsiębiorcy, trudności organizacyjnych, technicznych lub finansowych uniemożliwiających zapewnienie warunków dostępu i utrwalania;
2) złożenie wraz z pisemnym wnioskiem, o którym mowa w art. 179 ust. 6 ustawy, harmonogramu osiągnięcia przez przedsiębiorcę pełnej zdolności do zapewnienia warunków dostępu i utrwalania.

2. Wniosek, o którym mowa w ust. 1 pkt 2, przedsiębiorca składa najpóźniej w terminie 14 dni od dnia powstania okoliczności, o których mowa w ust. 1 pkt 1.

3. Złożenie wniosku, o którym mowa w ust. 1 pkt 2, nie zwalnia przedsiębiorcy od obowiązku zapewnienia warunków dostępu i utrwalania, w zakresie posiadanych możliwości technicznych, organizacyjnych i finansowych.

§ 11. Obowiązkowi zapewnienia warunków dostępu i utrwalania nie podlega wykonywanie działalności telekomunikacyjnej polegającej na:

1) dostarczaniu udogodnień towarzyszących;
2) rozpowszechnianiu lub rozprowadzaniu programów radiofonicznych lub telewizyjnych.

§ 12. Przedsiębiorcy dostosują się do wymagań wynikających z niniejszego rozporządzenia w terminie 12 miesięcy od dnia jego wejścia w życie.

§ 13. Czynności mające na celu rozpoczęcie i zakończenie dostępu lub utrwalania związanego z wykorzystaniem urządzeń, których mowa § 2, będących na wyposażeniu uprawnionych podmiotów wykonywane są przez upoważnionego funkcjonariusza, żołnierza lub pracownika tego podmiotu.

§ 14. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów

Uzasadnienie

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 179 ust. 12 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), które zostało wprowadzone ustawą o zmianie ustawy - Praw telekomunikacyjne oraz niektórych innych ustaw (Dz. U. Nr …, poz. …), a celem nowelizacji była implementacja do krajowego porządku prawnego postanowień dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 roku w sprawie zatrzymywania przetwarzanych danych w związku ze świadczeniem publicznych usług łączności elektronicznej oraz dostarczaniem publicznych sieci komunikacji elektronicznej, zmieniającej dyrektywę 2002/58/WE. Delegacja zawarta w art. 179 ust. 12 zastępuje uchylony przepis delegujący zawarty w art. 181, w poprzednich przepisach ustawy. Nowy przepis uwzględnia zmianę siatki pojęciowej oraz zmiany wprowadzonych w całym art. 179.

Rozporządzenie określa wymagania i sposób zapewnienia przez przedsiębiorców telekomunikacyjnych na rzecz uprawnionych podmiotów, warunków dostępu i utrwalania w odniesieniu do niektórych danych będących w ich posiadaniu, a także rodzaje działalności telekomunikacyjnej oraz rodzaje przedsiębiorców telekomunikacyjnych niepodlegających obowiązkowi zapewnienia warunków dostępu i utrwalania.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej

Projekt rozporządzenia nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

OCENA SKUTKÓWREGULACJI

Podmioty na które oddziałuje projektowane rozporządzenie
Projektowane rozporządzenie oddziałuje na przedsiębiorców telekomunikacyjnych obowiązanych do zapewnienia warunków dostępu i utrwalania na rzecz uprawnionych podmiotów warunków dostępu i utrwalania w odniesieniu do niektórych danych będących w ich posiadaniu oraz na podmiotu uprawnione na rzecz których świadczony jest ten obowiązek.

Zakres konsultacji
Projekt rozporządzenia zostanie przekazany w ramach konsultacji do szerokiego kręgu przedsiębiorców telekomunikacyjnych

Wpływ regulacji na:
1) sektor finansów publicznych w tym budżet państwa jednostek samorządu terytorialnego – brak wpływu;
2) rynek pracy – brak wpływu;
3) konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorstw – brak wpływy;
4) sytuacje i rozwój regionalny – brak wpływu.

Projekt

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW
z dnia

w sprawie sposobu przekazywania i udostępniania danych telekomunikacyjnych w przypadku upadłości operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych

Na podstawie art. 180a ust. 4 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa sposób:

1) przekazywania Prezesowi Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE", danych, o których mowa w art. 180c ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, zwanych dalej „danymi", przechowywanych przez operatora publicznej sieci telekomunikacyjnej lub dostawcę publicznie dostępnych usług telekomunikacyjnych w przypadku ogłoszenia jego upadłości, zwanego dalej „upadłym";
2) udostępniania przez Prezesa UKE danych podmiotom, o których mowa w art. 180a ust. 1 pkt 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, zwanych dalej „podmiotami uprawnionymi".

§ 2. 1. Upadły przekazuje dane Prezesowi UKE w terminie 90 dni od dnia wydania przez sąd postanowienia o ogłoszeniu upadłości.

2. Dane przekazuje się na informatycznych nośnikach danych w postaci zapisu w formacie tekstowym lub innym formacie umożliwiającym ich odczyt za pomocą powszechnie dostępnego sprzętu informatycznego i oprogramowania, wraz ze wskazaniem:

1) nazwy i wersji zastosowanego formatu oraz oprogramowania;
2) rodzaju sprzętu informatycznego, umożliwiającego odczyt danych.

3. W przypadku zastosowania przez upadłego specjalistycznych programów informatycznych do przetwarzania danych, przed przekazaniem Prezesowi UKE danych, upadły dokonuje ich konwersji do formatu, o którym mowa w ust. 2.

4. Upadły wraz z danymi przekazuje szczegółowy opis nazw, skrótów i struktury przekazywanych danych, pozwalający na jednoznaczne ich interpretowanie.

§ 3. Z czynności przekazania danych Prezes UKE sporządza protokół, w którym zamieszcza się:

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i poz. 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556 oraz z 2008 r. Nr 17, poz. 101.

1) oznaczenie upadłego, w szczególności jego nazwę, adres i numer z rejestru przedsiębiorców telekomunikacyjnych;

2) imię, nazwisko i stanowisko służbowe osoby przekazującej dane oraz oznaczenie dokumentu upoważniającego tę osobę do reprezentowania upadłego;

3) imię, nazwisko i stanowisko służbowe osoby przyjmującej dane oraz oznaczenie dokumentu upoważniającego tę osobę do reprezentowania Prezesa UKE;

4) wskazanie pojemności informatycznego nośnika danych, na którym przekazywane są dane, z podaniem ilości i wielkości plików zawartych na tym nośniku;

5) nazwę i określenie wersji zastosowanego formatu zapisu danych oraz nazwę i określenie wersji oprogramowania oraz rodzaju sprzętu informatycznego, za pomocą którego będzie możliwe odtwarzanie przekazywanych danych;

6) szczegółowy opis zastosowanych nazw, skrótów i kodów pozwalających na interpretowanie danych;

7) opis struktury danych zapisanych na informatycznym nośniku danych;

8) opis zabezpieczeń i wykaz zastosowanych haseł lub kodów dostępu - w przypadku zastosowania zabezpieczeń dostępu do przekazywanych danych.

§ 4. Na żądanie podmiotów uprawnionych Prezes UKE udostępnia dane w postaci zapisu w formacie tekstowym lub innym formacie umożliwiającym odczyt danych za pomocą powszechnie dostępnego sprzętu informatycznego i oprogramowania.

§ 5. Z czynności udostępniania danych Prezes UKE sporządza notatkę zawierającą:

1) datę i miejsce sporządzenia notatki oraz sygnaturę sprawy;

2) informacje dotyczące podstawy udostępnienia danych;

3) oznaczenie upadłego, którego dane są udostępniane, w szczególności jego nazwę, adres i numer z rejestru przedsiębiorców telekomunikacyjnych;

4) określenie zakresu danych, które udostępniono;

5) imię, nazwisko i stanowisko służbowe osoby udostępniającej dane oraz oznaczenie dokumentu upoważniającego tę osobę do reprezentowania Prezesa UKE;

6) imię, nazwisko i stanowisko służbowe osoby przyjmującej dane oraz oznaczenie dokumentu upoważniającego do przyjęcia udostępnionych danych;

7) wskazanie pojemności informatycznego nośnika danych, na którym udostępniane są dane, z podaniem ilości i wielkości plików zawartych na tym nośniku;

8) nazwę i określenie wersji zastosowanego formatu zapisu danych oraz nazwę i określenie wersji oprogramowania oraz rodzaju sprzętu informatycznego, za pomocą którego będzie możliwe odtwarzanie udostępnionych danych;

9) szczegółowy opis zastosowanych nazw, skrótów i kodów pozwalających na interpretowanie danych;

10) opis struktury danych zapisanych na informatycznym nośniku danych;

11) opis zabezpieczeń i wykaz zastosowanych haseł lub kodów dostępu - w przypadku zastosowania zabezpieczeń dostępu do udostępnianych danych.

§ 6. Rozporządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

UZASADNIENIE

Projekt rozporządzenia Prezesa Rady Ministrów w sprawie sposobu przekazywania i udostępniania danych telekomunikacyjnych w przypadku upadłości operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych, stanowi wykonanie upoważnienia zawartego w art. 180a ust. 4 ustawy z dnia 16 lipca 2004 r, Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.).

Regulacja niniejsza związana jest z transpozycją 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.

Przepisy projektu rozporządzenia regulują sposób przekazywania Prezesowi Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UK.6", danych telekomunikacyjnych zgromadzonych prze* operatora publicznej sieci telekomunikacyjnej lub dostawcę, publicznie dostępnych usług- telekomunikacyjnych - w przypadku ogłoszenia jego upadłości. Zaprojektowane regulacje określają format przekazywanych danych oraz dodatkowe informacje, które powinny być przekazane wraz z danymi w celu umożliwienia odczytywania przekazywanych danych. Rozporządzenie określa także sposób dokumentowania procesu przekazywania danych.

Rozporządzenie określa również sposób udostępniania danych telekomunikacyjnych przez Prezesa UKJi podmiotom, o których mowa w arl. I80a ust. 1 pkt 3 ustawy - Prawo telekomunikacyjne. W tym przypadku również określono formę przekazywania danych oraz sposób dokumentowania przypadków udostępniania danych.

Przedmiotowy projekt nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Przedmiotowy projekt jest zgodny z prawem unijnym.

OCENA SKUTKÓW REGULACJI

I. Podmioty, nu które oddziałuje rozporządzenie.

Podmiotami, do których adresowane jest rozporządzenie są operatorzy publicznych sieci telekomunikacyjnej i dostawcy publicznie dostępnych usług telekomunikacyjnych, po ogłoszeniu ich upadłości, Prezes UK..E oraz podmioty uprawnione, o których mowa w art. 180a ust. 1 pkt 3 ustawy- Prawo telekomunikacyjne,

II. Konsultacje społeczne.

W ramach konsultacji społecznych projekt będzie przedstawiony izbom zrzeszającym przedsiębiorców telekomunikacyjnych. Zgłoszone uwagi zostaną, wykorzystane w trakcie prac nad niniejszym projektem.

III. Wpływ na sektor finansów publicznych, w tym nn budżet państwa i budżet samorządu terytorialnego.

Wejście w życie rozporządzenia spowoduje dodatkowe wydatki budżetowe Prezesa UKE. Przepis art. 180a ust. 3 ustawy Prawa telekomunikacyjne nakłada obowiązek zabezpieczenia danych telekomunikacyjnych w przypadku ogłoszenia upadłości operatora publicznych sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych, poprzez przekazanie ich Prezesowi UKE do dalszego przechowywania i ochrony oraz udostępniania uprawnionym podmiotom. Prezes UKE będzie musiał zatem zapewnić warunki organizacyjne i techniczne dla przyjęcia, bezpiecznego przechowywania oraz udostępniania danych telekomunikacyjnych uprawnionym podmiotom. Udostępnianie danych wymagać będzie dokonywania odczytu danych oraz ich przeszukiwania w zakresie wskazanym przez uprawnione podmioty, zainteresowane udostępnieniem danych. Z uwagi na to, że przepisy rozporządzenia są nową regulacją i brak jest w tym względzie jakichkolwiek doświadczeń, trudne jest określenie skali obciążeń finansowych, które powstaną po wejściu ich w życie. Przede wszystkim nie jest możliwe do oszacowania jaką skalę będzie mieć proces przekazywania danych i ilu podmiotów będzie dotyczyć. Niezbędne jest jednak przygotowanie sprzętu informatycznego dedykowanego do odczytu i przygotowywania danych do udostępnienia oraz zapewnienie w tym względzie odpowiednio przygotowanego personelu. Szacowane koszty minimalne wyniosą ok. 200 tyś zl. Powyższy szacunek nie dotyczy kosztów eksploatacyjnych i materiałowych związanych z udostępnianiem danych uprawnionym podmiotom.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na budżet samorządu terytorialnego.

IV. Wpływ regulacji na rynek pracy.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na rynek pracy.

V. Wpływ regulacji nu konkurencyjność wewnętrzną i zewnętrzną gospodarki.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na konkurencyjność gospodarki i przedsiębiorczość.

VI. Wpływ regulacji na sytuację i rozwój regionalny.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na sytuację i rozwój regionalny,

VII. Zgodność z prawem Unii Europejskiej.

Przedmiot projektowanego aktu prawnego nie jest objęły jest zakresem prawa Unii Europejskiej.

Projekt

ROZPORZĄDZENIE MINISTRA INFRASTRUKTURY[1)]
z dnia

w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania

Na podstawie art. 180c ust. 2 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[2)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) szczegółowy wykaz danych niezbędnych do:

   a) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego inicjującego połączenie,

   b) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego, do którego kierowane jest połączenie,

   c) określenia daty i godziny połączenia oraz czasu jego trwania,

   d) określenia rodzaju połączenia telefonicznego,

   e) określenia lokalizacji telekomunikacyjnego urządzenia końcowego używanego w ruchomej publicznej sieci telefonicznej, dotyczącej połączenia lub próby uzyskania połączenia;

2) rodzaje operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania danych, o których mowa w pkt 1.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) czas CET - czas środkowoeuropejski;

[1)] Minister Infrastruktury kieruje działem administracji rządowej - łączność, na podstawie § 1 ust. 2 pkt 3 rozporządzenia Prezesa Rady Ministrów z dnia 16 listopada 2007 r. w sprawie szczegółowego zakresu działania Ministra Infrastruktury (Dz. U. Nr 216, poz. 1594).
[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556 oraz z 2008 r. Nr 17, poz. 101.

2) numer IMSI - międzynarodowy numer przydzielony do każdej karty identyfikującej użytkownika w ruchomej publicznej sieci telefonicznej;

3) numer IMEI - indywidualny numer identyfikujący telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej;

4) MMC (Mobile Country Codę) - identyfikator kraju, w którym znajduje się ruchoma publiczna sieć telefoniczna;

5) MNC (Mobile Network Codę) - identyfikator ruchomej publicznej sieci telefonicznej;

6) numer MSISDN - numer przydzielony abonentowi ruchomej publicznej sieci telefonicznej;

7) stacja BTS - urządzenie łączące telekomunikacyjne urządzenie końcowe używane w ruchomej publicznej sieci telefonicznej z częścią stałą tej sieci.

§ 3. W stacjonarnej publicznej sieci telefonicznej:

1) dane, o których mowa w § 1 pkt 1 lit. a, obejmują:

   a) numer użytkownika końcowego inicjującego połączenie,

   b) imię i nazwisko użytkownika końcowego inicjującego połączenie albo jego nazwę,

   c) adres użytkownika końcowego inicjującego połączenie,

   d) miejsce zainstalowania telekomunikacyjnego urządzenia końcowego, z którego inicjowano połączenie;

2) dane, o których mowa w § 1 pkt 1 lit. b, obejmują:

   a) numer użytkownika końcowego, do którego kierowane jest połączenie,

   b) numer użytkownika końcowego, do którego przekierowane zostało połączenie,

   c) imię i nazwisko użytkownika końcowego, do którego kierowane jest połączenie albo jego nazwę,

   d) imię i nazwisko użytkownika końcowego, do którego przekierowane zostało połączenie albo jego nazwę,

   e) adres użytkownika końcowego, do którego kierowane jest połączenie,

   f) adres użytkownika końcowego, do którego przekierowane zostało połączenie,

g) miejsce zainstalowania telekomunikacyjnego urządzenia końcowego, do którego kierowane jest połączenie, h) miejsce zainstalowania telekomunikacyjnego urządzenia końcowego, do którego przekierowane zostało połączenie;

3) dane, o których mowa w § 1 pkt 1 lit. c, obejmują:

a) datę i godzinę rozpoczęcia połączenia zgodnie z czasem CET, z dokładnością do 1 sekundy,

b) czas trwania połączenia z dokładnością do 1 sekundy;

4) dane, o których mowa w § 1 pkt 1 lit. d, obejmują określenie rodzaju usługi telekomunikacyjnej, z której skorzystał użytkownik końcowy, a w szczególności połączenia głosowego, transmisji danych lub przesłania wiadomości tekstowych.

§ 4. W ruchomej publicznej sieci telefonicznej:

1) dane, o których mowa w § 1 pkt 1 lit. a, obejmują:

a) numer MSISDN użytkownika końcowego inicjującego połączenie,

b) imię i nazwisko użytkownika końcowego inicjującego połączenie lub jego nazwę,

c) adres użytkownika końcowego inicjującego połączenie, a w przypadku usługi przedpłaconej, datę i godzinę początkowej aktywacji usługi przedpłaconej przez użytkownika końcowego inicjującego połączenie, zgodnie z czasem CET, z dokładnością do 1 sekundy oraz współrzędne geograficzne lokalizacji stacji BTS, z której dokonano aktywacji,

d) numer IMSI użytkownika końcowego inicjującego połączenie,

e) numer IMEI urządzenia końcowego inicjującego połączenie;

2) dane, o których mowa w § 1 pkt 1 lit. b, obejmują:

a) numer MSISDN użytkownika końcowego, do którego kierowane jest połączenie,

b) numer MSISDN użytkownika końcowego, do którego przekierowane zostało połączenie,

c) imię i nazwisko lub nazwa użytkownika końcowego, do którego kierowane jest połączenie,

d) imię i nazwisko lub nazwa użytkownika końcowego, do którego przekierowane zostało połączenie,

e) adres użytkownika końcowego, do którego kierowane jest połączenie,

f) adres użytkownika końcowego, do którego przekierowane zostało połączenie,

g) numer IMSI użytkownika końcowego, do którego kierowane jest połączenie,

h) numer IMSI użytkownika końcowego, do którego przekierowane zostało połączenie,

i) numer IMEI urządzenia końcowego, do którego kierowane jest połączenie,

j) numer IMEI urządzenia końcowego, do którego przekierowane zostało połączenie,

k) w przypadku usługi przedpłaconej datę i godzinę początkowej aktywacji usługi przedpłaconej przez użytkownika końcowego, do którego kierowane jest połączenie lub do którego przekierowane zostało połączenie, zgodnie z czasem CET, z dokładnością do 1 sekundy oraz współrzędne geograficzne lokalizacji stacji BTS, z której dokonano aktywacji;

3) dane, o których mowa w § 1 pkt 1 lit. c, obejmują:

a) datę i godzinę rozpoczęcia połączenia zgodnie z czasem CET, z dokładnością do 1 sekundy,

b) czas trwania połączenia z dokładnością do 1 sekundy;

4) dane, o których mowa w § 1 pkt 1 lit. d, obejmują określenie rodzaju usługi telekomunikacyjnej, z której skorzystał użytkownik końcowy, a w szczególności, połączenia głosowego, transmisji danych, przesłania krótkiej wiadomości tekstowej, rozszerzonej wiadomości tekstowej, wiadomości multimedialnej;

5) dane, o których mowa w § 1 pkt 1 lit. e, obejmują:

a) współrzędne geograficzne stacji BTS, w obszarze której znajdowało się telekomunikacyjne urządzenie końcowe użytkownika końcowego inicjującego połączenie w czasie inicjowania połączenia, a gdy użytkownik inicjujący połączenie znajdował się poza granicami kraju identyfikator kraju (MCC) i identyfikator ruchomej publicznej sieci telefonicznej (MNC), w której zainicjowano połączenie,

b) współrzędne geograficzne stacji BTS, w obszarze której znajdowało się telekomunikacyjne urządzenie końcowe używane przez użytkownika końcowego, do którego kierowane jest połączenie, w czasie rozpoczęcia odbioru tego połączenia, a gdy użytkownik końcowy wywoływany znajdował się poza granicami kraju identyfikator kraju (MCC) i identyfikator ruchomej publicznej sieci telefonicznej (MNC), do której zostało skierowane połączenie.

§ 5. Dostawca publicznie dostępnych usług telekomunikacyjnych świadczonych w stacjonarnej publicznej sieci telefonicznej i operator stacjonarnej publicznej sieci telefonicznej - do której podłączone jest urządzenie telekomunikacyjne użytkownika końcowego:

1) inicjującego połączenie - zatrzymuje i przechowuje dane, o których mowa w § 3 pkt 1, pkt 2 lit. a,pkt3, pkt4;

2) do którego kierowane jest połączenie - zatrzymuje i przechowuje dane, o których mowa w § 3 pkt 1 lit. a, pkt 2 lit. a - c, e, g, pkt 3;

3) do którego przekierowane zostało połączenie - zatrzymuje dane, o których mowa w § 3 pkt 1 lit. a, pkt 2 lit. a, b, d, f, h, pkt 3.

§ 6. Dostawca publicznie dostępnych usług telekomunikacyjnych świadczonych w publicznej ruchomej sieci telefonicznej i operator ruchomej publicznej sieci telefonicznej - do której podłączone jest urządzenie telekomunikacyjne użytkownika końcowego:

1) inicjującego połączenie - zatrzymuje i przechowuje dane, o których mowa w § 4 pkt 1, pkt 2 lit. a, pkt 3, pkt 4, pkt 5 lit. a;

2) do którego kierowane jest połączenie - zatrzymuje i przechowuje dane, o których mowa w § 4 pkt 1 lit. a, pkt 2 lit. a -c, e, g, i, k, pkt 3, pkt 5 lit. b;

3) do którego przekierowane zostało połączenie - zatrzymuje dane, o których mowa w § 4 pkt 1 lit. a, pkt 2 lit. a, b, d, f, h, j, k, pkt 3.

§ 7. Rozporządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

MINISTER INFRASTRUKTURY

W POROZUMIENIU

MINISTER SPRAW WEWNĘTRZNYCH

I ADMINISTRACJI

UZASADNIENIE

Projekt rozporządzenia Ministra Infrastruktury w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania, stanowi wykonanie upoważnienia zawartego w art. 180c ust. 2 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.).

Regulacja niniejsza wynika z konieczności transpozycji przepisów 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.

Zgodnie z w/w Dyrektywą operator publicznej sieci telekomunikacyjnej i dostawca publicznie dostępnych usług telekomunikacyjnych obowiązany jest do zatrzymywania i przechowywania przez okres od 6 do 24 miesięcy niektórych danych generowanych w sieci telekomunikacyjnej dotyczących zarówno połączeń zrealizowanych, jak i nieudanych prób połączeń.

W związku ze skorzystaniem przez Polskę z odroczenia terminu transpozycji przepisów w/w Dyrektywy w zakresie retencji danych związanych z dostępem do Internetu, telefonią internetową i internetową pocztą elektroniczną, przedmiotowa regulacja odnosi się jedynie do tych przepisów dyrektywy, w których jest mowa o usługach telekomunikacyjnych realizowanych w stacjonarnych i ruchomych publicznych sieciach telefonicznych.

Przedmiotowe rozporządzenie określa szczegółowy wykaz danych objętych obowiązkiem zatrzymywania, przechowywania, ochrony i udostępniania oraz rodzaje operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania.

Przedmiotowy projekt nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Przedmiotowy projekt jest zgodny z prawem unijnym.

OCENA SKUTKÓW REGULACJI

I. Podmioty, na które oddziałuje rozporządzenie.

Podmiotami, do których adresowane jest rozporządzenie są operatorzy publicznych sieci telekomunikacyjnej i dostawcy publicznie dostępnych usług telekomunikacyjnych oraz podmioty uprawnione, zgodnie z przepisami ustawy - Prawo telekomunikacyjne, do dostępu do danych podlegających obowiązkowemu zatrzymywaniu i przechowywaniu.

II. Konsultacje społeczne.

W ramach konsultacji społecznych projekt będzie przedstawiony izbom zrzeszającym przedsiębiorców telekomunikacyjnych. Zgłoszone uwagi zostaną wykorzystane w trakcie prac nad niniejszym projektem.

III. Wpływ na sektor finansów publicznych, w tym na budżet państwa i budżet samorządu terytorialnego.

Wejście w życie rozporządzenia nie będzie miało wpływu na budżet państwa ani budżet samorządu terytorialnego.

IV. Wpływ regulacji na rynek pracy.

Wejście w życie powyższego rozporządzenia będzie miało wpływ na rynek pracy. Wprowadzenie obowiązku bezwzględnego zatrzymywania danych przez operatorów publicznej sieci telekomunikacyjnej i dostawców publicznie dostępnych usług telekomunikacyjnych będzie generować istotne obciążenia finansowe po stronie w/w podmiotów. Z informacji zebranych podczas procesu negocjacji 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 wynika, że :

dostawcy publicznie dostępnych usług telekomunikacyjnych realizowanych w stacjonarnej publicznej sieci telefonicznej, świadczący usługę telekomunikacyjną użytkownikowi końcowemu i operatorzy stacjonarnej publicznej sieci telefonicznej, do której podłączone jest urządzenie telekomunikacyjne użytkownika końcowego, posiadający kilkadziesiąt tysięcy abonentów lub zakończeń sieci - poniosą koszty dodatkowe w wysokości ok. 2 min zł, w tym: na zapewnienie rejestrowania nieudanych prób połączeń ok. 1 min zł, na rozbudowę systemów IT do przechowywania danych ok. 1 min zł. Powyższe wyliczenie nie

obejmuje kosztów eksploatacji urządzeń do zatrzymywania i przechowywania danych oraz kosztów osobowych;

dostawcy publicznie dostępnych usług telekomunikacyjnych realizowanych w ruchomej publicznej sieci telefonicznej świadczący usługę telekomunikacyjną użytkownikowi końcowemu i operatorzy ruchomej publicznej sieci telefonicznej, do której podłączone jest urządzenie telekomunikacyjne użytkownika końcowego - poniosą koszty dodatkowe rzędu kilkudziesięciu min zł, w tym na inwestycje związane z rozbudową systemów zapisujących ok. 3 min zł, inwestycje związane ze zmianą systemów bilingowych ok. 2 min, inwestycje związane z rozbudową sprzętową systemu gromadzenia dzienników zdarzeń ok. 1 min. Największym obciążeniem jest konieczność gromadzenia informacji o nieudanych próbach połączeń. Aktualnie w ruchomej publicznej sieci telefonicznej połączenia niezrealizowane to aż około 65% wszystkich połączeń. Oznacza to trzykrotne zwiększenie ilości przetwarzanych i przechowywanych danych, które przez dostawców publicznie dostępnych usług telekomunikacyjnych nie są do niczego wykorzystywane. Skutkuje to pojawieniem się po ich stronie kosztu ok. 4,5 do 5 min zł. Ponadto istotne będą także koszty dostosowania systemów mediacyjnych do zmienionych formatów rekordów generowanych przez centrale.

V. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość.

Wejście w życie powyższego rozporządzenia będzie miało wpływ na konkurencyjność gospodarki z uwagi na dodatkowe koszty jakie poniosą operatorzy i dostawcy usług w związku z realizacją obowiązku zatrzymywania i przechowywania danych wskazanych w rozporządzeniu. Wprowadzone przepisy będą istotnie wpływać na działalność operatorów i dostawców usług posiadających mniej niż kilkadziesiąt tysięcy zakończeń sieci lub abonentów.

VI. Wpływ regulacji na sytuację i rozwój regionalny.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na sytuację i rozwój regionalny.

VII. Zgodność z prawem Unii Europejskiej.

Przedmiot projektowanego aktu prawnego objęty jest zakresem prawa Unii Europejskiej i stanowi transpozycję przepisów 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, do krajowego systemu prawnego.

Projekt

ROZPORZĄDZENIE
MINISTRA INFRASTRUKTURY[1)]
z dnia

w sprawie wzoru formularza służącego do przekazywania przez przedsiębiorcę telekomunikacyjnego Prezesowi Urzędu Komunikacji Elektronicznej informacji dotyczących udostępniania danych

Na podstawie art. 180g ust. 3 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[2)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa wzór formularza służącego do przekazywania przez przedsiębiorcę telekomunikacyjnego Prezesowi Urzędu Komunikacji Elektronicznej informacji o:

1) liczbie przypadków, w których organom, o których mowa w art. 180a ust. 1 pkt 3 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne, zwanej dalej „ustawą", udostępniono dane zgodnie z przepisami ustawy;
2) czasie, jaki upłynął między datą zatrzymania danych a datą złożenia przez podmioty, o których mowa w art. 180a ust. 1 pkt 3 ustawy, wniosku lub ustnego żądania o udostępnienie danych;
3) przypadkach, w których wniosek lub ustne żądanie, o których mowa w pkt 2, nie mógł być zrealizowany.

§ 2. Wzór formularza, o którym mowa w § 1, stanowi załącznik do rozporządzenia.

§ 3. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER INFRASTRUKTURY

[1)] Minister Infrastruktury kieruje działem administracji rządowej - łączność, na podstawie § 1 ust. 2 pkt 3 rozporządzenia Prezesa Rady Ministrów z dnia 16 listopada 2007 r. w sprawie szczegółowego zakresu działania Ministra Infrastruktury (Dz. U. Nr 216, poz. 1594).

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556 oraz z 2008 r. Nr 17, poz. 101.

UZASADNIENIE

Projekt rozporządzenia Ministra Infrastruktury w sprawie wzoru formularza służącego do przekazywania informacji dotyczących udostępniania danych stanowi wykonanie upoważnienia zawartego w art. 180g ust. 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.), zwanego dalej „ustawą".

Regulacja niniejsza wynika z konieczności transpozycji do polskiego prawa przepisów 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 zmieniającej dyrektywę 2002/58/WE, a w szczególności art. 10 tej Dyrektywy, nakładającego na państwa członkowskie obowiązek przekazywania corocznie Komisji Europejskiej statystyki na temat zatrzymywania danych generowanych lub przetwarzanych w ramach świadczenia ogólnie dostępnych usług łączności elektronicznej lub udostępniania sieci komunikacji publicznej. Statystyki takie powinny obejmować:

- przypadki, w których właściwym organom udzielone zostały informacje zgodnie z mającym zastosowanie prawem krajowym,
- czas, jaki upłynął między datą zatrzymania danych a datą wniosku o przekazanie danych złożonego przez właściwy organ,
- przypadki, w których wnioski o dane nie mogły zostać zrealizowane.

W przepisie art. 180g ust. 2 ustawy Prezes Urzędu Komunikacji Elektronicznej został wskazany jako organ przekazujący Komisji Europejskiej powyższe informacje. Informacje te będą opracowywane w oparciu o informacje przekazywane Prezesowi przez operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych. Przedmiotowe rozporządzenie określa wzór formularza służącego do przekazywania Prezesowi Urzędu Komunikacji Elektronicznej informacji o udostępnianych danych przez operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych.

Przedmiotowy projekt nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Przedmiotowy projekt jest zgodny z prawem unijnym.

OCENA SKUTKÓW REGULACJI

I. Podmioty, na które oddziałuje rozporządzenie

Podmiotami, do których adresowane jest rozporządzenie są operatorzy publicznej sieci telekomunikacyjnej i dostawcy publicznie dostępnych usług telekomunikacyjnych oraz Prezes Urzędu Komunikacji Elektronicznej.

II. Konsultacje społeczne

W ramach konsultacji społecznych projekt będzie przedstawiony izbom zrzeszającym przedsiębiorców telekomunikacyjnych. Zgłoszone uwagi zostaną wykorzystane w trakcie prac nad niniejszym projektem.

III. Wpływ na sektor finansów publicznych, w tym na budżet państwa i budżet samorządu terytorialnego.

Wejście w życie rozporządzenia nie będzie miało wpływu na budżet państwa i budżet samorządu terytorialnego

IV. Wpływ regulacji na rynek pracy.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na rynek pracy.

V. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na konkurencyjność gospodarki.

VI. Wpływ regulacji na sytuację i rozwój regionalny.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na sytuację i rozwój regionalny.

VII. Zgodność z prawem Unii Europejskiej.

Przedmiot projektowanego aktu prawnego objęty jest zakresem prawa Unii Europejskiej. Projekt określa wzór formularza służącego do przekazywania informacji Prezesowi Urzędu Komunikacji Elektronicznej, które następnie będą wykorzystywane przez Prezesa do sporządzenia informacji dla Komisji Europejskiej - zgodnie z art. 10 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 zmieniającej dyrektywę 2002/5 8 /WE.

Załącznik
do rozporządzenia Ministra Infrastruktury
z dnia. .....2008 r. (poz .....)

Informacja
dotycząca udostępniania danych
za rok .....

Nazwa przedsiębiorcy telekomunikacyjnego:

Numer w rejestrze przedsiębiorców telekomunikacyjnych:

Lp.	Nazwa podmiotu wnioskującego o udostępnienie danych	Sposób realizacji wniosku		Liczba wniosków																								Razem
					Czas, jaki upłynął między datą zatrzymania danych a datą złożenia wniosku o ich udostępnienie (w miesiącach)																								
				X*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	>24	
1.		Udostępniono dane																										
		Nie udostępniono danych z powodu	braku dostępu[2)]																									
			utraty																									
			zniszczenia ze względu na upływ terminu, o którym mowa wart. 180a ust. 1 pkt 2 ustawy z dnia 16 lipca 2004r. - Prawo telekomunikacyjne																									
			Inne[3)']																									
Ogółem																												

Objaśnienia:
[8]pole wypełnia się w sytuacji, gdy brak jest możliwości określenia czasu, jaki upłynął między datą zatrzymania danych a datą złożenia wniosku o ich udostępnienie; [2)] dotyczy wniosków o udostępnienie danych, które nie są dostępne przedsiębiorcy telekomunikacyjnemu i w związku z tym nie podlegają obowiązkowi zatrzymania na podstawie art. 180a ust. 1 pkt 1 ustawy z dnia 16 lipca 2004r. - Prawo telekomunikacyjne; ' należy wpisać powód nieudostępnienia danych.

Miejscowość i data sporządzenia informacji

Podpis osoby upoważnionej do reprezentowania przedsiębiorcy telekomunikacyjnego

12-10-tg

Projekt

ROZPORZĄDZENIE MINISTRA INFRASTRUKTURY

z dnia

w sprawie danych dotyczących infrastruktury telekomunikacyjnej eksploatowanej lub używanej przez przedsiębiorcę, niezbędnej do przygotowania systemów łączności na potrzeby obronne państwa

Na podstawie art. 180f ust. 3 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[2)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) szczegółowy zakres danych dotyczących infrastruktury telekomunikacyjnej eksploatowanej lub używanej przez przedsiębiorcę telekomunikacyjnego, niezbędnej do przygotowania systemów łączności na potrzeby obronne państwa, w tym systemu kierowania bezpieczeństwem narodowym;
2) formę i tryb dostarczania danych, o których mowa w pkt 1, oraz ich aktualizacji.

§2. 1. Dane, o których mowa w § 1 pkt 1, obejmują lokalizację infrastruktury telekomunikacyjnej eksploatowanej lub używanej przez przedsiębiorcę telekomunikacyjnego oraz jej charakterystykę.

2. Przedsiębiorca telekomunikacyjny dostarcza niezwłocznie dane, o których mowa w ust. 1, na żądanie Prezesa Urzędu Komunikacji Elektronicznej, w formie wypełnionych formularzy.

3. Ustala się wzory formularzy, o których mowa w ust. 2:

1) „Formularz 1 - Ogólne dane o infrastrukturze telekomunikacyjnej niezbędnej do przygotowania systemów łączności na potrzeby obronne państwa" - stanowiący załącznik nr 1 do rozporządzenia;
2) „Formularz 2 - Karta urządzenia telekomunikacyjnego" - stanowiący załącznik nr 2 do rozporządzenia.

4. Formularze, o których mowa w ust. 2, przedsiębiorca przekazuje na informatycznym nośniku danych, a w przypadku braku takiej możliwości w formie papierowej, z zachowaniem przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.).

[1)] Minister Infrastruktury kieruje działem administracji rządowej - łączność, na podstawie § 1 ust. 2 pkt 3 rozporządzenia Prezesa Rady Ministrów z dnia 16 listopada 2007 r. w sprawie szczegółowego zakresu działania Ministra Infrastruktury (Dz. U. Nr 216, poz. 1594).

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i poz. 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834 z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556 oraz z 2008r. Nr 17, poz. 101.

§3. 1. Przedsiębiorca telekomunikacyjny obowiązany jest do aktualizacji danych przekazanych do Prezesa Urzędu Komunikacji Elektronicznej, o których mowa w § 1 pkt 1.

2. Aktualizacji danych dokonuje się w formie:

1) Formularza 1, o którym mowa w § 2 ust. 3 pkt 1; oraz
2) Formularza 2, o którym mowa w § 2 ust. 3 pkt 2 - dla urządzenia telekomunikacyjnego, którego dotyczą zmiany

- w terminie 30 dni od dnia wystąpienia zmiany w danych przekazanych do Prezesa Urzędu Komunikacji Elektronicznej.

§ 4. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia

MINISTER INFRASTRUKTURY

UZASADNIENIE

Projekt rozporządzenia Ministra Infrastruktury w sprawie danych dotyczących infrastruktury telekomunikacyjnej eksploatowanej lub używanej przez przedsiębiorcę stanowi wykonanie upoważnienia zawartego w art. 180f ust. 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800).

Regulacja niniejsza zapewni uzyskanie danych niezbędnych do realizacji przepisów rozporządzenia Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa (Dz. U. nr 180, poz. 1855), zgodnie z którymi Prezes Urzędu Komunikacji Elektronicznej dokonuje analizy możliwości przedsiębiorców telekomunikacyjnych w zakresie ich wykorzystania na potrzeby obronne państwa oraz zapewnia utworzenie bazy danych o przedsiębiorcach telekomunikacyjnych, niezbędnej do przygotowania i wykorzystania obronnych systemów łączności.

Projektowane rozporządzenie umożliwi pozyskiwanie uzyskanie przez Prezesa Urzędu Komunikacji Elektronicznej danych niezbędnych do tworzenia takiej bazy oraz aktualizacji danych o wybranych elementach infrastruktury telekomunikacyjnej przedsiębiorców telekomunikacyjnych.

Dotychczas nie było narzędzia prawnego pozwalającego skutecznie pozyskiwać w/w dane. Wejście w życie przedmiotowego rozporządzenia umożliwi Prezesowi Urzędu Komunikacji Elektronicznej właściwe wykonywanie zadań w zakresie obronności.

Przedmiotowe rozporządzenie określa zakres danych dotyczących infrastruktury telekomunikacyjnej eksploatowanej lub używanej przez przedsiębiorcę oraz formę, tryb ich dostarczania i aktualizacji.

Przedmiotowy projekt nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

OCENA SKUTKÓW REGULACJI

I. Podmioty, **na które oddziałuje rozporządzenie.**

Podmiotami, do których adresowane jest rozporządzenie są przedsiębiorcy telekomunikacyjni oraz Prezes Urzędu Komunikacji Elektronicznej.

II. Konsultacje społeczne.

W ramach konsultacji społecznych projekt będzie przedstawiony izbom zrzeszającym przedsiębiorców telekomunikacyjnych. Zgłoszone uwagi zostaną wykorzystane w trakcie prac nad niniejszym projektem.

III. Wpływ na sektor fmansów publicznych, w tym **na budżet państwa i budżet samorządu** terytorialnego.

Wejście w życie rozporządzenia nie będzie miało wpływu na budżet państwa, budżet samorządu terytorialnego

IV. Wpływ regulacji na rynek pracy.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na rynek pracy.

V. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na konkurencyjność wewnętrzną i zewnętrzna gospodarki.

VI. Wpływ regulacji na sytuację i rozwój regionów.

Wejście w życie powyższego rozporządzenia nie będzie miało wpływu na sytuację i rozwój regionalny.

VII. Zgodność z prawem Unii Europejskiej.

Przedmiot projektowanego aktu prawnego nie jest objęty jest prawem Unii Europejskiej.

Załączniki do rozporządzenia Ministra Infrastruktury
z dnia ..... 2008 r. (Dz. U. Nr ..., poz. ...)
Załącznik nr 1

Formularz 1
Ogólne dane o infrastrukturze telekomunikacyjnej niezbędnej do przygotowania systemów łączności na potrzeby obronne państwa *

1	Wprowadzenie danych	
2	Aktualizacja danych	

3	Według stanu na dzień (dd mm rrrr)			

Podstawowe dane o przedsiębiorcy telekomunikacyjnym

Firma przedsiębiorcy lub nazwa innego podmiotu uprawnionego do wykonywania działalności gospodarczej na podstawie odrębnych przepisów

4	

Numer w rejestrze przedsiębiorców telekomunikacyjnych

5	

Lokalizacja infrastruktury telekomunikacyjnej przedsiębiorcy telekomunikacyjnego i jej ogólna charakterystyka

Lokalizacja urządzeń telekomunikacyjnych

kraj

6		

województwo(a)

7	dolnośląskie		powiaty	
8	kujawsko-pomorskie		powiaty	
9	lubelskie		powiaty	
10	lubuskie		powiaty	
11	łódzkie		powiaty	
12	małopolskie		powiaty	
13	mazowieckie		powiaty	
14	opolskie		powiaty	
15	podkarpackie		powiaty	
16	podlaskie		powiaty	
17	pomorskie		powiaty	
18	śląskie		powiaty	
19	świętokrzyskie		powiaty	
20	warmińsko-mazurskie		powiaty	
21	wielkopolskie		powiaty	
22	zachodniopomorskie		powiaty	

Liczba używanych lub eksploatowanych urządzeń telekomunikacyjnych:

23	spełniających kryteria dotyczące wydzielenia kanałów transmisyjnych oraz zasilania		
24	obsługiwanych		
25	podlegających obowiązkowej ochronie		
26	objętych umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Obrony Narodowej		
27	objętych umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Spraw Wewnętrznych i Administracji		

.....

Miejscowość, data i podpis osoby wypełniającej formularz

.....

Data i podpis osoby uprawnionej do reprezentowania przedsiębiorcy telekomunikacyjnego

Objaśnienia sposobu wypełniania

*** w formularzu należy ująć dane dotyczące urządzeń telekomunikacyjnych, które objęte są umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Obrony Narodowej lub Ministerstwa Spraw Wewnętrznych i Administracji albo posiadają zasoby transmisyjne umożliwiające wydzielenie minimum 4 kanałów 2Mbit/sek oraz źródło zasilania z rezerwą mocy minimum 10kVA . Dla każdego z urządzeń telekomunikacyjnych spełniających te wymagania należy wypełnić formularz 2 - Karta urządzenia telekomunikacyjnego i załączyć do formularza 1.**

Nr pola	Wskaźnik	Opis
1	Wprowadzenie danych	Jeżeli dane dotyczące infrastruktury telekomunikacyjnej dostarczane są po raz pierwszy należy wpisać znak **X**, w przypadku aktualizacji danych pole pozostawić niewypełnione.
2	Aktualizacja danych	Jeżeli formularz jest dokumentem aktualizującym dane o infrastrukturze telekomunikacyjnej należy wpisać znak **X**.
3	Według stanu na dzień	Należy wpisać datę wypełnienia formularza, odpowiednio w pola dzień, miesiąc, rok.
5	Numer w rejestrze przedsiębiorców telekomunikacyjnych	Należy wpisać numer w rejestrze przedsiębiorców telekomunikacyjnych, prowadzonym przez Prezesa Urzędu Komunikacji Elektronicznej.
6	kraj	Należy wpisać znak **X** jeżeli przedsiębiorca używa lub eksploatuje urządzenia telekomunikacyjne na obszarze całego kraju.
7	dolnośląskie	Jeżeli przedsiębiorca używa lub eksploatuje urządzenia telekomunikacyjne we wszystkich powiatach województwa wpisać znak **X** przy nazwie województwa. Jeżeli przedsiębiorca używa lub eksploatuje urządzenia telekomunikacyjne tylko w niektórych powiatach województwa w polu "powiaty" należy wpisać nazwy powiatów, na terenie których znajdują się te urządzenia.
8	kujawsko-pomorskie	
9	lubelskie	
10	lubuskie	
11	łódzkie	
12	małopolskie	
13	mazowieckie	
14	opolskie	
15	podkarpackie	
16	podlaskie	
17	pomorskie	
18	śląskie	
19	świętokrzyskie	
20	warmińsko-mazurskie	
21	wielkopolskie	
22	zachodniopomorskie	

23	Spełniających kryteria dotyczące wydzielenia kanałów transmisyjnych oraz zasilania	Należy wpisać łączną liczbę urządzeń telekomunikacyjnych, które posiadają zasoby transmisyjne umożliwiające wydzielenie minimum 4 kanałów 2Mbit/sek oraz źródło zasilania z rezerwą mocy minimum 10kVA.
24	Obsługiwanych	Należy wpisać liczbę urządzeń telekomunikacyjnych posiadających stałą obsługę przez całą dobę.
25	Podlegających obowiązkowej ochronie	Należy wpisać liczbę urządzeń telekomunikacyjnych, które zostały ujęte w ewidencji (prowadzonej przez właściwego wojewodę obszarów, obiektów i urządzeń podlegajacych obowiązkowej ochronie - zgodnie z art. 5 ust. 5 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2005 r. Nr 145, poz. 1221 z późn. zm.).
26	Objętych umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Obrony Narodowej	Należy wpisać liczbę urządzeń telekomunikacyjnych objetych umową na dostosowanie do współpracy z ruchomymi urządzenian telekomunikacyjnymi Ministerstwa Obrony Narodowej.
27	Objętych umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Spraw Wewnętrznych i Administracji	Należy wpisać liczbę urządzeń telekomunikacyjnych objętych umową na dostosowanie do współpracy z ruchomymi urządzenian telekomunikacyjnymi Ministerstwa Spraw Wewnętrznych i Administracji.

Załącznik nr 2

Formularz 2
Karta urządzenia telekomunikacyjnego

1	Wprowadzenie danych	
2	Aktualizacja danych	

3	Według stanu na dzień (dd mm rrrr)			

Podstawowe dane o przedsiębiorcy telekomunikacyjnym

Firma przedsiębiorcy lub nazwa innego podmiotu uprawnionego do wykonywania działalności gospodarczej na podstawie odrębnych przepisów

4	

Numer w rejestrze przedsiębiorców telekomunikacyjnych

5	

Dane o urządzeniu telekomunikacyjnym

Nazwa urządzenia telekomunikacyjnego

6	

Identyfikator urządzenia telekomunikacyjnego w systemie informatycznym przedsiębiorcy telekomunikacyjnego

7	

Nadana klauzula tajności dla informacji zawierających szczegółowe dane o urządzeniu telekomunikacyjnym

8	zastrzeżone	
9	poufne	
10	tajne	
11	ściśle tajne	

Czy urządzenie telekomunikacyjne jest

12	obsługiwane	
13	dzierżawione innemu przedsiębiorcy	
14	dzierżawione od innego przedsiębiorcy	

15	Data zakończenia eksploatacji lub używania urządzenia telekomunikacyjnego (dd mm rrrr)			

Lokalizacja urządzenia telekomunikacyjnego

Współrzędne geograficzne (w układzie odniesienia WGS 84 , format pozycji hddd mm' ss,s")

długość geograficzna	16	**E**		°		'		,	''
szerokość geograficzna	17	**N**		°		'		,	''

Adres

kraj	18	
województwo	19	
powiat	20	
gmina	21	
miejscowość	22	

ulica	23	
numer domu	24	
numer lokalu	25	
kod pocztowy	26	
poczta	27	
informacje dodatkowe	28	

Charakterystyka

29	Charakterystyka urządzenia telekomunikacyjnego, część opisowa

Czy urządzenie telekomunikacyjne podlega obowiązkowej ochronie ?

30	

Czy do urządzenia telekomunikacyjnego jest możliwość dojazdu z drogi publicznej pojazdem transportowym o masie całkowitej minimum 10 ton ?

31	

Czy w lokalizacji urządzenia telekomunikacyjnego jest możliwość rozwinięcia anten ?

32	

Czy w lokalizacji urządzenia telekomunikacyjnego znajduje się maszt antenowy z możliwością zamontowania dodatkowych elementów antenowych ?

33	

Czy istnieje możliwość wydzielenia w obiekcie, w którym znajduje się urządzenie telekomunikacyjne, oddzielnego pomieszczenia o powierzchni minimum 10 m²?

34	

Czy urządzenie telekomunikacyjne objęte jest umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi:

35	Ministerstwa Obrony Narodowej	
35	Ministerstwa Spraw Wewnętrznych i Administracji	

Czy urządzenie telekomunikacyjne spełnia wymagania w zakresie przygotowania przyłączy energetycznych i teletechnicznych ?

37	

Czy urządzenie telekomunikacyjne posiada przyłącze energetyczne:

38	trójfazowe, rezerwa mocy minimum 15kVA	
39	jednofazowe, rezerwa mocy minimum 10kVA	

Czy urządzenie telekomunikacyjne posiada zasilenie awaryjne:

40	z sieci energetycznej, przyłącze trójfazowe, rezerwa mocy minimum 10kVA	
41	z agregatów prądotwórczych, rezerwa mocy minimum 10kVA	

Czy urządzenie telekomunikacyjne ma zapewnione serwisowanie przez:

42	firmę zewnętrzną	
43	własny personel techniczny	

Jaki jest czas naprawy urządzenia telekomunikacyjnego w przypadku uszkodzeń:

44	powodujących całkowitą niesprawność urządzenia telekomunikacyjnego	
45	powodujących pogorszenie funkcjonalności	

Warunki podłączenia do urządzenia telekomunikacyjnego ruchomych urządzeń telekomunikacyjnych

46	Procedura realizacji podłączenia ruchomych urządzeń telekomunikacyjnych Ministerstwa Obrony Narodowej lub Ministerstwa Spraw Wewnętrznych i Administracji

.....

Miejscowość, data i podpis osoby wypełniającej formularz

.....

Data i podpis osoby uprawnionej do reprezentowania przedsiębiorcy telekomunikacyjnego

Objaśnienia sposobu wypełniania

Nr pola	Wskaźnik	Opis
1	Wprowadzenie danych	Jeżeli dane dotyczące urządzenia telekomunikacyjnego dostarczane są po raz pierwszy należy wpisać znak **X** , w przypadku aktualizacji danych pole pozostawić niewypełnione.
2	Aktualizacja danych	Jeżeli formularz jest dokumentem aktualizującym dane o urządzeniu telekomunikacyjnym należy wpisać znak **X**.
3	Według stanu na dzień	Należy wpisać datę wypełnienia formularza, odpowiednio w pola dzień, miesiąc, rok.
5	Numer w rejestrze przedsiębiorców telekomunikacyjnych	Należy wpisać numer w rejestrze przedsiębiorców telekomunikacyjnych, prowadzonym przez Prezesa Urzędu Komunikacji Elektronicznej.
6	Nazwa urządzenia telekomunikacyjnego	Należy wpisać pełną nazwę urządzenia telekomunikacyjnego charakteryzującą realizowane przez niego funkcje.
7	Identyfikator urządzenia telekomunikacyjnego w systemie informatycznym przedsiębiorcy telekomunikacyjnego	Należy wpisać numer identyfikujący urządzenie telekomunikacyjne w systemie informatycznym przedsiębiorcy telekomunikacyjnego.
8	Nadana klauzula tajności dla informacji zawierających szczegółowe dane o urządzeniu telekomunikacyjnym - zastrzeżone	Należy wpisać znak **X** w pole odpowiadajace nadanej klauzuli tajności.
9	Nadana klauzula tajności dla informacji zawierających szczegółowe dane o urządzeniu telekomunikacyjnym - poufne	
10	Nadana klauzula tajności dla informacji zawierających szczegółowe dane o urządzeniu telekomunikacyjnym - tajne	
11	Nadana klauzula tajności dla informacji zawierających szczegółowe dane o urządzeniu telekomunikacyjnym - ściśle tajne	
12	Czy urządzenie telekomunikacyjne jest obsługiwane ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne jest obsługiwane.
13	Czy urządzenie telekomunikacyjne jest dzierżawione innemu przedsiębiorcy ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne jest dzierżawione innemu przedsiębiorcy.
14	Czy urządzenie telekomunikacyjne jest dzierżawione od inego przedsiębiorcy ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne jest dzierżawione od innego przedsiębiorcy telekomunikacyjnego.
15	Data zakończenia eksploatacji lub używania urządzenia telekomunikacyjnego	Pole wypełnia się tylko w przypadku aktualizacji danych. Należy wpisać datę zakończenia używania lub eksloatacji urządzenia telekomunikacyjnego odpowiednio w pola, dzień - dd, miesiąc - mm, rok - rrrr.
16	długość geograficzna	Dane należy przedstawić w układzie odniesienia WGS 84 , format pozycji hddd mm' ss,s" (N 51 21' 28,7"). Miejsce pomiaru - wejście główne do obiektu budowlanego, w którym znajduje się urządzenie telekomunikacyjne, lub główna brama wjazdowa. Pomiaru należy dokonać przy użyciu GPS lub odczytać z mapy w skali nie mniejszej niż 1:25000. Zapis długości geograficznej wschodniej w przedziale od 14 stopni do 24 stopni 30 minut. Zapis szerokości geograficznej północnej z przedziału od 49 stopni do 55 stopni 30 minut.
17	szerokość geograficzna	
18	kraj	Miejsce gdzie znajduje się obiekt budowlany, w którym jest zainstalowane urządzenie telekomunikacyjne - dane należy wpisać we właściwe pola.
19	województwo	
20	powiat	
21	gmina	
22	miejscowość	
23	ulica	
24	numer domu	
25	numer lokalu	
26	kod pocztowy	

27	poczta	
28	informacje dodatkowe	Należy podać informacje uzupełniające w zakresie umożliwiającym zlokalizowanie urządzenia telekomunikacyjnego, szczególnie w przypadku jego ooddalenia od wskazanej w adresie miejscowości (nazwa fizjograficzna lub numer działki).
29	Charakterystyka urządzenia telekomunikacyjnego, część opisowa	Jako załącznik do formularza należy sporządzić charakterystykę urządzenia telekomunikacyjnego zawierającą szczegółowe dane techniczne i funkcjonalne oraz opis warunków dojazdu do obiektu, warunków zamocowania i rozwinięcia anten. Charakterystykę należy sporządzić w formacie pdf lub na oddzielnym arkuszu papieru oraz oznaczyć nazwą przedsiębiorcy telekomunikacyjnego, nazwą urządzenia lub jego identyfikatorem w systemie informatycznym przedsiębiorcy.
30	Czy urządzenie telekomunikacyjne podlega obowiązkowej ochronie ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne zostało ujęte w ewidencji (prowadzonej przez właściwego wojewodę) obszarów, obiektów i urządzeń podlegajacych obowiązkowej ochronie - zgodnie z art. 5 ust. 5 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2005 r. Nr 145, poz. 1221 z późn. zm.).
31	Czy do urządzenia telekomunikacyjnego jest możliwość dojazdu z drogi publicznej pojazdem transportowym o masie całkowitej minimum 10 ton ?	Należy wpisać znak **X** jeżeli do urządzenia telekomunikacyjnego jest możliwy dojazd z drogi publicznej dla pojazdów dwuśladowych o masie całkowitej minimum 10 ton, wysokości 3,5 m, szerokości 2,6 m, długości z przyczepą 11 m oraz promieniem skrętu większym niż 9 m.
32	Czy w lokalizacji urządzenia telekomunikacyjnego jest możliwość rozwinięcia anten ?	Należy wpisać znak **X** jeżeli w lokalizacji urządzenia telekomunikacyjnego jest możliwość rozwinięcia anten na polu o wymiarach 32 m x 32 m, o długości fidera antenowego 40 m i maksymalnej wysokości masztu 24 m.
33	Czy w lokalizacji urządzenia telekomunikacyjnego znajduje się maszt antenowy z możliwością zamontowania dodatkowych elementów antenowych ?	Należy wpisać znak **X** jeżeli w lokalizacji urządzenia telekomunikacyjnego znajduje się maszt antenowy z możliwością zamontowania dodatkowych elementów antenowych.
34	Czy istnieje możliwość wydzielenia w obiekcie, w którym znajduje się urządzenie telekomunikacyjne, oddzielnego pomieszczenia o powierzchni minimum 10 m^2 ?	Należy wpisać znak **X** jeżeli w obiekcie budowlanym, w którym znajduje się urządzenie telekomunikacyjne można wydzielić oddzielne pomieszczenie o powierzchni minimum 10 m^2 (wysokość 2,5 m) oraz zainstalować urządzenia w standardowych szafach 19 calowych. Pomieszczenie powinno mieć doprowadzone zasilanie 220V 50Hz i wolny przepust kablowy.
35	Czy urządzenie telekomunikacyjne objęte jest umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Obrony Narodowej ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne jest objętę umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Obrony Narodowej.
36	Czy urządzenie telekomunikacyjne objęte jest umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Spraw Wewnętrznych i Administracji ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne jest objęte umową na dostosowanie do współpracy z ruchomymi urządzeniami telekomunikacyjnymi Ministerstwa Spraw Wewnętrznych i Administracji.
37	Czy urządzenie telekomunikacyjne spełnia wymagania w zakresie przygotowania przyłączy energetycznych i teletechnicznych ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne posiada: 1) **przyłącze energetyczne wyposażone w:** - 2 gniazda ABL-17 - 32 A (minimalna moc zasilania 2x5,0 kVA, napięcie 230 +/- 5V, częstotliwość 50 +/- 1Hz, wykonane w obudowie IP 54 z szyną Cu dla PE); - skrzynkę rozdzielczą IP 54; - szynę Cu 100x30x5mm; - 2 jednofazowe liczniki energii elektrycznej E12-W ; - ochronniki przepięć; - przetwornicę 48/24V (AC/DC) do zasilania konwerterów K0-2g TRANSBIT (przy braku gwarantowanej sieci 230V). 2) **przyłącze teletechniczne zawierające:** - 2 styki elektryczne (PS 2) 2Mb,120 Ohm; - 2 styki optyczne (CTOS 976) 2Mb (światłowód wielomodowy w oknie 1300nm, moc nadajnika 1,2mW, czułość odbiornika -26dBm); - 2 konwertery K0-2g firmy TRANSBIT; - 2 złącza CTOS 976 z patchcordem światłowodowym.
38	Czy urządzenie telekomunikacyjne posiada przyłącze energetyczne trójfazowe, rezerwa mocy minimum 15kVA ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne posiada przyłącze energetyczne trójfazowe z rezerwą mocy minimum 15kVA.
39	Czy urządzenie telekomunikacyjne posiada przyłącze energetyczne jednofazowe, rezerwa mocy minimum 10kVA ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne posiada przyłącze energetyczne jednofazowe z rezerwą mocy minimum 10kVA.
40	Czy urządzenie telekomunikacyjne posiada zasilanie awaryjne z sieci energetycznej - przyłącze trójfazowe, rezerwa mocy minimum 10kVA ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne posiada zasilanie awaryjne z sieci energetycznej - przyłącze trójfazowe z rezerwą mocy minimum 10kVA
41	Czy urządzenie telekomunikacyjne posiada zasilanie awaryjne z agregatów prądotwórczych, rezerwa mocy minimum 10kVA ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne posiada zasilanie awaryjne z agregatów prądotwórczych z rezerwą mocy minimum 10kVA.
42	Czy urządzenie telekomunikacyjne ma zapewnione serwisowanie przez firmę zewnętrzną ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne ma zapewnione serwisowanie przez firmę zewnętrzną.
43	Czy urządzenie telekomunikacyjne ma zapewnione serwisowanie przez własny personel techniczny ?	Należy wpisać znak **X** jeżeli urządzenie telekomunikacyjne ma zapewnione serwisowanie przez własny personel techniczny.
44	Jak jest czas naprawy urządzenia telekomunikacyjnego w przypadku uszkodzeń powodujących całkowitą niesprawność urządzenia telekomunikacyjnego ?	Należy wpisać czas naprawy w godzinach dla uszkodzeń powodujących całkowitą niesprawność urządzenia telekomunikacyjnego lub przerwę w działaniu 25% funkcji podstawowych tego urządzenia.
45	Jak jest czas naprawy urządzenia telekomunikacyjnego w przypadku uszkodzeń powodujących pogorszenie funkcjonalności ?	Należy wpisać czas naprawy w godzinach dla uszkodzeń powodujących pogorszenie funkcjonalności lub wydajności urządzenia telekomunikacyjnego.
46	Procedura realizacji podłączenia ruchomych urządzeń telekomunikacyjnych Ministerstwa Obrony Narodowej lub Ministerstwa Spraw Wewnętrznych i Administracji	Jako załącznik do formularza należy sporządzić procedurę podłączenia ruchomych urządzeń telekomunikacyjnych Ministerstwa Obrony Narodowej lub Ministerstwa Spraw Wewnętrznych i Administracji. Procedurę należy sporządzić w formacie pdf lub na oddzielnym arkuszu papieru oraz oznaczyć nazwą przedsiębiorcy telekomunikacyjnego, nazwą urządzenia lub jego identyfikatorem w systemie informatycznym przedsiębiorcy. W przypadku, gdy procedury podłączenia będą takie same dla grupy urządzeń telekomunikacyjnych należy sporządzić dla tej grupy urządzeń jedną procedurę podając nazwy i identyfikatory wszystkich urządzeń, których procedura dotyczy.

Projekt

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia …….. 2008 r.

w sprawie określenia wymagań technicznych i eksploatacyjnych dla interfejsów umożliwiających wykonywanie przedsiębiorcom telekomunikacyjnym zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego

Na podstawie art. 182 ustawy z dnia 14 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z póz. zm.[1)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa wymagania techniczne i eksploatacyjne dla interfejsów, o których mowa w art. 179 ust. 4a ustawy z dnia 14 lipca 2004 r. – Prawo telekomunikacyjne, zwane dalej „ustawą", umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, o których mowa w art. 179 ust. 3 i art. 180d ustawy.

§ 2. 1. Określenia użyte w rozporządzeniu oznaczają:

1) Interfejs HI – styk między systemem operatora telefonii, a systemem uprawnionego podmiotu;
2) HI1 – styk administracyjny;
3) HI 2 – styk przesyłu danych skojarzonych;
4) HI 3 – styk przesyłu treści przekazu;
5) CC – treść przekazu;
6) CS – [Circuit Switched] dane skojarzone;
7) CRI – [Call Related Information] informacja dotycząca połączenia;
8) PS – [Packed Switched] transmisja pakietowa;
9) LEMF - systemem uprawnionego podmiotu umożliwiający dostęp do wybranych treści przekazów telekomunikacyjnych;
10) ADMF - systemem operatora telefonii ruchomej umożliwiający realizację dostępu do wybranych treści przekazów telekomunikacyjnych;

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82 poz. 556 oraz z 2008 r. Nr 17, poz. 101 i Nr ..., poz. ...

11) MSISDN - [Mobile Station International ISDN Number] miedzynarodowy numer abonenta sieci ISDN;

12) IMEI - [International Mobile Equipment Identity] miedzynarodowy numer identyfikacyjny terminala;

13) IMSI - [International Mobile Subscriber Identity] miedzynarodowy numer abonenta ruchomego IMSI;

14) LOGIN – nazwa użytkownika logującego się do sieci, używana w procesie jego uwierzytelnienia;

15) IP – [Internet Protocol] protokół internetowy;

16) ETSI – European Telekommunikations Standarts Institiute.

2. Pojęcia użyte w rozporządzeniu są tożsame ze standardami 3GPP i ETSI.

§ 3. 1. Interfejs HI jest w całości elektroniczny i zdalny.

2. Służy do dostarczania wybranych wyników przechwytywania w czasie rzeczywistym dla usług czasu rzeczywistego. Usługi, zawierające element zwłoki, takie jak usługi pocztowe mogą być dostarczane z uwzględnieniem opóźnienia w przekazywaniu wyników przechwytywania.

3. Interfejs jest dzielony na trzy styki HI-1, HI-2 oraz HI-3:

1) HI-1 – służy do przesyłania wiadomości administracyjnych: aktywacji, deaktywacji, modyfikacji zleceń objęcia monitoringiem konkretnego zakończenia sieci. Styk Hi-1 umożliwia obustronną transmisję sygnałów;

2) HI-2 – służy do przesyłu informacji skojarzonych z objętymi kontrolą operacyjną przekazami telekomunikacyjnymi oraz treści sms;

3) HI – 3 służy do przekazu treści monitorowanych przekazów.

§ 4. 1. Styk HI-1 powinien umożliwiać włączanie, modyfikacje i wyłączanie obiektów bez udziału pracowników przedsiębiorcy telekomunikacyjnego przez uprawnionych funkcjonariuszy uprawnionych podmiotów, z lokalizacji wskazanej przez uprawniony podmiot.

2. Szczegółowy opis techniczny styku HI-1 określa załącznik nr 1 do rozporządzenia.

§ 5. Jeżeli przedsiębiorca telekomunikacyjny stosuje w ramach świadczonych usług mechanizmy szyfrujące, to obowiązany jest udostępniać je podmiotom uprawnionym w formie rozszyfrowanej.

§ 6. Przekazywanie wyników przechwytywania odbywa się przez łącza stałe.

§ 7. Uprawniony podmiot może wyrazić zgodę na dopuszczenie udziału uprawnionych pracowników przedsiębiorcy telekomunikacyjnego przy włączaniu, modyfikacji i wyłączaniu obiektów. Zakres udziału pracowników operatora określa się w formie porozumienia stron, wskazując wymagania formalne co do sposobu dokumentowania czynności wykonanych przez pracowników operatora i dokumentowania faktu dostępu pracownika operatora do danych należących do uprawnionego podmiotu. Zawarcie porozumienia z jednym z uprawnionych podmiotów nie zwalnia operatora sieci telekomunikacyjnej od obowiązku przygotowania styku HI-1 dla pozostałych uprawnionych podmiotów, w sposób określony

w § 4.

§ 8. 1. W przypadku zawarcia porozumienia, o którym mowa w § 7, przedsiębiorcy telekomunikacyjnemu mogą być przekazane wyłącznie określone kategorie informacji:

1) numer wniosku;
2) data zatwierdzenia;
3) organ zatwierdzający;
4) czas na jaki została zarządzona kontrola operacyjna;
5) kryterium wyboru;
6) numer stacji końcowej lub zakończenia sieci.

2. Przekazywanie informacji następuje w formie elektronicznej przez uprawnione podmioty w sposób zapewniający bezpieczną transmisję i przechowywanie.

3. Porozumienie, o którym mowa w § 7, może dopuszczać przekazywanie zlecenia przez uprawnione podmioty przedsiębiorcy telekomunikacyjnemu, w formie dokumentacji papierowej.

4. W przypadku zawarcia porozumienia, o którym mowa w § 7, czas jaki upłynie od momentu otrzymania zlecenia do momentu faktycznego, technicznego włączenia monitoringu przez pracowników operatora, nie może być dłuższy niż:

1) w godzinach 8:00-16:00 – 30 minut;
2) w godzinach 16:01 – 07.59 - 1 godzina.

§ 9. 1. Interfejs HI w całości oparty jest na technologii IP.

2. W styku HI-3 dopuszcza się stosowanie n-kapsulacji E1 do IP.

3. Szczegółowe opisy techniczne styków HI-2 oraz HI-3 określają załączniki nr 2-4 do rozporządzenia.

§ 10. Komunikacja między systemem monitoringu przedsiębiorcy telekomunikacyjnego a systemem monitoringu uprawnionego podmiotu odbywa się z wykorzystaniem publicznych adresów IP i wskazanych portów. Nie stosuje się adresów i numerów portów przydzielanych w sposób dynamiczny.

§ 11. Szyfrowanie styku z LEMF będzie realizowane poza interfejsem HI na poziomie warstwy fizycznej łącza. Przedsiębiorca telekomunikacyjny zapewnia, na swój koszt, stworzenie warunków umożliwiających podmiotom uprawnionym instalację oraz eksploatację urządzeń szyfrujących w lokalizacji interfejsu, zapewnia też ich ochronę fizyczną i ustala z uprawnionymi podmiotami warunki serwisowania tych urządzeń.

§ 12. Interfejs danego systemu monitoringu przedsiębiorcy telekomunikacyjnego dostępny jest w jednym punkcie styku (lokalizacji) dla wszystkich uprawnionych podmiotów. Na potrzeby systemu redundantnego tworzy się zapasowy punkt styku.

§ 13. 1. Za harmonogram włączania i wyłączania obserwacji odpowiada system monitoringu LEMF uprawnionego podmiotu.

2. Wysyłanie zleceń aktywacji ma miejsce w chwili rzeczywistego uruchamiania monitoringu. Dopuszcza się możliwość wysyłania zleceń aktywacji z wyprzedzeniem. Wyprzedzenie należy uzgodnić na etapie uzgadniania zasad współpracy poprzez interfejs. Każde zlecenie aktywacji musi mieć określony czas zakończenia kontroli operacyjnej.

3. Odstęp czasu między rozpoczęciem a zakończeniem kontroli operacyjnej nie może przekroczyć ściśle określonej wartości wynikającej z przepisów prawa.

4. Przesunięcie chwili zakończenia obserwacji ponad ten czas możliwe jest tylko za pomocą zlecenia modyfikacji. Zmiana czasu rozpoczęcia monitoringu wymaga usunięcia poprzedniego zlecenia i włączenia nowego.

§ 14. System monitoringu operatora przesyła do systemu podmiotu uprawnionego informację o czasie faktycznego wykonania polecenia aktywacji/deaktywacji/modyfikacji, w przypadku błędu w trakcie wykonywania polecenia, przesyła informację o fakcie pojawienia się błędu lub braku możliwości wykonania polecenia.

§ 15. Zlecenie modyfikacji czasu trwania kontroli operacyjnej dotyczy jedynie czasu jej wyłączenia lub zmiany trybu online/offline. Zlecenie trybu online nie może powodować przerwania rejestracji i transmisji offline dla danego obiektu.

§ 16. System monitoringu operatora nie dokonuje ingerencji i interpretacji dostarczanych treści. Dla celów monitoringu online stosuje się kompresję mowy służącą optymalizacji wykorzystania istniejącego pasma.

§ 17. System monitoringu operatora, ze względu na możliwe awarie, gromadzi treści komunikatów i informacji z nimi związanych monitorowanych obiektów w buforze zapewniającym ich przechowywanie przez co najmniej 72 godziny. Interfejs HI przekazuje je bez zbędnej zwłoki do systemu monitoringu uprawnionego podmiotu. Po uzyskaniu potwierdzenia przekazania treści komunikatów i informacji z nimi związanych, system operatora usuwa je ze swoich zasobów.

§ 18. Przedsiębiorca telekomunikacyjny wyposaża swój system w urządzenie rejestrujące wszystkie działania podejmowane na styku HI-1. Rejestracja ta obejmuje polecenia aktywacji/deaktywacji/modyfikacji wydane przez akredytowanych w systemie przedsiębiorcy telekomunikacyjnego pracowników uprawnionego podmiotu lub operatora dla każdego LIID wraz z kryteriami wyboru i czasem trwania monitoringu.

§ 19. 1. W przypadku awarii urządzenia, o którym mowa w § 18, lub braku łączności pomiędzy systemem operatora a tym urządzeniem, system operatora uniemożliwia dokonanie wszelkiego rodzaju zmian na styku HI-1.

2. W przypadku opracowania procedury dokumentowania w formie papierowej czynności wykonywanych w trakcie trwania awarii urządzenia, o którym mowa w § 18, wymogu określonego w ust. 1 nie stosuje się.

§ 20. Przedsiębiorca telekomunikacyjny jest obowiązany do stworzenia szczególnych warunków ochrony urządzenia, o którym mowa w § 18, oraz przechowywanych w nim danych poprzez:

1) zapewnienie oddzielnego pomieszczenia posiadającego dodatkową ochronę fizyczną;
2) wydzielony system zasilania awaryjnego;
3) dostęp tylko komisyjny;
4) uniemożliwienie dokonania zatarcia lub modyfikacji informacji.

§ 21. W przypadku awarii elementów sieci operatora system wysyła do systemów uprawnionych podmiotów informację o fakcie awarii wraz z określeniem zasięgu awarii (numery central/stacji BTS objętych awarią) przesyłając jednocześnie do każdego z uprawnionych podmiotów informacje o numerach LIID objętych awarią , które znajdują się w jego dyspozycji.

§ 22. Po usunięciu awarii, system monitoringu operatora niezwłocznie przesyła informacje do systemu uprawnionego podmiotu o czasie trwania przerwy w przechwytywaniu

danych.

§ 23. Interfejs umożliwia przesyłanie wiadomości diagnostycznych pozwalających w szczególności na stwierdzenie czy połączenie między systemami jest aktywne.

§ 24. 1. Dane przekazywane za pośrednictwem interfejsów HI są obligatoryjnie zabezpieczane zgodnie z wymaganiami określonymi w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.).

2. Wymóg zabezpieczenia, o którym mowa w ust. 1, przekazów dokonywanych za pośrednictwem styków HI-2 i HI-3 wchodzi w życie po upływie 24 miesięcy od daty wejścia w życie rozporządzenia.

§ 25. Mechanizm podpisów elektronicznych ma zapewnić, że żądania, które sterują uruchomieniem kontroli korespondencji będą wprowadzane i przesyłane tylko przez uprawnione do tego osoby, oraz że każde żądanie można będzie jednoznacznie przypisać zlecającemu je użytkownikowi LEMF.

§ 26. 1. Formatem stosowanego podpisu elektronicznego żądań HI jest CMS (Cryptographics Message Syntax) zdefiniowany w RFC 3852. Na potrzeby stosowania podpisu elektronicznego wykorzystywane są certyfikaty X.509 w wersji 3 (z uwzględnieniem wymagań technicznych zawartych w rozporządzeniu wykonawczym do ustawy o podpisie elektronicznym) oraz infrastruktura klucza publicznego PKI.

2. Sposób i zakres informacji zabezpieczonych podpisem elektronicznym określa załącznik nr 5 rozporządzenia.

§ 27. Interfejs HI zapewnia w szczególności następujące kryteria wyboru identyfikujące obiekty obserwacji w sieciach telekomunikacyjnych stosownie do rodzaju sieci:

1) MSISDN;
2) IMSI;
3) numer IMEI;
4) LOGIN;
5) adres IP;
6) adres MAC.

§ 28. Usługi obsługiwane przez interfejs HI1 w szczególności obejmują:

1) GSM/UMTS CS - usługi oparte na komutacji łączy: audio, fax, modem, sms, video-połączenia;
2) GSM/UMTS PS - usługi oparte na komutacji pakietów: technologia IP;
3) PWLAN - usługę bezprzewodowej sieci IP;
4) XDSL - szerokopasmowy stacjonarny dostęp do Internetu.

§ 29. Struktura interfejsu powinna pozwalać na dodanie nowych kryteriów w miarę rozwoju usług i możliwości sieci w zakresie identyfikacji użytkowników.

§ 30. W celu identyfikacji obiektów monitorowanych w systemach przedsiębiorców telekomunikacyjnych wykorzystany jest numer LIID.

§ 31.W każdym przypadku numer LIID, dla danego kryterium wyboru, obejmuje tylko jedną usługę do monitorowania.

§ 32. Liczba monitorowanych zakończeń sieci dostępnych dla każdego z uprawnionych podmiotów:

1) 0,05% pojemności każdej centrali wchodzącej w skład sieci przedsiębiorcy, lub
2) 0,03% zakończeń sieci przedsiębiorcy, w których wykonywana jest działalność telekomunikacyjna podlegająca obowiązkowi wykonywania zadań

- z tym, że nie może być mniejsza niż trzy.

§ 33. Określenie składni numeru LIID:

1) pierwsze pole dla określenia uprawnionego podmiotu;
2) pola 2 i 3 – od 00 do 17 - organ wydający zarządzenie/wniosek;
3) pola 4 - 6 – numer kolejny wniosku;
4) pole 7 – oznaczenie kwartału wydania wniosku;
5) pola 8 i 9 – rok wydania wniosku;
6) pola 10 i 11 – jednostka dedykująca;
7) pole 12 – oznaczenie operatora;
8) pola 13 - 17 – numer kolejny włączenia.

§ 34. Komunikacja przesyłu danych:

1) interfejsy HI służą do przesyłania wiadomości administracyjnych (HI1), informacji skojarzonych (HI2) i treści monitorowanych przekazów (HI3); wykorzystują do tego szereg protokołów sieciowych różnych warstw, aby dostarczyć dane do określonego miejsca przeznaczenia w sieci;
2) warstwa fizyczna i warstwa sieciowa jest wspólna dla wszystkich interfejsów HI; poszczególne interfejsy HI są wspomagane przez protokoły wyższych warstw takich jak TCP, FTP czy ULIC;
3) urządzenia sieciowe na styku pomiędzy systemami przedsiębiorcy telekomunikacyjnego i uprawnionego podmiotu oferują warstwę fizyczną standardu Ethernet. do obsługi każdego z uprawnionych podmiotów przewidziany jest oddzielny interfejs Ethernet;
4) wybór protokołu, dostosowanie przesyłanych informacji oraz szyfrowanie sygnału na łączach WAN leży w gestii podmiotów uprawnionych, jedynym wymogiem jest, aby interfejs do operatora był standardu Ethernet;
5) interfejsy HI (HI1, HI2, HI3) wykorzystują do przesyłania danych w warstwie sieciowej protokół minimum IPv4; dla wszystkich interfejsów HI stosowana jest adresacja publiczna IP zarówno po stronie przedsiębiorcy telekomunikacyjnego, jak również uprawnionego podmiotu; na styku WAN do uprawnionych podmiotów wykorzystywana jest adresacja publiczna IP nadawana przez operatora, z maską 29 bitów.

§ 35. Interfejs HA-B służy do dostarczania przez przedsiębiorcę telekomunikacyjnego uprawnionym podmiotom danych, o których mowa w art. 180d ustawy.

§ 36. Interfejs jest w całości elektroniczny i zdalny, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy uprawnionym podmiotem a tym przedsiębiorcą.

§ 37. Prawidłowe działanie interfejsu zapewnia się przez zastosowanie obiegu dokumentacji czynności w formie elektronicznej.

§ 38. Komunikacja pomiędzy uprawnionym podmiotem a interfejsem przedsiębiorcy telekomunikacyjnego odbywa się za pośrednictwem łącz stałych.

§ 39. Przedsiębiorca telekomunikacyjny wyposaża swój system w urządzenie rejestrujące wszystkie działania podejmowane w systemie. Rejestracja ta obejmuje wszystkie zapytania złożone przez akredytowanych w systemie pracowników uprawnionego podmiotu lub operatora.

§ 40. 1. W przypadku awarii urządzenia, o którym mowa w § 39, system operatora odrzuca składane przez uprawnionych pracowników zapytania wysyłając jednocześnie informację o fakcie awarii.

2. W przypadku opracowania procedury dokumentowania w formie papierowej czynności wykonywanych w trakcie trwania awarii urządzenia, o którym mowa w § 39, wymogu określonego w ust. 1 nie stosuje się.

§ 41. Przedsiębiorca telekomunikacyjny jest obowiązany do stworzenia szczególnych warunków ochrony urządzenia, o którym mowa w § 39, oraz przechowywanych w nim danych poprzez:

1) wydzielony system zasilania awaryjnego;
2) dostęp tylko komisyjny;
3) uniemożliwienie dokonania zatarcia lub modyfikacji informacji.

§ 42. 1. Przedsiębiorca telekomunikacyjny obowiązany jest do budowy Interfejsu HI A-B lub modyfikacji istniejących urządzeń w sposób, który umożliwi przesyłanie danych i składanie zapytań w formacie XML. Szczegółowy opis stosowanego formatu określa załącznik nr 6.

2. Operatorzy, którzy stosują inny format niż określony w załączniku nr 6 do rozporządzenia, mogą go dalej stosować przy spełnieniu następujących warunków:

1) przekazania podmiotom uprawnionym na swój koszt narzędzia do konwersji danych do formatu określonego w załączniku nr 6 do rozporządzenia;
2) zastosowanie przez operatora innego formatu, niż określony w załączniku nr 6 do rozporządzenia, nie może utrudniać dostępu uprawnionych podmiotów, do pełnego katalogu danych, niż określony w art. 180d ustawy;
3) szczegółowe warunki organizacyjne i techniczne określone są w porozumieniu zawartym pomiędzy przedsiębiorcą telekomunikacyjnym a uprawnionym podmiotem.

3. W przypadku przedsiębiorców telekomunikacyjnych, którzy zasięgiem działania nie wykraczają poza obszar jednego powiatu lub posiadają mniej niż 100 tys. zakończeń sieci, dane o których mowa w art. 161 ustawy, mogą być przekazywane uprawnionym

podmiotom na nośnikach teleinformatycznych w sposób inny niż określony w załączniku nr 6 do rozporządzenia.

§ 43. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

59-10-aa

UZASADNIENIE

Rozporządzenie stanowi realizację upoważnienia ustawowego zawartego w art. 182 *ustawy z dnia 14 lipca 2004 r. – Prawo telekomunikacyjne* (Dz. U. Nr 171, poz. 1800, z późn. zm.), zgodnie z którym Rada Ministrów określi w drodze rozporządzenia wymagania techniczne i eksploatacyjne dla interfejsów, o których mowa w art. 179 ust. 4a ww. ustawy, umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, o którym mowa w art. 179 ust. 3 i w art. 180d tejże ustawy.

Kierując się zasadą minimalizacji nakładów przedsiębiorcy telekomunikacyjnego i podmiotów uprawnionych, opracowano przedmiotowy akt prawny, wskazujący wymagania techniczne i eksploatacyjne dla interfejsów jako jedną z możliwości wykonywania przez przedsiębiorców telekomunikacyjnych zadań i obowiązków na rzecz obronności i bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

W celu realizacji obowiązku określonego w art. 5 ustawy z dnia 7 lipca 2005 r. *o działalności lobbingowej w procesie stanowienia prawa* (Dz. U. Nr 169, poz. 1414) projekt przedmiotowego aktu prawnego zostanie zamieszczony na stronach podmiotowych Kancelarii Prezesa Rady Ministrów oraz Ministerstwa Spraw Wewnętrznych i Administracji w Biuletynie Informacji Publicznej.

Ze względu na konieczność rozstrzygnięcia potrzeby notyfikacji w świetle ustawy z dnia 12 września 2002 r. *o normalizacji* (Dz.U. Nr 169, poz. 1386) oraz rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. *w sprawie sposobu funkcjonowania krajowego systemu norm i aktów prawnych* (Dz. U. Nr 239, poz. 2039 z późn. zm.) projekt rozporządzenia powinien być przekazany ministrowi właściwemu do spraw gospodarki, jako krajowemu koordynatorowi systemu notyfikacji norm i aktów prawnych.

Projekt nie jest objęty zakresem prawa Unii Europejskiej.

OCENA SKUTKÓW REGULACJI

1. Podmioty, na które oddziałują projektowane regulacje.

Do podmiotów, na które oddziałują projektowane regulacje należą:

- przedsiębiorcy telekomunikacyjni wpisani do rejestru prowadzonego przez Urząd Komunikacji Elektronicznej,
- organy administracji rządowej,
- uprawnione podmioty tj. Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, organy kontroli skarbowej.

2. Konsultacje.

W ramach konsultacji społecznych planuje się przekazać projekt do:

- Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji,
- Polskiej Izby Komunikacji Elektronicznej,
- Polskiej Izby Informatyki i Telekomunikacji.

3. Wpływ regulacji na sektor finansów publicznych.

Wejście w życie projektowanego rozporządzenia nie spowoduje dodatkowych skutków finansowych dla budżetu państwa i budżetów jednostek samorządu terytorialnego.

4. Wpływ regulacji na rynek pracy.

Przyjęcie projektowanej regulacji nie będzie oddziaływać na rynek pracy.

5. Wpływ regulacji na konkurencyjność wewnętrzną i zewnętrzną gospodarki.

Przyjęcie uregulowań prawnych zaproponowanych w projekcie *ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw* oraz w projekcie przedmiotowego rozporządzenia wpłynie na realne obniżenie kosztów funkcjonowania przedsiębiorców telekomunikacyjnych w porównaniu z aktualnym stanem prawnym. Po pierwsze część kosztów przeniesiona jest na podmioty uprawnione, a porozumienia (umowy) kształtują faktyczny podział kosztów. W związku z powyższym regulacje te będą działać stymulująco na rozwój przedsiębiorczości telekomunikacyjnej. Proponowane regulacje nie mają wpływu na konkurencyjność gospodarki w zakresie rynku telekomunikacyjnego. Przedsiębiorcy telekomunikacyjni oraz podmioty uprawnione w świetle projektowanych przepisów Prawa telekomunikacyjnego mogą na podstawie odrębnych umów określić, iż warunki dostępu i utrwalania zapewnia się za pomocą interfejsów zlokalizowanych w miejscach obejmowanych przez sieć przedsiębiorcy telekomunikacyjnego. Umowa może określać współudział stron w kosztach zastosowania interfejsów. Biorąc pod uwagę autonomiczność woli stron przy kształtowaniu zobowiązań umownych nie ma praktycznych możliwości wskazania kosztów

realizacji zapisów rozporządzenia. Rozporządzenie reguluje jednocześnie wymagania techniczne i eksploatacyjne dla interfejsów umożliwiających uzyskiwanie przez podmioty uprawnione danych, o których mowa w art. 180d projektowanej ustawy. Z uwagi na fakt, że dane te będą niejednokrotnie obejmować tysiące pojedynczych rekordów. Konieczne jest aby dane te przekazywane były w postaci elektronicznej. Postać elektroniczna przekazywanych danych niesie ze sobą wiele korzyści. Są to miedzy innymi, łatwość archiwizacji danych, łatwe przeszukiwanie i analiza danych (z wykorzystaniem systemów informatycznych), łatwość przesyłania danych. Dlatego istnieje konieczność wskazania jednolitego dla wszystkich przedsiębiorców telekomunikacyjnych formatu danych, który mógłby być wykorzystywany do tego celu. Dodatkowo powinny istnieć ogólnodostępne narzędzia umożliwiające konwersje przesyłanych przez operatora danych do wymaganego formatu oraz pozwalające na tworzenie podmiotom uprawnionym aplikacji analizujących dane otrzymane w tym formacie. Formatem spełniającym powyższe wymagania jest XML. Jest on wspierany przez wiele systemów baz danych oraz istnieje wiele komercyjnych i darmowych narzędzi do jego generowania, weryfikowania i analizy. Dokumenty XML pozwalają także na szybkie zweryfikowanie ich poprawności.

60-10-aa

Załączniki
do rozporządzenia
Rady Ministrów
z dnia

Załącznik nr 1

Specyfikacja techniczna styku HI-1 interfejsu HI

1. Rodzaje Wiadomości HI1

Interfejs HI1 w swoich założeniach służyć ma do realizowania funkcji administracyjnych i jako taki przesyła i obsługuje wiadomości płynące w obu kierunku między LEMF a ADMF. Jeśli chodzi o wiadomości inicjowane przez LEMF (czyli wiadomości w kierunku z LEMF do ADMF) to są to głownie wiadomości mające na celu aktywację, modyfikacje lub deaktywację obserwacji. Możliwe jest również generowanie zapytań ze strony LEMF o listę obserwacji lub konkretną obserwację w celu sprawdzenia i/lub dokonania porównania baz danych po stronie LEMF i ADMF. Jeśli chodzi o wiadomości inicjowane przez ADMF (czyli wiadomości w kierunku z ADMF do LEMF) to mogą to być w szczególności informacje o początkach i końcach alarmów lub też notyfikacje pewnych zdarzeń. W obu kierunkach możliwe jest wysyłanie wiadomości testujących mających na celu sprawdzenie poprawnego funkcjonowania interfejsu HI1.

2. Kierunek z LEMF do ADMF

Szczegółowe definicje określające ten ruch zawarte są w specyfikacji ASN.1 Interfejsu HI1: H1LEMFOperations.

Hello

Hello – jest wiadomością testową umożliwiającą stronie LEMF sprawdzenie poprawności działania interfejsu HI1.

HELLO		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
Version	ENUMERATED	wersja protokołu (1)
Request	CHOICE	typ zapytania (1 – simpleRequest)
simpleRequest	CHOICE	rodzaj zapytania (1 - **helloRequest**)
Message	UTF8String	tekst

Aktywacja

Szczegółowa definicja w UnsignedRequestDetail

Activate – jest wiadomością przenoszącą parametry umożliwiające stronie ADMF założenie żądanej przez LEMF obserwacji celu.

ACTIVATE		
PARAMETR		*OPIS*
Version	ENUMERATED	wersja protokołu (1)
Request	CHOICE	typ zapytania (2 – signedRequest)
Time	TimeStamp	godzina i data wystawienia zlecenia aktywacji
Command	CHOICE	typ polecenia (1- **Activate**)
Liid	OCTET STRING	format: LEAID+TARGET (SEQ), 17 znaków ASCII
Target	CHOICE	kryterium monitorowania i jego wartość [1)]
startTimestamp	TimeStamp	godzina i data aktywacji celu
stopTimestamp	TimeStamp	godzina i data dezaktywacji celu
service	CHOICE	rodzaj żądanej usługi [2)]
monitoringType	ENUMERATED	aktywacja tylko dla IRI lub IRI+CC [3)]

onlineMonitoring	BOOLEAN	dla serwisu CircuitSwitchd wybór dodatkowego typu monitorowania online
forwardingAddress	PrintableString	opcjonalnie (występuje tylko dla service=CircuitSwitched); numer przekierowania dla voice online (sipURL)

[1)] target

1 – MSISDN

2 – IMSI

3 – IMEI

4 – login

[2)] service

1 – CircuitSwitched

2 – PacketSwitched

3 – WIFI

4 – DSL

[3)] monitoringType

1 – iri

2 - iriCC

Dezaktywacja

Szczegółowa definicja w UnsignedRequestDetail

Deactivate – jest wiadomością przenoszącą parametry umożliwiające stronie ADMF wyłączenie (deaktywację) żądanej przez LEMF obserwacji celu.

MODIFICATE		
PARAMETR		*OPIS*
version	ENUMERATED	wersja protokołu (1)
request	CHOICE	typ zapytania (2 – signedRequest)
time	TimeStamp	godzina i data wystawienia zlecenia aktywacji
Command	CHOICE	typ polecenia (2 – **Deactivate**)
liid	OCTET STRING	format: LEAID+TARGET (SEQ), 17 znaków ASCII

Modyfikacja

Szczegółowa definicja w UnsignedRequestDetail

Modificate – jest wiadomością przenoszącą parametry umożliwiające stronie ADMF modyfikację czasu zakończenia żądanej przez LEMF obserwacji celu i/lub zmianę typu monitorowania na offline

MODIFICATE		
PARAMETR		*OPIS*
version	ENUMERATED	wersja protokołu (1)
request	CHOICE	typ zapytania (2 – signedRequest)
time	TimeStamp	godzina i data wystawienia zlecenia aktywacji
Command	CHOICE	typ polecenia (3 – **Modificate**)
liid	OCTET STRING	format: LEAID+TARGET (SEQ), 17 znaków ASCII
stopTimestamp	TimeStamp	godzina i data deaktywacji celu
service	CHOICE	rodzaj żądanej usługi (taki jak w wiadomości Activate)

Action acknowledge

Odpowiedź ze strony ADMF/DF na wiadomości: Hello, Aktywacja, Dezaktywacja, Modyfikacja.

ACTION_ACK		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
version	ENUMERATED	wersja protokołu (1)
respond	CHOICE	typ odpowiedzi (1 – generalRespond)
result	ENUMERATED	wynik operacji [4)]
message	PrintableString	ten sam tekst co w hello

[4)] result

1 – ok

2 – missing-parametr

3 – unknown-parametr

4 – unknown-parameter value

5 – incorrect-BER

6 – badSignature

7 – certificateExpired

10 – unknownError

11 – unsupportedService

List

LIID-LIST – żądanie listy LIIDów monitorowanych lub oczekujących w ADMF.

LIID-LIST		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
version	ENUMERATED	wersja protokołu (1)
request	CHOICE	typ zapytania (1 – simpleRequest)
simpleRequest	CHOICE	rodzaj zapytania (2 – **list**)
type	ENUMERATED	zapytanie o konkretny LIID lub o wszystkie [5)]
liid	OCTET STRING	opcjonalny (występuje tylko dla type=2); format: LEAID+TARGET (SEQ), 17 znaków ASCII

[5)] type

1 – all

2 – specific

List – Odpowiedź (1)

LIID-LIST-DATA – odpowiedź na LLID-LIST, gdzie type = 1.
Pole status może przyjąć tylko wartości 1, 2 lub 4.

LIID-LIST-DATA		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
version	ENUMERATED	wersja protokołu (1)
respond	CHOICE	typ odpowiedzi (2 – **listRespond**)
liid	OCTET STRING	format: LEAID+TARGET (SEQ), 17 znaków ASCII
status	ENUMERATED	status LIID w ADMF [6)]

message	UTF8String	wiadomość dodatkowa
liid	OCTET STRING	format: LEAID+TARGET (SEQ), 17 znaków ASCII
status	ENUMERATED	status LIID w ADMF [6)]
message	UTF8String	wiadomość dodatkowa
…		
…		
…		

[6)] status

0 – notFound

1 – waiting

2 – cnActivated

3 – unknown

4 – deActivated

List – Odpowiedź (2)

LIID-LIST-DATA – odpowiedź na LLID-LIST, gdzie type = 2.
Pole status może przyjąć wszystkie zdefiniowane wartości.

LIID-LIST-DATA		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
version	ENUMERATED	wersja protokołu (1)
respond	CHOICE	typ odpowiedzi (2 – **listRespond**)
liid	OCTET STRING	format: LEAID+TARGET (SEQ), 17 znaków ASCII
status	ENUMERATED	status LIID w ADMF [6)]
message	UTF8String	wiadomość dodatkowa

[6)] status

0 – notFound

1 – waiting

2 – cnActivated

3 – unknown

4 – deActivated

3. Kierunek z ADMF do LEMF

Szczegółowe definicje określające ten ruch zawarte są w specyfikacji ASN.1 Interfejsu HI1: H1ADMFOperations.

Hello

Hello – jest wiadomością testową umożliwiającą stronie ADMF sprawdzenie poprawności działania interfejsu HI1.

HELLO		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
version	ENUMERATED	wersja protokołu (1)
Content	CHOICE	typ zapytania (1 –InfoIndicator)

InfoIndicatoor	CHOICE	rodzaj zapytania (1 - **HelloRequest**)
message	UTF8String	tekst

Alarm

Alarm – jest wiadomością umożliwiającą stronie ADMF poinformowanie LEMF o różnego rodzaju problemach, czasach wystąpienia tych problemów oraz czasach ich usunięcia ze wskazaniem na przyczynę.

ALARM		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
version	ENUMERATED	wersja protokołu (1)
content	CHOICE	typ zapytania (1 – InfoIndicator)
InfoIndicator	CHOICE	rodzaj zapytania (2 - **AlarmIndicator**)
identity	INTEGER	numer pozwalający na jednoznaczną identyfikacje alarmu razem z timestamp-on
alarmID	AlarmID	AlarmID jest typu ENUMERATED. Numery opisuja przyczynę alarmu [1)]
description	PrintableString	Dodatkowy, opcjonalny opis błędu, np. kod błędu z MSC
timestamp	TimeStamp	Godzina i data wysłania alarmu
Timestamp-on	TimeStamp	Czas wystąpienia zdarzenia objętego alarmem
Timestamp-off	TimeStamp	Czas wystąpienia zdarzenia odwrotnego do objętego alarmem
status	AlarmStatus	Typ AlarmStatus mówi o aktywności alarmu i jest ENUMERATED (0-off, 1-on)
nature-of-alarm	Nature-of-The-Intercepted-call	Ten typ jest ENUMERATED i wskazuje na rodzaje błędnych transakcji[2)]
range-of-alarm	NetPart Type	Wskazuje na przyczynę problemu po stronie CN. 0-whole, 2- part
targettype	ENUMERATED	Wskazuje na konkretną sesję dla konkretnego LIID lub wszystkie obserwacje. 1-all, 2-specific
liid	OCTET STRING	format: LEAID+TARGET (SEQ), 17 znaków ASCII
cid	UTF8String	Zgodnie z HI2 wskazuje na konkretna sesję lub rozmowę
cid-GPRS	OCTET STRING	Zgodnie z HI2 wskazanie na konkretna sesję

[1)] alarmID

0 - przepełnienie bufora w kierunku LEMF (IRI i/lub CC tracone)

1 - problem z monitoringiem online

2 - problem z zapisywaniem danych HI3 (LEMF)

3 - problem z zapisywaniem danych HI2 (LEMF)

4 - problem z monitoringiem online (LEMF)

5 - brak lub przeciążenie komunikacji z CN na interfejsie HI1 (SM operatora)

6 - brak lub przeciążenie komunikacji z CN na interfejsie HI2 (SM operatora)

7 - brak lub przeciążenie komunikacji z CN na interfejsie HI3 (SM operatora)

8 - brak lub przeciążenie komunikacji z CN na interfejsie HI3 on-line (SM operatora)

9 - poważne uszkodzenie SM => konieczne sprawdzenie spójności BD (SM operatora)

10 - zarządzanie obserwacjami prawidłowe, ale inne funkcje SM mogą nie działać (np. część obserwacji stracona) (SM operatora)

11 - obserwacja nie założona w CN a czas na nią (LIID obowiązkowy) (SM operatora)

12 - obserwacja nie usunieta z CN a czas na nią (LIID obowiązkowy) (SM operatora)

13 - po stronie CN LI całkowicie nie funkcjonowało, BD obserwacji odbudowane w CN (SM operatora)

14 - po stronie CN pewne funkcje LI nie działały (SM operatora)

15 - informacja wprowadzana ręcznie: uszkodzenie w CN lub SM (SM operatora)

20 - informacja wprowadzana ręcznie o pracach planowych w systemie SM operatora (SM operatora)

…

[2)]nature-of-alarm

0 - the possible UUS content is sent through the HI2 or HI3 "data" interface

- the possible call content is established through the HI3 "circuit" interface

1 - the SMS content is sent through the HI2 or HI3 "data" interface

2 - the UUS content is sent through the HI2 or HI3 "data" interface

3 - the possible call content call is established through the HI3 "circuit" interface

- the possible data are sent through the HI3 "data" interface

4 - the data are sent through the HI3 "data" interface

5 - the data are sent through the HI3 "data" interface

6 - the possible call content call is established through the HI3 "circuit" interface

- the possible data are sent through the HI3 "data" interface

11 - wIFI

Notification

Notification – jest wiadomością umożliwiającą stronie ADMF poinformowanie LEMF o faktycznym czasie rozpoczęcia i zakończeniu obserwacji w sieci operatora.

NOTIFICATION		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
version	ENUMERATED	wersja protokołu (1)
content	CHOICE	typ zapytania (1 – InfoIndicator)
InfoIndicator	CHOICE	rodzaj zapytania (3 - **NotificationIndicator**)
identity	INTEGER	numer pozwalający (razem z timestamp-on) na jednoznaczną identyfikacje notyfikacji
notyficationID	NotyficationID	Typ ENUMERATED: target-activated (0), target-deactivated (1), target-modificated (2),…
description	PrintableString	Dodatkowy, opcjonalny opis notyfikacji
timestamp	TimeStamp	Godzina i data wysłania notyfikacji
TimestampEvent	TimeStamp	Czas wystąpienia zdarzenia, którego dotyczy powiadomienie
liid	OCTET STRING	format: LEAID+TARGET (SEQ), 17 znaków ASCII

Action acknowledge

Odpowiedź ze strony LEMF na wiadomości: Hello, Alarm, Notyfikacja.

ACTION_ACK		
PARAMETR	*TYP POLA DANYCH*	*OPIS*
version	ENUMERATED	wersja protokołu (1)
respond	CHOICE	typ odpowiedzi (1 – **generalRespond**)
result	ENUMERATED	wynik operacji [4)]
message	UTF8String	Jeśli odpowiada na Hello zwraca ten sam tekst który wysłany był w wiadomości hello

[4)] result

1 – ok

2 – missing-parametr

3 – unknown-parametr

4 – unknown-parameter value

5 – incorrect-BER

6 – badSignature

7 – certificateExpired

10 – unknownError

Szczegółowa definicja interfejsów HI.
Specyfikacja ASN.1. Kodowanie BER.

1. HI1LEMFPDU

```
HI1LEMFOperations DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
IMPORTS
  LawfulInterceptionIdentifier,
  TimeStamp
FROM
  UnsignedRequestDetail;

HI1LEMFPDU ::= SEQUENCE
{
  version [0] Version,
  content [1] Content,
  ...
}
```

```
Version ::= ENUMERATED
{
  version1 (1),
  ...
}

Content ::= CHOICE
{
  request [1] Request,
  respond [2] Respond,
  ...
}
SignedRequest ::= SEQUENCE
{
  version [1] SignedRequestVersion,
  signStandard [2] OBJECT IDENTIFIER,
  -- CryptographicMessageSyntax2004 { iso(1) member-body(2) us(840) rsadsi(113549)
pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24)
  cmsDERSignedRequest     [3] OCTET STRING,
  -- cmsDERSignedRequest [3] ANY DEFINED BY signStandard
  ...
}

Request ::= CHOICE
{
  simpleRequest [1] SimpleRequest,
  signedRequest [2] SignedRequest,
  ...
}

SimpleRequest ::= CHOICE
{
  helloRequest [1] HelloRequest,
  listRequest [2] ListRequest,
  ...
}

SignedRequestVersion ::= ENUMERATED
{
  v1 (0),
  ...
}
HelloRequest ::= SEQUENCE
{
  message [1] UTF8String,
```

```
  ...
}

Respond ::= CHOICE
{
  generalRespond [1] GeneralRespond,
  listRespond [2] ListRespond,
  ...
}

GeneralRespond ::= SEQUENCE
{
  result [1] Result,
  message [2] UTF8String OPTIONAL,
  -- return Hello request message
  ...
}

Result ::= ENUMERATED
{
  ok (1),
  missing-parameter (2),
  unknown-parameter (3),
  unknown-parameter-value (4),
  incorrect-BER (5),
  badSignature (6),
  certificateExpired (7),
  unknownError (10),
  unsupportedService (11),
  ...
}CheckRespond ::= SEQUENCE
{
  liid [1] LawfulInterceptionIdentifier,
  checkStatus [2] CheckStatus,
  message [3] UTF8String OPTIONAL,
  ...
}

CheckStatus ::= ENUMERATED
{
  notFound (0),
  waiting (1),  -- założone przez lemf, nie ma w cn (czeka na zatwierdzenie lub )
  cnActivated (2), -- jest w cn
  unknown (3),
  deActivated (4), -- po deaktywowaniu w cn
  ...
```

```
}

ListRequest ::= SEQUENCE
{
  type [1] ListType,
  liid [2] LawfulInterceptionIdentifier OPTIONAL,
  ...
}

ListRespond ::= SET OF CheckRespond

ListType ::= ENUMERATED
{
  all (1),
  specific (2),
  ...
}

END
```

2. UnsignedRequestDetail

```
UnsignedRequestDetail DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

UnsignedRequestDetail ::= SEQUENCE
{
  time [1] TimeStamp,
  command [2] Command,
  ...
}

Command ::= CHOICE
{
  activate [1] Activate,
  deactivate [2] Deactivate,
  modificate [3] Modificate,
  ...
}

Activate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  startTimestamp [2] TimeStamp,
  stopTimestap [3] TimeStamp,
```

```
  service [4] Service,
  warrantID [5] UTF8String,
  ...
}

Modificate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  stopTimestap [3] TimeStamp,
  service [4] Service,
  warrantID [5] UTF8String,
  -- w strukturze service dopuszczalna jest tylko zmiana tyou monitorowania z online na
offlien
  ...
}

Deactivate ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  warrantID [5] UTF8String OPTIONAL,
  ...
}

Service ::= CHOICE
{
  circuitSwitched [1] CircuitSwitched,
  packetSwitched [2] PacketSwitched,
  wifi [3] WIFI,
  xdsl [4] XDSL,
  ...
}CircuitSwitched ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  onlineMonitoring [3] BOOLEAN,
  -- offline - zawsze,
  -- online - jak będzie ustawiony parametr forwardingAddress to oznacza online
  forwardingAddress [4] ForwardingAddress OPTIONAL,
  -- tylko jak ustawiony parametr nolineMonitoring = true
  stereo [5] Stereo,
  ...
}

Stereo ::= ENUMERATED
{
  off (0),
```

```
  on (1)
}

PacketSwitched ::= SEQUENCE
{
  target [1] Target,
  monitoringType [2] MonitoringType,
  ...
}

WIFI ::= SEQUENCE
{
  target [1] Target,
  ...
}

XDSL ::= SEQUENCE
{
  target [1] Target,
  ...
}

Target ::= CHOICE
{
  mSISDN [1] MSISDN,
  iMSI [2] IMSI,
  iMEI [3] IMEI,
  login [4] Login,
  ...
}

MSISDN ::= OCTET STRING (SIZE (1..9))
IMSI ::= OCTET STRING (SIZE (3..8))
IMEI ::= OCTET STRING (SIZE (8))
Login ::= OCTET STRING (SIZE (1..120))

ForwardingAddress ::= SEQUENCE
{
  sipUrl [1] SIPURL,
  ...
}

SIPURL ::= UTF8String
MonitoringType ::= ENUMERATED
{
  iri (1),
```

```
  iriCC (2),
  ...
}

LawfulInterceptionIdentifier ::= OCTET STRING (SIZE (1..25))
-- It is recommended to use ASCII characters in "a"…"z", "A"…"Z", "-", "_", ".", and
"0"…"9".
-- For subaddress option only "0"..."9" shall be used.
-- 17 znakow numerycznych ASCII
-- format: LEAID + TARGET(SEQ)
-- TARGET - (15 znakow) nadawany sekwencyjnie dla kazdego LEAID
-- LEAID -(2 znaki) 00 – LEMF operatora, 01 - ABW, 02 - Policja, 03 - CBŚ, 04 - SG, 05 -
CBA, 06 - SKW

TimeStamp ::= CHOICE
{
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.
  localTime [0] LocalTimeStamp,

  utcTime [1] UTCTime
}
LocalTimeStamp ::= SEQUENCE
{
  generalizedTime [0] GeneralizedTime,
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.

  winterSummerIndication [1] ENUMERATED
  {
    notProvided(0),
    winterTime(1),
    summerTime(2),
    ...
  }
}

END
```

3. HI1ADMFPDU

```
HI1ADMFOperations DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
```

```
IMPORTS
  LawfulInterceptionIdentifier,
  TimeStamp
FROM
UnsignedRequestDetail;
HI1ADMFPDU ::= SEQUENCE
{
  version [0] Version,
  content [1] Content
}

Version ::= ENUMERATED
{
  version1 (1),
  ...
}

Content ::= CHOICE
{
  info [0] InfoIndicator,
  acknowledge[1] Acknowledge,
  ...
}

InfoIndicator ::= CHOICE
{
  helloRequest [1] HelloRequest,
  alarm      [2] AlarmIndicator,
  notification [3] NotificationIndicator,
  ...
}

HelloRequest ::= SEQUENCE
{
  message [1] UTF8String,
  ...
}

AlarmIndicator ::= SEQUENCE
{
  identity [0] INTEGER,    -- numer pozwalający na jednoznaczną identyfikacje alarmu
razem z timestamp-on
  alarmID    [1] AlarmID,
  description[2] UTF8String OPTIONAL,  -- dodatkowe informacje, opis, kod błędu (np. z
alarmu z MSC), tzw. powód
  timestamp  [3] TimeStamp,                                    -- czas wysłania alarmu
```

```
  timestamp-on [4] TimeStamp OPTIONAL,                        -- czas wystąpienia
alarmowanego zdarzenia
  timestamp-off [5] TimeStamp OPTIONAL,                       -- czas wystąpienia zdarzenia
odwrotnego do zdarzenia alarmowanego
  status [6] AlarmStatus OPTIONAL,                            -- powstanie/ustanie alarmu
  -- podobne nature-Of-The-intercepted-call z HI2 (jeżeli błąd globalny to wszystkie
service)
  nature-of-alarm   [7] Nature-Of-The-intercepted-call OPTIONAL,
  range-of-alarm [8] NetPartType OPTIONAL,    -- dotyczy całej sieci CN czy tylko jej
części (np.: tylko jeden GGSN, jedna centrala)
  targettype [9] TargetType OPTIONAL,         -- dotyczy konkretnego LIID lub konkretnej
sesji albo wszystkich obserwacji
  liid [10] LawfulInterceptionIdentifier OPTIONAL,
  cid  [11] UTF8String OPTIONAL,        -- z HI2 (chodzi o wskazanie konkretnej rozmowy
lub sesji)
  cid-GPRS [12] GPRSCorrelationNumber OPTIONAL,            -- z HI2 (chodzi o wskazanie
konkretnej rozmowy lub sesji)
  ...
}

Nature-Of-The-intercepted-call ::= ENUMERATED
{
  -- Nature of the intercepted "call":
  gSM-ISDN-PSTN-circuit-call(0),
  -- the possible UUS content is sent through the HI2 or HI3 "data" interface
  -- the possible call content call is established through the HI3 "circuit" interface
  gSM-SMS-Message(1),
  -- the SMS content is sent through the HI2 or HI3 "data" interface
  uUS4-Messages(2),
  -- the UUS content is sent through the HI2 or HI3 "data" interface
  tETRA-circuit-call(3),
  -- the possible call content call is established through the HI3 "circuit" interface
  -- the possible data are sent through the HI3 "data" interface
  teTRA-Packet-Data(4),
  -- the data are sent through the HI3 "data" interface
  gPRS-Packet-Data(5),
  -- the data are sent through the HI3 "data" interface
  uMTS-circuit-call(6),
  -- the possible call content call is established through the HI3 "circuit" interface
  -- the possible data are sent through the HI3 "data" interface
  wIFI (11),
  xDSL [12],
    ...
}

NotificationIndicator ::= SEQUENCE
```

```
{
  identity [0] INTEGER,                        -- numer pozwalający na jednoznaczną
identyfikacje alarmu razem z timestamp-on
  notificationID [1] NotificationID,
  description[2] UTF8String OPTIONAL,          -- dodatkowe informacje, opis, kod błędu
(np. z MSC), tzw. powód
  timestamp [3] TimeStamp,                     -- czas wysłania powiadomienia
  timestampEvent [4] TimeStamp,                -- czas wystąpienia zdarzenia, którego
dotyczy powiadomienie
  liid [5] LawfulInterceptionIdentifier OPTIONAL,
  ...
}

AlarmID ::= ENUMERATED
{
  sm-buffer-overflow (0),                      -- bufory wyjściowe w kierunku LEMF
przepełnine => IRI i/lub CC tracone (operator)
  lemf-hi3-online-delivery-failure (1),        -- problem z monitoringiem online (LEMF)
  lemf-hi3-delivery-failure (2),        -- problem z zapisywaniem danych HI3 (LEMF)
  lemf-hi2-delivery-failure (3),        -- problem z zapisywaniem danych HI2 (LEMF)
  lemf-hi1-delivery-failure (4),        -- problem z monitoringiem online (LEMF)
  sm-hi1-failure (5),                   -- brak lub przeciążenie komunikacji z CN na
interfejsie HI1 (SM operatora)
  sm-hi2-failure (6),                   -- brak lub przeciążenie komunikacji z CN na
interfejsie HI2 (SM operatora)
  sm-hi3-failure (7),                   -- brak lub przeciążenie komunikacji z CN na
interfejsie HI3 (SM operatora)
  sm-hi3-online-failure (8),            -- brak lub przeciążenie komunikacji z CN na
interfejsie HI3 (SM operatora)
  major-system-failure (9),             -- poważne uszkodzenie SM => konieczne
sprawdzenie spójności BD (SM operatora)
  -- zarządzanie obserwacjami prawidłowe, ale inne funkcje SM mogą nie działać (np. część
obserwacji stracona) (SM operatora)
  minor-system-failure (10),
  cn-activation-error (11),             -- obserwacja nie założona w CN a czas na nią
(LIID obowiązkowy) (SM operatora)
  cn-deactivation-error   (12),         -- obserwacja nie usunieta z CN a czas na nią
(LIID obowiązkowy) (SM operatora)
  major-cn-li-failure (13),             -- po stronie CN LI całkowicie nie funkcjonowało,
BD obserwacji odbudowane w CN (SM operatora)
  minor-cn-li-failure (14),             -- po stronie CN pewne funkcje LI nie działały
(SM operatora)
  manual-system-failure (15),           -- informacja wprowadzana ręcznie: uszkodzenie w
CN lub SM (SM operatora)
  manual-system-maintenance (20),       -- informacja wprowadzana ręcznie o pracach
planowych w systemie SM operatora (SM operatora)
```

```
  ...
}

AlarmStatus ::= ENUMERATED
{
  off  (0),
  on (1),
  ...
}
NetPartType ::= ENUMERATED
{
  whole (1),
  part (2),
  ...
}

TargetType ::= ENUMERATED
{
  all (1),
  specific (2),
  ...
}

NotificationID ::= ENUMERATED
{
  target-activated (0),
  target-deactivated (1),
  target-modificated (2),
  ...
}

Acknowledge ::= CHOICE
{
  respond    [0] GeneralRespond,
  ...
}

GeneralRespond ::= SEQUENCE
{
  result     [1] Result,
  message    [2] UTF8String OPTIONAL,
  ...
}

Result ::= ENUMERATED
{
```

```
  ok (1),
  missing-parameter (2),
  unknown-parameter (3),
  unknown-parameter-value (4),
  incorrect-BER (5),
  badSignature (6),
  certificateExpired (7),
  unknownError (10),
  ...
}

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))

END
```

Załącznik nr 2

Specyfikacja techniczna styku HI-2 interfejsu HI

1. Warstwa fizyczna

Warstwa fizyczna ma znaczenie lokalne pomiędzy dwoma urządzeniami sieciowymi i ma znaczenie tylko na styku systemów miedzy operatorem a uprawnionym podmiotem.

2.Warstwa sieciowa

Dla każdego podmiotu uprawnionego określone są dedykowane adresy publiczne IPv4 dla DF (HI2). Służby określają adresację publiczną IPv4 po swojej stronie. Adresy IP nie mogą być takie same dla wszystkich operatorów w danym systemie LEMF, jak i nie mogą być takie same dla uprawnionych podmiotów w danym systemie ADMF/DF.

3. Warstwa transportowa

Stosowany jest protokół FTP (RFC 959),
Połączenie jest nawiązywane tylko w kierunku MF ► LEMF
Wykorzystywany jest tylko tryb passive protokołu FTP,
Serwer FTP po stronie LEMF nasłuchuje na portach

- 20 (data connection),
- 21 (control connection),

Protokól FTP zostaje ograniczony do następujących komend:

- USER NAME (USER),
- PASSWORD (PASS),
- DATA PORT (PORT),
- PASSIVE (PASV),
- REPRESENTATION TYPE (TYPE) - ASCII Non-print,
- FILE STRUCTURE (STRU) - File,
- TRANSFER MODE (MODE) - Stream,
- STORE (STOR),
- RENAME FROM (RNFR),
- RENAME TO (RNTO),
- ABORT (ABOR),
- CHANGE WORKING DIRECTORY (CWD),
- PRINT WORKING DIRECTORY (PWD),

- NOOP (NOOP),
- LOGOUT (QUIT).

Nazwa przesyłanego pliku jest zmieniana na docelową po udanym nagraniu; plik tymczasowy posiada dodatkowe rozszerzenie .tmp (LIID_seq.ext_tmp),
Nazwa pliku po przesłaniu składa się z LIID i numeru sekwencyjnego (LIID_seq.ext),
Zawartość pliku czyli dane IRI kodowanie są w formacie ASN.1/BER.

4. Warstwa aplikacyjna

Dla usług CS oraz PS interfejs został opracowany na podstawie specyfikacji ETSI TS 101 671 wersja 2.13.1 (rozdziały 5.2, 8). W dokumencie znajduje się szczegółowy opis interfejsu HI2 oraz jego definicje w ASN.1.
Dla usług zawierających się w IPAccess (WiFi-WLAN, xDSL) interfejs w pełni zgodny jest ze specyfikacją ETSI TS 102 232-1 wersja 2.2.1 oraz TS 102 232-3 wersja 2.1.1. W dokumencie znajduje się szczegółowy opis specyfikacji interfejsu HI2 oraz jego definicje w ASN.1.
Nie stosujemy mechanizmu ROSE tzn. przesyłania danych IRI przy użyciu protokołów transportowych, tj. TCP, UDP
Dla wszystkich usług rekordy IRI przekazywane są w plikach przy użyciu protokołu FTP.
Przesyłany plik może zawierać wiele pojedyńczych rekordów IRI zakodowanych w standardzie ASN1/BER.
Wartości parametrów IRI należy definiować w formatach zalecanych przez standardy telekomunikacyjne, które ich dotyczą (np. ISDN user part, DSS1, MAP czy IP)
W przypadku interfejsu HI2 przez warstwę aplikacyjną należy rozumieć kodowanie zawartości plików, a nie protokół FTP użyty do ich transportu.
Interfejs nie wymaga stosowania podpisu elektronicznego.

4.1 Zmiany w stosunku do specyfikacji ETSI

Dla wszystkich obsługiwanych usług wprowadzono nowy typ PartyExtendedIdentity rozszerzający parametry IRI o dane personalne abonentów uczestniczących w przekazie informacji.

```
PartyInformation ::= SEQUENCE
{
  ...
  partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity
OPTIONAL,
  ...
}

PartyExtendedIdentity ::= SEQUENCE
{
  subscriptionType [1] ENUMERATED
  {
    postpaid (0),
    prepaid  (1),
    ...
  } OPTIONAL,

  activationDate [2] TimeStamp OPTIONAL,
  deactivationDate [3] TimeStamp OPTIONAL,
```

```
  subscriber [4] Subscriber OPTIONAL,
  postalAddress [5] PostalAddress OPTIONAL,
  mailAddress [6] PostalAddress OPTIONAL,
  ...
}

Subscriber ::= CHOICE
{
  company [1] Company,
  person [2] Person,
  ...
}

Company ::= SEQUENCE
{
  name [0] UTF8String,
  regon  [1] OCTET STRING (SIZE (5)),
  -- BCD coded 9 digits
  -- F digit not used
  ...
}

Person ::= SEQUENCE
{
  firstName [0] UTF8String,
  surname [1] UTF8String,
  pesel   [2] OCTET STRING (SIZE (6)) OPTIONAL,
  -- BCD coded 11 digits
  -- F digit not used
  passportNumber [3] OCTET STRING (SIZE (7..14)) OPTIONAL,
  -- ASCII coded
  ...
}

PostalAddress ::= SEQUENCE
{
  street [1] UTF8String OPTIONAL,
  buildingNumber [2] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  apartmentNumber [3] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  postcode [4] OCTET STRING (SIZE (1..8)) OPTIONAL,
  city [5] UTF8String OPTIONAL,
  country [6] UTF8String OPTIONAL
}
```

5. Usługi CS i PS

Niewykorzystywane parametry:

- iRISequence typu IRISequence w strukturze IRIsContent (brak możliwości agregacji rekordów IRI w strukturze ASN.1)

- ringingDuration w strukturze IRI-Parameters
- conversationDuration w strukturze IRI-Parameters (czas rozmowy można wyznaczyć w inny sposób)
- callContentLinkInformation w strukturze IRI-Parameters (brak danej funkcjonalności)
- cC-Link-Identifier w w strukturze IRI-Parameters
- national-Parameters
- network-Element-Identifier w strukurze Network-Identifier

6.Usługi IPAccess (WLAN, xDSL)

W przypadku wspomnianych usług specyfikacja zgodna jest w pełni ze standardami ETSI TS 102 232-1 oraz TS 102 232-3. Jedynym dodatkiem jest wyspecyfikowane już pole PartyExtendedIdentity.

Szczegółowa specyfikacja HI2

```
HI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) hi2(1) version9(9)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- ==============================
-- Object Identifier Definitions
-- ==============================

-- LawfulIntercept DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4)
etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
hi2DomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId hi2(1)}
hi2OperationId OBJECT IDENTIFIER ::= {hi2DomainId version9(9)}

IRIsContent ::= CHOICE
{
  iRIContent IRIContent,
  iRISequence IRISequence -- NOT USED
}

IRISequence ::= SEQUENCE OF IRIContent -- NOT USED
-- Aggregation of IRIContent is an optional feature.
```

```
-- It may be applied in cases when at a given point in time several IRI records are
-- available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent immediately and shall
-- not held in the DF or MF in order to apply aggregation.
-- When aggregation is not to be applied, IRIContent needs to be chosen.

IRIContent ::= CHOICE
{
  iRI-Begin-record [1] IRI-Parameters,
  -- At least one optional parameter must be included within the iRI-Begin-Record.
  iRI-End-record [2] IRI-Parameters,
  iRI-Continue-record [3] IRI-Parameters,
  -- At least one optional parameter must be included within the iRI-Continue-Record.
  iRI-Report-record [4] IRI-Parameters,
  -- At least one optional parameter must be included within the iRI-Report-Record.
  ...
}

IRI-Parameters ::= SEQUENCE
{
  domainID [0] OBJECT IDENTIFIER (hi2OperationId) OPTIONAL,
  -- for the sending entity the inclusion of the Object Identifier is mandatory
  iRIversion [23] ENUMERATED
  {
    version2(2),
    ...,
    version3(3),
    version4(4),
    version5(5),
    version6(6),
    version7(7),
    lastVersion(8)
  } OPTIONAL,
  -- Optional parameter "iRIversion" (tag 23) is redundant starting from TS 101 671
v2.4.1
  -- where to the object identifier "domainID" was introduced into IRI-Parameters.
  -- In order to keep backward compatibility, even when the version of the "domainID"
  -- parameter will be incremented it is recommended to always send to LEMF the same:
  -- enumeration value "lastVersion(8)".
  -- if not present, it means version 1 is handled

  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is associated to the target.

  communicationIdentifier [2] CommunicationIdentifier,
```

```
  -- used to uniquely identify an intercepted call.
  -- Called "callIdentifier" in Edition 1 of ES 201 671.

  timeStamp [3] TimeStamp,
  -- date and time of the event triggering the report.

  intercepted-Call-Direct [4] ENUMERATED
  {
    not-Available(0),
    originating-Target(1),
    -- In case of GPRS, this indicates that the PDP context activation, modification
    -- or deactivation is MS requested.
    terminating-Target(2),
    -- In case of GPRS, this indicates that the PDP context activation, modification
    -- or deactivation is network initiated.
    ...
  } OPTIONAL,

  intercepted-Call-State [5] Intercepted-Call-State OPTIONAL,

  ringingDuration [6] OCTET STRING (SIZE (3)) OPTIONAL, -- NOT USED
  -- Duration in seconds. BCD coded : HHMMSS

  conversationDuration [7] OCTET STRING (SIZE (3)) OPTIONAL, -- NOT USED
  -- Duration in seconds. BCD coded : HHMMSS

  locationOfTheTarget [8] Location OPTIONAL,
  -- location of the target subscriber

  partyInformation [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
  -- This parameter provides the concerned party (Originating, Terminating or forwarded
  -- party), the identity(ies) of the party and all the information provided by the
party.

  callContentLinkInformation [10] SEQUENCE
  {
    cCLink1Characteristics [1] CallContentLinkCharacteristics OPTIONAL,
    -- Information concerning the Content of Communication Link Tx channel established
    -- toward the LEMF (or the sum signal channel, in case of mono mode).

    cCLink2Characteristics [2] CallContentLinkCharacteristics OPTIONAL,
    -- Information concerning the Content of Communication Link Rx channel established
    -- toward the LEMF.
    ...
  } OPTIONAL, -- NOT USED
```

```
  release-Reason-Of-Intercepted-Call [11] OCTET STRING (SIZE (2)) OPTIONAL,
  -- Release cause coded in ITU-T Q.850 [31] format.
  -- This parameter indicates the reason why the intercepted call cannot be established
or
  -- why the intercepted call has been released after the active phase.

  nature-Of-The-intercepted-call [12] ENUMERATED
  {
    -- Nature of the intercepted "call":
    gSM-ISDN-PSTN-circuit-call(0),
    -- the possible UUS content is sent through the HI2 or HI3 "data" interface
    -- the possible call content call is established through the HI3 "circuit" interface
    gSM-SMS-Message(1),
    -- the SMS content is sent through the HI2 or HI3 "data" interface
    uUS4-Messages(2),
    -- the UUS content is sent through the HI2 or HI3 "data" interface
    tETRA-circuit-call(3),
    -- the possible call content call is established through the HI3 "circuit" interface
    -- the possible data are sent through the HI3 "data" interface
    teTRA-Packet-Data(4),
    -- the data are sent through the HI3 "data" interface
    gPRS-Packet-Data(5),
    -- the data are sent through the HI3 "data" interface
    ...,
    uMTS-circuit-call(6)
    -- the possible call content call is established through the HI3 "circuit" interface
    -- the possible data are sent through the HI3 "data" interface
  } OPTIONAL,

  serverCenterAddress [13] PartyInformation OPTIONAL,
  -- e.g. in case of SMS message this parameter provides the address of the relevant
  -- server within the calling (if server is originating) or called
  -- (if server is terminating) party address parameters

  sMS [14] SMS-report OPTIONAL,
  -- this parameter provides the SMS content and associated information

  cC-Link-Identifier [15] CC-Link-Identifier OPTIONAL, -- NOT USED
  -- Depending on a network option, this parameter may be used to identify a CC link
  -- in case of multiparty calls.

  national-Parameters [16] National-Parameters OPTIONAL, -- NOT USED

  gPRSCorrelationNumber [18] GPRSCorrelationNumber OPTIONAL,

  gPRSevent [20] GPRSEvent OPTIONAL,
```

```
  -- This information is used to provide particular action of the target
  -- such as attach/detach

  sgsnAddress [21] DataNodeAddress OPTIONAL,

  gPRSOperationErrorCode [22] GPRSOperationErrorCode OPTIONAL,
  ...,
  ggsnAddress [24] DataNodeAddress OPTIONAL,

  qOS [25] UmtsQos OPTIONAL,
  -- This parameter is duplicated from TS 133 108 [61].

  networkIdentifier [26] Network-Identifier OPTIONAL,
  -- This parameter is duplicated from TS 133 108 [61].

  sMSOriginatingAddress [27] DataNodeAddress OPTIONAL,
  -- This parameter is duplicated from TS 133 108 [61].

  sMSTerminatingAddress [28] DataNodeAddress OPTIONAL,
  -- This parameter is duplicated from TS 133 108 [61].

  iMSevent [29] IMSevent OPTIONAL,

  sIPMessage [30] OCTET STRING OPTIONAL,
  -- This parameter is duplicated from TS 133 108 [61].

  servingSGSN-number [31] OCTET STRING (SIZE (1..20)) OPTIONAL,
  -- This parameter is duplicated from TS 133 108 [61].

  servingSGSN-address [32] OCTET STRING (SIZE (5..17)) OPTIONAL,
  -- Octets are coded according to TS 123 003
  -- This parameter is duplicated from TS 133 108 [61].
  -- tARGETACTIVITYMONITOR [33] TARGETACTIVITYMONITOR OPTIONAL,
  -- to be included after publication of the AT-D specification
  -- Parameter is used in TS 101 909-20-1 [69]

  ldiEvent [34] LDIevent OPTIONAL,
  -- The "Location Dependent Interception" parameter is duplicated from TS 133 108 [61].

  correlation [35] CorrelationValues OPTIONAL,
  -- This parameter is duplicated from TS 133 108 [61]

  national-HI2-ASN1parameters [255] National-HI2-ASN1parameters OPTIONAL
}

-- ==================
```

```
-- PARAMETERS FORMATS
-- ==================
CommunicationIdentifier ::= SEQUENCE
{
  communication-Identity-Number [0] OCTET STRING (SIZE (1..8)) OPTIONAL,
  -- Temporary Identifier of an intercepted call to uniquely identify an intercepted
call.
  -- This parameter is mandatory if there is associated
  -- information sent over HI3interface (CClink, data,..) or when
  -- CommunicationIdentifier is used for IRI other than IRI-Report-record
  -- This parameter was called "call-Identity-Number" in Edition 1 (v1.1.1) ES 201 671.
  -- The individual digits of the communication-Identity-Number shall be represented in
  -- ASCII format, e.g. "12345678" = 8 octets 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38.

  network-Identifier [1] Network-Identifier,
  ...
}
-- NOTE: The same "CommunicationIdentifier" value is sent :
-- with the HI3 information for correlation purpose between the IRI and the information
sent on
-- the HI3 interfaces (CCLink, data, ..) with each IRI associated to a same intercepted
call
-- for correlation purpose between the different IRI.

Network-Identifier ::= SEQUENCE
{
  operator-Identifier [0] OCTET STRING (SIZE (1..5)),
  -- It is a notification of the NWO/AP/SvP in ASCII- characters.
  -- The parameter is mandatory.
  -- format: MNC + MVNO
  network-Element-Identifier [1] Network-Element-Identifier OPTIONAL, -- NOT USED
  ...
}

Network-Element-Identifier ::= CHOICE
{
  e164-Format [1] OCTET STRING (SIZE (1..25)),
  -- E164 address of the node in international format. Coded in the same format as the
  -- calling party number parameter of the ISUP (parameter part: EN 300 356 [5]).

  x25-Format [2] OCTET STRING (SIZE (1..25)),
  -- X25 address

  iP-Format [3] OCTET STRING (SIZE (1..25)),
  -- IP address
```

```
  dNS-Format [4] OCTET STRING (SIZE (1..25)),
  -- DNS address
  ...,
  iP-Address [5] IPAddress,
  ...
}

CC-Link-Identifier ::= OCTET STRING (SIZE (1..8))
-- Depending on a network option, this parameter may be used to identify a CClink
-- in case of multiparty calls.
-- The individual digits of the communication-Identity-Number shall be represented in
-- ASCII format, e.g. "12345678" = 8 octets 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38.

TimeStamp ::= CHOICE
{
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.
  localTime [0] LocalTimeStamp,

  utcTime [1] UTCTime
}

LocalTimeStamp ::= SEQUENCE
{
  generalizedTime [0] GeneralizedTime,
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.

  winterSummerIndication [1] ENUMERATED
  {
    notProvided(0),
    winterTime(1),
    summerTime(2),
    ...
  }
}

PartyInformation ::= SEQUENCE
{
  party-Qualifier [0] ENUMERATED
  {
    originating-Party(0),
    -- In this case, the partyInformation parameter provides the identities related to
    -- the originating party and all information provided by this party.
```

```
    -- This parameter provides also all the information concerning the redirecting
    -- party when a forwarded call reaches a target.
    terminating-Party(1),
    -- In this case, the partyInformation parameter provides the identities related to
    -- the terminating party and all information provided by this party.
    forwarded-to-Party(2),
    -- In this case, the partyInformation parameter provides the identities related to
    -- the forwarded to party and parties beyond this one and all information
    -- provided by this parties, including the call forwarding reason.
    gPRS-Target(3),
    ...
  },

  partyIdentity [1] SEQUENCE
  {
    imei [1] OCTET STRING (SIZE (8)) OPTIONAL,
    -- See MAP format ETS 300 974 [32]

    tei [2] OCTET STRING (SIZE (1..15)) OPTIONAL,
    -- ISDN-based Terminal Equipment Identity

    imsi [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
    -- See MAP format ETS 300 974 [32] International Mobile
    -- Station Identity E.212 number beginning with Mobile Country Code

    callingPartyNumber [4] CallingPartyNumber OPTIONAL,
    -- The calling party format is used to transmit the identity of a calling party

    calledPartyNumber [5] CalledPartyNumber OPTIONAL,
    -- The called party format is used to transmit the identity of a called party or
    -- a forwarded to party.

    msISDN [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
    -- MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format ETS 300 974 [32], clause 14.7.8.
    ...,

    e164-Format [7] OCTET STRING (SIZE (1..25)) OPTIONAL,
    -- E164 address of the node in international format. Coded in the same format as
    -- the calling party number parameter of the ISUP (parameter part: EN 300 356 [5])

    sip-uri [8] OCTET STRING OPTIONAL,
    -- Session Initiation Protocol - Uniform Resource Identifier. See RFC 3261 [59].
    -- This parameter is duplicated from TS 133 108 [61].

    tel-url [9] OCTET STRING OPTIONAL
```

```
    -- See "URLs for Telephone Calls", RFC 3966 [68].
    -- This parameter is duplicated from TS 133 108 [61].
  },

  services-Information [2] Services-Information OPTIONAL,
  -- This parameter is used to transmit all the information concerning the
  -- complementary information associated to the basic call

  supplementary-Services-Information [3] Supplementary-Services OPTIONAL,
  -- This parameter is used to transmit all the information concerning the
  -- activation/invocation of supplementary services during a call or out-of call not
  -- provided by the previous parameters.

  services-Data-Information [4] Services-Data-Information OPTIONAL,
  -- This parameter is used to transmit all the information concerning the complementary
  -- information associated to the basic data call.
  partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity OPTIONAL,
  ...
}

PartyExtendedIdentity ::= SEQUENCE
{
  subscriptionType [1] ENUMERATED
  {
    postpaid (0),
    prepaid  (1),
    ...
  } OPTIONAL,

  activationDate [2] TimeStamp OPTIONAL,
  deactivationDate [3] TimeStamp OPTIONAL,
  subscriber [4] Subscriber OPTIONAL,
  postalAddress [5] PostalAddress OPTIONAL,
  mailAddress [6] PostalAddress OPTIONAL,
  ...
}

Subscriber ::= CHOICE
{
  company [1] Company,
  person [2] Person,
  ...
}

Company ::= SEQUENCE
{
```

```
  name [0] UTF8String,
  regon      [1] OCTET STRING (SIZE (5)),
  -- BCD coded 9 digits
  -- F digit not used
  ...
}

Person ::= SEQUENCE
{
  firstName [0] UTF8String,
  surname [1] UTF8String,
  pesel       [2] OCTET STRING (SIZE (6)) OPTIONAL,
  -- BCD coded 11 digits
  -- F digit not used
  passportNumber [3] OCTET STRING (SIZE (7..14)) OPTIONAL,
  -- ASCII coded
  ...
}

PostalAddress ::= SEQUENCE
{
  street [1] UTF8String OPTIONAL,
  buildingNumber [2] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  apartmentNumber [3] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  postcode [4] OCTET STRING (SIZE (1..8)) OPTIONAL,
  city [5] UTF8String OPTIONAL,
  country [6] UTF8String OPTIONAL
}

CallingPartyNumber ::= CHOICE
{
  iSUP-Format [1] OCTET STRING (SIZE (1..25)),
  -- Encoded in the same format as the calling party number (parameter field)
  -- of the ISUP (see EN 300 356 [5]).

  dSS1-Format [2] OCTET STRING (SIZE (1..25)),
  -- Encoded in the format defined for the value part of the Calling party number
  -- information element of DSS1 protocol EN 300 403-1 [6].
  -- The DSS1 Information element identifier and the DSS1 length are not included.
  ...,

  mAP-Format [3] OCTET STRING (SIZE (1..25))
  -- Encoded as AddressString of the MAP protocol ETS 300 974 [32].
}
```

```
CalledPartyNumber ::= CHOICE
{
  iSUP-Format [1] OCTET STRING (SIZE (1..25)),
  -- Encoded in the same format as the called party number (parameter field)
  -- of the ISUP (see EN 300 356 [5]).

  mAP-Format [2] OCTET STRING (SIZE (1..25)),
  -- Encoded as AddressString of the MAP protocol ETS 300 974 [32].

  dSS1-Format [3] OCTET STRING (SIZE (1..25)),
  -- Encoded in the format defined for the value part of the Called party number
information
  -- element of DSS1 protocol EN 300 403-1 [6].
  -- The DSS1 Information element identifier and the DSS1 length are not included.
  ...
}

Location ::= SEQUENCE
{
  e164-Number [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
  -- Coded in the same format as the ISUP location number (parameter
  --field) of the ISUP (see EN 300 356 [5]).

  globalCellID [2] OCTET STRING (SIZE (5..7)) OPTIONAL,
  -- See MAP format (see ETS 300 974 [32]).
  -- Refers to Cell Global Identification defined in TS GSM 03.03.
  -- Octets are coded according to TS GSM 04.08.
  -- The internal structure is defined as follows:
  -- Mobile Country Code: 3 digits according to CCITT Rec E.212
  -- 1 digit filler (1111)
  -- Mobile Network Code: 2 digits according to CCITT Rec E.212
  -- Location Area Code: 2 octets according to TS GSM 04.08
  -- Cell Identity: 2 octets (CI) according to TS GSM 04.08

  tetraLocation [3] TetraLocation OPTIONAL,

  rAI [4] OCTET STRING (SIZE (6)) OPTIONAL,
  -- The Routeing Area Identifier (RAI) in the current SGSN is coded in accordance with
  -- TS 124 008 [41] without the Routing Area Identification IEI (only the
  -- last 6 octets are used).

  gsmLocation [5] GSMLocation OPTIONAL,

  umtsLocation [6] UMTSLocation OPTIONAL,
```

```
  sAI [7] OCTET STRING (SIZE (7)) OPTIONAL,
  -- format: PLMN-ID 3 octets (no. 1-3),
  -- LAC 2 octets (no. 4-5),
  -- SAC 2 octets (no. 6-7)
  -- (according to 3GPP TS 125 431 [62]).

  oldRAI [8] OCTET STRING (SIZE (6)) OPTIONAL,
  -- the "Routeing Area Identifier" in the old SGSN is coded in accordance with
  -- TS 124 008 (41) without the Routing Area Identification IEI
  -- (only the last 6 octets are used).
  -- This parameter is duplicated from TS 133 108 [61].

TetraLocation ::= CHOICE
{
  ms-Loc [1] SEQUENCE
  {
    mcc [1] INTEGER (0..1023),
    -- 10 bits EN 300 392-1 [40]
    mnc [2] INTEGER (0..16383),
    -- 14 bits EN 300 392-1 [40]
    lai [3] INTEGER (0..65535),
    -- 14 bits EN 300 392-1 [40]
    ci [4] INTEGER OPTIONAL
  },
  -- (to be completed)

  ls-Loc [2] INTEGER
  -- (to be confirmed and completed)
}

GSMLocation ::= CHOICE
{
  geoCoordinates [1] SEQUENCE
  {
    latitude [1] PrintableString (SIZE(7..10)),
    -- format: XDDMMSS.SS

    longitude [2] PrintableString (SIZE(8..11)),
    -- format: XDDDMMSS.SS

    mapDatum [3] MapDatum DEFAULT wGS84,
    ...,
    azimuth [4] INTEGER (0..359) OPTIONAL
    -- The azimuth is the bearing, relative to true north.
  },
  -- format: XDDDMMSS.SS
```

```
  -- X : N(orth), S(outh), E(ast), W(est)
  -- DD or DDD : degrees (numeric characters)
  -- MM : minutes (numeric characters)
  -- SS.SS : seconds, the second part (.SS) is optional
  -- Example:
  -- latitude short form N502312
  -- longitude long form E1122312.18

  utmCoordinates [2] SEQUENCE
  {
    utm-East [1] PrintableString (SIZE(10)),

    utm-North [2] PrintableString (SIZE(7)),
    -- Universal Transverse Mercator
    -- example utm-East 32U0439955
    -- utm-North 5540736

    mapDatum [3] MapDatum DEFAULT wGS84,
    ...,
    azimuth [4] INTEGER (0..359) OPTIONAL
    -- The azimuth is the bearing, relative to true north.
  },

  utmRefCoordinates [3] SEQUENCE
  {
    utmref-string PrintableString (SIZE(13)),
    mapDatum MapDatum DEFAULT wGS84,
    ...
  },
  -- example 32UPU91294045

  wGS84Coordinates [4] OCTET STRING
  -- format is as defined in TS 101 109 [57]; polygon type of shape is not allowed.
}

MapDatum ::= ENUMERATED
{
  wGS84,
  -- World Geodetic System 1984
  wGS72,
  eD50,
  -- European Datum 50
  ...
}

UMTSLocation ::= CHOICE
```

```
{
  point [1] GA-Point,

  pointWithUnCertainty [2] GA-PointWithUnCertainty,

  polygon [3] GA-Polygon,
  ...
}

GeographicalCoordinates ::= SEQUENCE
{
  latitudeSign ENUMERATED
  {
    north,
    south
  },

  latitude INTEGER (0..8388607),

  longitude INTEGER (-8388608..8388607),
  ...
}

GA-Point ::= SEQUENCE
{
  geographicalCoordinates GeographicalCoordinates,
  ...
}

GA-PointWithUnCertainty ::=SEQUENCE
{
  geographicalCoordinates GeographicalCoordinates,

  uncertaintyCode INTEGER (0..127)
}

maxNrOfPoints INTEGER ::= 15

GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF SEQUENCE
{
  geographicalCoordinates GeographicalCoordinates,
  ...
}

CallContentLinkCharacteristics ::= SEQUENCE
{
```

```
  cCLink-State [1] CCLink-State OPTIONAL,
  -- current state of the CCLink

  release-Time [2] TimeStamp OPTIONAL,
  -- date and time of the release of the Call Content Link.

  release-Reason [3] OCTET STRING (SIZE(2)) OPTIONAL,
  -- Release cause coded in Q.850 [31] format.

  lEMF-Address [4] CalledPartyNumber OPTIONAL,
  -- Directory number used to route the call toward the LEMF.
  ...
}

CCLink-State ::= ENUMERATED
{
  setUpInProcess(1),
  -- The set-up of the call is in process.
  callActive(2),
  callReleased(3),
  lack-of-resource(4),
  -- The lack-of-resource state is sent when a CC Link cannot
  -- be established because of lack of resource at the MF level.
  ...
}

Intercepted-Call-State ::= ENUMERATED
{
  idle(1),
  -- When the intercept call is released, the state is IDLE and the reason is provided
  -- by the release-Reason-Of-Intercepted-Call parameter.
  setUpInProcess(2),
  -- The set-up of the call is in process.
  connected(3),
  -- The answer has been received.
  ...
}

Services-Information ::= SEQUENCE
{
  iSUP-parameters [1] ISUP-parameters OPTIONAL,

  dSS1-parameters-codeset-0 [2] DSS1-parameters-codeset-0 OPTIONAL,
  ...,
  mAP-parameters [3] MAP-parameters OPTIONAL
}
```

```
ISUP-parameters ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one additional ISUP parameter TLV coded not already
defined in
-- the previous parameters. The Tag value is the one given in EN 300 356 [5].
-- In version 1 of the present document "iSUP-parameters" is defined as mandatory.
-- It might occur that no ISUP parameter is available. In that case in a version 1
-- implementation the value "zero" may be included in the first octet string of the SET.
-- The Length and the Value are coded in accordance with the parameter definition in
-- EN 300 356 [5]. Hereafter are listed the main parameters.
-- However other parameters may be added:
-- Transmission medium requirement: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "calling party".
-- Transmission medium requirement prime: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "calling party".

DSS1-parameters-codeset-0 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-0. The parameter is
coded as
-- described in EN 300 403-1 [6] (The DSS1 Information element identifier and the DSS1
length
-- are included). Hereafter are listed the main parameters
-- (However other parameters may be added):
-- Bearer capability: this parameter may be repeated. Format defined in EN 300 403-1 [6].
-- This parameter can be provided with the "Party Information" of the "calling party",
-- "called party" or "forwarded to party".
-- High Layer Compatibility: this parameter may be repeated. Format defined in EN 300
403-1 [6]
-- This parameter can be provided with the "Party Information" of the "calling party",
-- "called party" or "forwarded to party".
-- Low Layer capability: this parameter may be repeated. Format defined in EN 300 403-1
[6].
-- This parameter can be provided with the "Party Information" of the "calling party",
-- "called party" or "forwarded to party".

MAP-parameters ::= SET SIZE (1..256) OF OCTET STRING (SIZE(1..256))
-- Each "OCTET STRING" contains one MAP parameter. The parameter is coded as described in
-- ETS 300 974 [32] (The map-TS-Code is included).

Supplementary-Services ::= SEQUENCE
{
  standard-Supplementary-Services [1] Standard-Supplementary-Services OPTIONAL,
  non-Standard-Supplementary-Services [2] Non-Standard-Supplementary-Services OPTIONAL,
  other-Services [3] Other-Services OPTIONAL,
  ...
}
```

```
Standard-Supplementary-Services ::= SEQUENCE
{
  iSUP-SS-parameters [1] ISUP-SS-parameters OPTIONAL,
  dSS1-SS-parameters-codeset-0 [2] DSS1-SS-parameters-codeset-0 OPTIONAL,
  dSS1-SS-parameters-codeset-4 [3] DSS1-SS-parameters-codeset-4 OPTIONAL,
  dSS1-SS-parameters-codeset-5 [4] DSS1-SS-parameters-codeset-5 OPTIONAL,
  dSS1-SS-parameters-codeset-6 [5] DSS1-SS-parameters-codeset-6 OPTIONAL,
  dSS1-SS-parameters-codeset-7 [6] DSS1-SS-parameters-codeset-7 OPTIONAL,
  dSS1-SS-Invoke-components [7] DSS1-SS-Invoke-Components OPTIONAL,
  mAP-SS-Parameters [8] MAP-SS-Parameters OPTIONAL,
  mAP-SS-Invoke-Components [9] MAP-SS-Invoke-Components OPTIONAL,
  ...
}

Non-Standard-Supplementary-Services ::= SET SIZE (1..20) OF CHOICE
{
  simpleIndication [1] SimpleIndication,
  sciData [2] SciDataMode,
  ...
}

Other-Services ::= SET SIZE (1..50) OF OCTET STRING (SIZE (1..256))
-- Reference manufacturer manuals.

ISUP-SS-parameters ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- It must be noticed this parameter is retained for compatibility reasons.
-- It is recommended not to use it in new work but to use ISUP-parameters parameter.
-- Each "OCTET STRING" contains one additional ISUP parameter TLV coded not already
defined in
-- the previous parameters. The Tag value is the one given in EN 300 356 [5].
-- The Length and the Value are coded in accordance with the parameter definition in EN
300 356 [5].
-- Hereafter are listed the main parameters. However other parameters may be added:
-- Connected Number: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "called party" or "forwarded to party".
-- RedirectingNumber: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "originating
party".
-- Original Called Party Number: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "originating
party".
-- Redirection information: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "originating party", "forwarded to party" or/and "Terminating party".
```

```
-- Redirection Number: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "forwarded to party" or "Terminating party".
-- Call diversion information: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "forwarded to party" or "Terminating party".
-- Generic Number: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "calling party", "called party" or "forwarded to party".
-- This parameters are used to transmit additional identities (additional, calling party
-- number, additional called number, …).
-- Generic Notification: format defined in EN 300 356 [5].
-- This parameter may be provided with the "Party Information" of the
-- "calling party", "called party" or "forwarded to party".
-- This parameters transmit the notification to the other part of the call of the
supplementary
-- services activated or invoked by a subscriber during the call.
-- CUG Interlock Code: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "calling party".

DSS1-SS-parameters-codeset-0 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-0. The parameter is
coded as
-- described in EN 300 403-1 [6] (The DSS1 Information element identifier and the DSS1
length
-- are included). Hereafter are listed the main parameters (However other parameters may
be added):
-- Calling Party Subaddress: format defined in EN 300 403-1 [6].
-- This parameter can be provided with the "Party Information" of the "calling party".
-- Called Party Subaddress: format defined in EN 300 403-1 [6].
-- This parameter can be provided with the "Party Information" of the "calling party".
-- Connected Subaddress: format defined in recommendation (see EN 300 097-1 [14]).
-- This parameter can be provided with the "Party Information" of the
-- "called party" or "forwarded to party".
-- Connected Number: format defined in recommendation (see EN 300 097-1 [14]).
-- This parameter can be provided with the "Party Information" of the
-- "called party" or "forwarded to party".
-- Keypad facility: format defined in EN 300 403-1 [6].
-- This parameter can be provided with the "Party Information" of the
-- "calling party", "called party" or "forwarded to party".
-- Called Party Number: format defined in EN 300 403-1 [6].
-- This parameter could be provided with the "Party Information" of the "calling party"
-- when target is the originating party; it contains the dialled digits before
modification
-- at network level (e.g. IN interaction, translation, etc …).
-- User-user: format defined in EN 300 286-1 [23]).
```

```
-- This parameter can be provided with the "Party Information" of the
-- "calling party", "called party" or "forwarded to party".

DSS1-SS-parameters-codeset-4 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-4. The parameter is
coded as
-- described in the relevant recommendation.

DSS1-SS-parameters-codeset-5 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-5. The parameter is
coded as
-- described in the relevant national recommendation.

DSS1-SS-parameters-codeset-6 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-6. The parameter is
coded as
-- described in the relevant local network recommendation.

DSS1-SS-parameters-codeset-7 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one DSS1 parameter of the codeset-7. The parameter is
coded as
-- described in the relevant user specific recommendation.

DSS1-SS-Invoke-Components ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one DSS1 Invoke or Return Result component.
-- The invoke or return result component is coded as
-- described in the relevant DSS1 supplementary service recommendation.
-- Invoke or Return Result component (BeginCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (AddCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (SplitCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (DropCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (IsolateCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (ReattachCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (PartyDISC): EN 300 185-1 [19]
-- Invoke or Return Result component (MCIDRequest): EN 300 130-1 [16]
-- Invoke or Return Result component (Begin3PTY): EN 300 188-1 [20]
-- Invoke or Return Result component (End3PTY): EN 300 188-1 [20]
-- Invoke or Return Result component (ECTExecute): EN 300 369-1 [25]
-- Invoke or Return Result component (ECTInform): EN 300 369-1 [25]
-- Invoke or Return Result component (ECTLinkIdRequest): EN 300 369-1 [25]
-- Invoke or Return Result component (ECTLoopTest): EN 300 369-1 [25]
-- Invoke or Return Result component (ExplicitECTExecute): EN 300 369-1 [25]
-- Invoke or Return Result component (ECT: RequestSubaddress): EN 300 369-1 [25]
-- Invoke or Return Result component (ECT: SubaddressTransfer): EN 300 369-1 [25]
-- Invoke or Return Result component (CF: ActivationDiversion): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: DeactivationDiversion): EN 300 207-1 [21]
```

```
-- Invoke or Return Result component (CF: ActivationStatusNotification): EN 300 207-1
[21]
-- Invoke or Return Result component (CF: DeactivationStatusNotification): EN 300 207-1
[21]
-- Invoke or Return Result component (CF: InterrogationDiversion): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: InterrogationServedUserNumber): EN 300 207-1
[21]
-- Invoke or Return Result component (CF: DiversionInformation): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: CallDeflection): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: CallRerouteing): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: DivertingLegInformation1): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: DivertingLegInformation2): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: DivertingLegInformation3): EN 300 207-1 [21]
-- other invoke or return result components ...

MAP-SS-Invoke-Components ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one MAP Invoke or Return Result component.
-- The invoke or return result component is coded as
-- described in the relevant MAP supplementary service recommendation.

MAP-SS-Parameters ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one MAP Parameter. The parameter is coded as
-- described in the relevant MAP supplementary service recommendation.

SimpleIndication ::= ENUMERATED
{
  call-Waiting-Indication(0),
  -- The target has received a call waiting indication for this call
  add-conf-Indication(1),
  -- this call has been added to a conference
  call-on-hold-Indication(2),
  -- indication that this call is on hold
  retrieve-Indication(3),
  -- indication that this call has been retrieved
  suspend-Indication(4),
  -- indication that this call has been suspended
  resume-Indication(5),
  -- indication that this call has been resumed
  answer-Indication(6),
  -- indication that this call has been answered
  ...
}

SciDataMode ::= OCTET STRING (SIZE (1..256))

SMS-report ::= SEQUENCE
```

```
{
  communicationIdentifier [1] CommunicationIdentifier,
  -- used to uniquely identify an intercepted call: the same used for the
  -- relevant IRI
  -- Called "callIdentifier" in Edition 1 (v.1.1.1) ES 201 671.

  timeStamp [2] TimeStamp,
  -- date and time of the report. The format is
  -- the one defined in case a) of the ASN.1 recommendation X.680 [33].
  -- (year month day hour minutes seconds)

  sMS-Contents [3] SEQUENCE
  {
    initiator [1] ENUMERATED
    {
      -- party which sent the SMS
      target(0),
      server(1),
      undefined-party(2),
      ...
    },

    transfer-status [2] ENUMERATED
    {
      succeed-transfer(0),
      --the transfer of the SMS message succeeds
      not-succeed-transfer(1),
      undefined(2),
      ...
    } OPTIONAL,

    other-message [3] ENUMERATED
    {
      -- In case of terminating call, indicates if the server will send other SMS.
      yes(0),
      no(1),
      undefined(2),
      ...
    } OPTIONAL,

    content [4] OCTET STRING (SIZE (1..270)) OPTIONAL,
    -- Encoded in the format defined for the SMS mobile.
    ...
  }
}
```

```
LawfulInterceptionIdentifier ::= OCTET STRING (SIZE (1..25))
-- It is recommended to use ASCII characters in "a"…"z", "A"…"Z", "-", "_", ".", and
"0"…"9".
-- For subaddress option only "0"..."9" shall be used.
-- 17 znakow numerycznych ASCII
-- format: LEAID + TARGET(SEQ)
-- TARGET - (15 znakow) nadawany sekwencyjnie dla kazdego LEAID
-- LEAID -(2 znaki) 00 – LEMF operatora, 01 - ABW, 02 - Policja, 03 - CBŚ, 04 - SG, 05 -
CBA, 06 - SKW

National-Parameters ::= SET SIZE (1..40) OF OCTET STRING (SIZE (1..256))
-- Content defined by national law.

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))

GPRSEvent ::= ENUMERATED
{
  pDPContextActivation(1),
  startOfInterceptionWithPDPContextActive(2),
  pDPContextDeactivation(4),
  gPRSAttach(5),
  gPRSDetach(6),
  cellOrRAUpdate(10),
  sMS(11),
  ...,
  pDPContextModification(13)
}
-- see TS 101 509 [42]

Services-Data-Information ::= SEQUENCE
{
  gPRS-parameters [1] GPRS-parameters OPTIONAL,
  ...
}

GPRS-parameters ::= SEQUENCE
{
  pDP-address-allocated-to-the-target [1] DataNodeAddress OPTIONAL,
  aPN [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
  pDP-type [3] OCTET STRING (SIZE(2)) OPTIONAL,
  ...
}

GPRSOperationErrorCode ::= OCTET STRING (SIZE(2))
-- Refer to TS 124 008 [41] for values (GMM cause or SM cause parameter).
```

```
DataNodeAddress ::= CHOICE
{
  ipAddress [1] IPAddress,
  x25Address [2] X25Address,
  ...
}

IPAddress ::= SEQUENCE
{
  iP-type [1] ENUMERATED
  {
    iPV4(0),
    iPV6(1),
    ...
  },

  iP-value [2] IP-value,

  iP-assignment [3] ENUMERATED
  {
    static(1),
    -- The static coding shall be used to report a static address.
    dynamic(2),
    -- The dynamic coding shall be used to report a dynamically allocated address.
    notKnown(3),
    -- The notKnown coding shall be used to report other then static or dynamically
    -- allocated IP addresses.
    ...
  } OPTIONAL,
  ...
}

IP-value ::= CHOICE
{
  iPBinaryAddress [1] OCTET STRING (SIZE(4..16)),
  iPTextAddress [2] IA5String (SIZE(7..45)),
  ...
}

X25Address ::= OCTET STRING (SIZE(1..25))

National-HI2-ASN1parameters ::= SEQUENCE
{
  countryCode [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [67],
  -- the country to which the parameters inserted after the extension marker apply.
```

```
  ...
  -- In case a given country wants to use additional national parameters according to its
law,
  -- these national parameters should be defined using the ASN.1 syntax and added after
the
  -- extension marker (...).
  -- It is recommended that "version parameter" and "vendor identification parameter" are
  -- included in the national parameters definition. Vendor identifications can be
  -- retrieved from the IANA web site (see annex H). Besides, it is recommended to avoid
  -- using tags from 240 to 255 in a formal type definition.
}

UmtsQos ::= CHOICE
{
  qosMobileRadio [1] OCTET STRING,
  -- The qosMobileRadio parameter shall be coded in accordance with the § 10.5.6.5 of
  -- document [9] without the Quality of service IEI and Length of
  -- quality of service IE (. That is, first
  -- two octets carrying 'Quality of service IEI' and 'Length of quality of service
  -- IE' shall be excluded).

  qosGn [2] OCTET STRING
  -- qosGn parameter shall be coded in accordance with § 7.7.34 of document [17]
}

IMSevent ::= ENUMERATED
{
  unfilteredSIPmessage (1),
  -- This value indicates to LEMF that the whole SIP message is sent.
  ...,
  sIPheaderOnly (2)
  -- If warrant requires only IRI then specific content in a 'sIPMessage'
  -- (e.g. 'Message', etc.) has been deleted before sending it to LEMF.
}

LDIevent ::= ENUMERATED
{
  targetEntersIA (1),
  targetLeavesIA (2),
  ...
}

CorrelationValues ::= CHOICE
{
  iri-to-CC [0] IRI-to-CC-Correlation,
  -- correlates IRI to Content(s)
```

```
  iri-to-iri [1] IRI-to-IRI-Correlation,
  -- correlates IRI to IRI
  both-IRI-CC [2] SEQUENCE
  {
    -- correlates IRI to IRI and IRI to Content(s)
    iri-CC [0] IRI-to-CC-Correlation,
    iri-IRI [1] IRI-to-IRI-Correlation
  }
}

IRI-to-CC-Correlation ::= SEQUENCE
{
  -- correlates IRI to Content
  cc [0] SET OF OCTET STRING,
  -- correlates IRI to multiple CCs

  iri [1] OCTET STRING OPTIONAL
  -- correlates IRI to CC with signaling
}

IRI-to-IRI-Correlation ::= OCTET STRING
-- correlates IRI to IRI


END -- of HI2Operations
CS, PS
```

```
HI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) hi2(1) version9(9)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- ==============================
-- Object Identifier Definitions
-- ==============================

-- LawfulIntercept DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4)
etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
hi2DomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId hi2(1)}
```

```
hi2OperationId OBJECT IDENTIFIER ::= {hi2DomainId version9(9)}

IRIsContent ::= CHOICE
{
  iRIContent IRIContent,
  iRISequence IRISequence -- NOT USED
}

IRISequence ::= SEQUENCE OF IRIContent -- NOT USED
-- Aggregation of IRIContent is an optional feature.
-- It may be applied in cases when at a given point in time several IRI records are
-- available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent immediately and shall
-- not held in the DF or MF in order to apply aggregation.
-- When aggregation is not to be applied, IRIContent needs to be chosen.

IRIContent ::= CHOICE
{
  iRI-Begin-record [1] IRI-Parameters,
  -- At least one optional parameter must be included within the iRI-Begin-Record.
  iRI-End-record [2] IRI-Parameters,
  iRI-Continue-record [3] IRI-Parameters,
  -- At least one optional parameter must be included within the iRI-Continue-Record.
  iRI-Report-record [4] IRI-Parameters,
  -- At least one optional parameter must be included within the iRI-Report-Record.
  ...
}

IRI-Parameters ::= SEQUENCE
{
  domainID [0] OBJECT IDENTIFIER (hi2OperationId) OPTIONAL,
  -- for the sending entity the inclusion of the Object Identifier is mandatory
  iRIversion [23] ENUMERATED
  {
    version2(2),
    ...,
    version3(3),
    version4(4),
    version5(5),
    version6(6),
    version7(7),
    lastVersion(8)
  } OPTIONAL,
  -- Optional parameter "iRIversion" (tag 23) is redundant starting from TS 101 671
v2.4.1
  -- where to the object identifier "domainID" was introduced into IRI-Parameters.
```

```
  -- In order to keep backward compatibility, even when the version of the "domainID"
  -- parameter will be incremented it is recommended to always send to LEMF the same:
  -- enumeration value "lastVersion(8)".
  -- if not present, it means version 1 is handled

  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is associated to the target.

  communicationIdentifier [2] CommunicationIdentifier,
  -- used to uniquely identify an intercepted call.
  -- Called "callIdentifier" in Edition 1 of ES 201 671.

  timeStamp [3] TimeStamp,
  -- date and time of the event triggering the report.

  intercepted-Call-Direct [4] ENUMERATED
  {
    not-Available(0),
    originating-Target(1),
    -- In case of GPRS, this indicates that the PDP context activation, modification
    -- or deactivation is MS requested.
    terminating-Target(2),
    -- In case of GPRS, this indicates that the PDP context activation, modification
    -- or deactivation is network initiated.
    ...
  } OPTIONAL,

  intercepted-Call-State [5] Intercepted-Call-State OPTIONAL,

  ringingDuration [6] OCTET STRING (SIZE (3)) OPTIONAL, -- NOT USED
  -- Duration in seconds. BCD coded : HHMMSS

  conversationDuration [7] OCTET STRING (SIZE (3)) OPTIONAL, -- NOT USED
  -- Duration in seconds. BCD coded : HHMMSS

  locationOfTheTarget [8] Location OPTIONAL,
  -- location of the target subscriber

  partyInformation [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
  -- This parameter provides the concerned party (Originating, Terminating or forwarded
  -- party), the identity(ies) of the party and all the information provided by the
party.

  callContentLinkInformation [10] SEQUENCE
  {
    cCLink1Characteristics [1] CallContentLinkCharacteristics OPTIONAL,
```

```
    -- Information concerning the Content of Communication Link Tx channel established
    -- toward the LEMF (or the sum signal channel, in case of mono mode).

    cCLink2Characteristics [2] CallContentLinkCharacteristics OPTIONAL,
    -- Information concerning the Content of Communication Link Rx channel established
    -- toward the LEMF.
    ...
  } OPTIONAL, -- NOT USED

  release-Reason-Of-Intercepted-Call [11] OCTET STRING (SIZE (2)) OPTIONAL,
  -- Release cause coded in ITU-T Q.850 [31] format.
  -- This parameter indicates the reason why the intercepted call cannot be established
or
  -- why the intercepted call has been released after the active phase.

  nature-Of-The-intercepted-call [12] ENUMERATED
  {
    -- Nature of the intercepted "call":
    gSM-ISDN-PSTN-circuit-call(0),
    -- the possible UUS content is sent through the HI2 or HI3 "data" interface
    -- the possible call content call is established through the HI3 "circuit" interface
    gSM-SMS-Message(1),
    -- the SMS content is sent through the HI2 or HI3 "data" interface
    uUS4-Messages(2),
    -- the UUS content is sent through the HI2 or HI3 "data" interface
    tETRA-circuit-call(3),
    -- the possible call content call is established through the HI3 "circuit" interface
    -- the possible data are sent through the HI3 "data" interface
    teTRA-Packet-Data(4),
    -- the data are sent through the HI3 "data" interface
    gPRS-Packet-Data(5),
    -- the data are sent through the HI3 "data" interface
    ...,
    uMTS-circuit-call(6)
    -- the possible call content call is established through the HI3 "circuit" interface
    -- the possible data are sent through the HI3 "data" interface
  } OPTIONAL,

  serverCenterAddress [13] PartyInformation OPTIONAL,
  -- e.g. in case of SMS message this parameter provides the address of the relevant
  -- server within the calling (if server is originating) or called
  -- (if server is terminating) party address parameters

  sMS [14] SMS-report OPTIONAL,
  -- this parameter provides the SMS content and associated information
```

```
cC-Link-Identifier [15] CC-Link-Identifier OPTIONAL, -- NOT USED
-- Depending on a network option, this parameter may be used to identify a CC link
-- in case of multiparty calls.

national-Parameters [16] National-Parameters OPTIONAL, -- NOT USED

gPRSCorrelationNumber [18] GPRSCorrelationNumber OPTIONAL,

gPRSevent [20] GPRSEvent OPTIONAL,
-- This information is used to provide particular action of the target
-- such as attach/detach

sgsnAddress [21] DataNodeAddress OPTIONAL,

gPRSOperationErrorCode [22] GPRSOperationErrorCode OPTIONAL,
...,
ggsnAddress [24] DataNodeAddress OPTIONAL,

qOS [25] UmtsQos OPTIONAL,
-- This parameter is duplicated from TS 133 108 [61].

networkIdentifier [26] Network-Identifier OPTIONAL,
-- This parameter is duplicated from TS 133 108 [61].

sMSOriginatingAddress [27] DataNodeAddress OPTIONAL,
-- This parameter is duplicated from TS 133 108 [61].

sMSTerminatingAddress [28] DataNodeAddress OPTIONAL,
-- This parameter is duplicated from TS 133 108 [61].

iMSevent [29] IMSevent OPTIONAL,

sIPMessage [30] OCTET STRING OPTIONAL,
-- This parameter is duplicated from TS 133 108 [61].

servingSGSN-number [31] OCTET STRING (SIZE (1..20)) OPTIONAL,
-- This parameter is duplicated from TS 133 108 [61].

servingSGSN-address [32] OCTET STRING (SIZE (5..17)) OPTIONAL,
-- Octets are coded according to TS 123 003
-- This parameter is duplicated from TS 133 108 [61].
-- tARGETACTIVITYMONITOR [33] TARGETACTIVITYMONITOR OPTIONAL,
-- to be included after publication of the AT-D specification
-- Parameter is used in TS 101 909-20-1 [69]

ldiEvent [34] LDIevent OPTIONAL,
```

```
  -- The "Location Dependent Interception" parameter is duplicated from TS 133 108 [61].

  correlation [35] CorrelationValues OPTIONAL,
  -- This parameter is duplicated from TS 133 108 [61]

  national-HI2-ASN1parameters [255] National-HI2-ASN1parameters OPTIONAL
}

-- ==================
-- PARAMETERS FORMATS
-- ==================
CommunicationIdentifier ::= SEQUENCE
{
  communication-Identity-Number [0] OCTET STRING (SIZE (1..8)) OPTIONAL,
  -- Temporary Identifier of an intercepted call to uniquely identify an intercepted
call.
  -- This parameter is mandatory if there is associated
  -- information sent over HI3interface (CClink, data,..) or when
  -- CommunicationIdentifier is used for IRI other than IRI-Report-record
  -- This parameter was called "call-Identity-Number" in Edition 1 (v1.1.1) ES 201 671.
  -- The individual digits of the communication-Identity-Number shall be represented in
  -- ASCII format, e.g. "12345678" = 8 octets 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38.

  network-Identifier [1] Network-Identifier,
  ...
}
-- NOTE: The same "CommunicationIdentifier" value is sent :
-- with the HI3 information for correlation purpose between the IRI and the information
sent on
-- the HI3 interfaces (CCLink, data, ..) with each IRI associated to a same intercepted
call
-- for correlation purpose between the different IRI.

Network-Identifier ::= SEQUENCE
{
  operator-Identifier [0] OCTET STRING (SIZE (1..5)),
  -- It is a notification of the NWO/AP/SvP in ASCII- characters.
  -- The parameter is mandatory.
  -- format: MNC + MVNO
  network-Element-Identifier [1] Network-Element-Identifier OPTIONAL, -- NOT USED
  ...
}

Network-Element-Identifier ::= CHOICE
{
  e164-Format [1] OCTET STRING (SIZE (1..25)),
```

```
  -- E164 address of the node in international format. Coded in the same format as the
  -- calling party number parameter of the ISUP (parameter part: EN 300 356 [5]).

  x25-Format [2] OCTET STRING (SIZE (1..25)),
  -- X25 address

  iP-Format [3] OCTET STRING (SIZE (1..25)),
  -- IP address

  dNS-Format [4] OCTET STRING (SIZE (1..25)),
  -- DNS address
  ...,
  iP-Address [5] IPAddress,
  ...
}

CC-Link-Identifier ::= OCTET STRING (SIZE (1..8))
-- Depending on a network option, this parameter may be used to identify a CClink
-- in case of multiparty calls.
-- The individual digits of the communication-Identity-Number shall be represented in
-- ASCII format, e.g. "12345678" = 8 octets 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38.

TimeStamp ::= CHOICE
{
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.
  localTime [0] LocalTimeStamp,

  utcTime [1] UTCTime
}

LocalTimeStamp ::= SEQUENCE
{
  generalizedTime [0] GeneralizedTime,
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.

  winterSummerIndication [1] ENUMERATED
  {
    notProvided(0),
    winterTime(1),
    summerTime(2),
    ...
  }
```

```
}

PartyInformation ::= SEQUENCE
{
  party-Qualifier [0] ENUMERATED
  {
    originating-Party(0),
    -- In this case, the partyInformation parameter provides the identities related to
    -- the originating party and all information provided by this party.
    -- This parameter provides also all the information concerning the redirecting
    -- party when a forwarded call reaches a target.
    terminating-Party(1),
    -- In this case, the partyInformation parameter provides the identities related to
    -- the terminating party and all information provided by this party.
    forwarded-to-Party(2),
    -- In this case, the partyInformation parameter provides the identities related to
    -- the forwarded to party and parties beyond this one and all information
    -- provided by this parties, including the call forwarding reason.
    gPRS-Target(3),
    ...
  },

  partyIdentity [1] SEQUENCE
  {
    imei [1] OCTET STRING (SIZE (8)) OPTIONAL,
    -- See MAP format ETS 300 974 [32]

    tei [2] OCTET STRING (SIZE (1..15)) OPTIONAL,
    -- ISDN-based Terminal Equipment Identity

    imsi [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
    -- See MAP format ETS 300 974 [32] International Mobile
    -- Station Identity E.212 number beginning with Mobile Country Code

    callingPartyNumber [4] CallingPartyNumber OPTIONAL,
    -- The calling party format is used to transmit the identity of a calling party

    calledPartyNumber [5] CalledPartyNumber OPTIONAL,
    -- The called party format is used to transmit the identity of a called party or
    -- a forwarded to party.

    msISDN [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
    -- MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format ETS 300 974 [32], clause 14.7.8.
    ...,
```

```
    e164-Format [7] OCTET STRING (SIZE (1..25)) OPTIONAL,
    -- E164 address of the node in international format. Coded in the same format as
    -- the calling party number parameter of the ISUP (parameter part: EN 300 356 [5])

    sip-uri [8] OCTET STRING OPTIONAL,
    -- Session Initiation Protocol - Uniform Resource Identifier. See RFC 3261 [59].
    -- This parameter is duplicated from TS 133 108 [61].

    tel-url [9] OCTET STRING OPTIONAL
    -- See "URLs for Telephone Calls", RFC 3966 [68].
    -- This parameter is duplicated from TS 133 108 [61].
  },

  services-Information [2] Services-Information OPTIONAL,
  -- This parameter is used to transmit all the information concerning the
  -- complementary information associated to the basic call

  supplementary-Services-Information [3] Supplementary-Services OPTIONAL,
  -- This parameter is used to transmit all the information concerning the
  -- activation/invocation of supplementary services during a call or out-of call not
  -- provided by the previous parameters.

  services-Data-Information [4] Services-Data-Information OPTIONAL,
  -- This parameter is used to transmit all the information concerning the complementary
  -- information associated to the basic data call.
  partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity OPTIONAL,
  ...
}

PartyExtendedIdentity ::= SEQUENCE
{
  subscriptionType [1] ENUMERATED
  {
    postpaid (0),
    prepaid  (1),
    ...
  } OPTIONAL,

  activationDate [2] TimeStamp OPTIONAL,
  deactivationDate [3] TimeStamp OPTIONAL,
  subscriber [4] Subscriber OPTIONAL,
  postalAddress [5] PostalAddress OPTIONAL,
  mailAddress [6] PostalAddress OPTIONAL,
  ...
}
```

```
Subscriber ::= CHOICE
{
  company [1] Company,
  person [2] Person,
  ...
}

Company ::= SEQUENCE
{
  name [0] UTF8String,
  regon      [1] OCTET STRING (SIZE (5)),
  -- BCD coded 9 digits
  -- F digit not used
  ...
}

Person ::= SEQUENCE
{
  firstName [0] UTF8String,
  surname [1] UTF8String,
  pesel       [2] OCTET STRING (SIZE (6)) OPTIONAL,
  -- BCD coded 11 digits
  -- F digit not used
  passportNumber [3] OCTET STRING (SIZE (7..14)) OPTIONAL,
  -- ASCII coded
  ...
}

PostalAddress ::= SEQUENCE
{
  street [1] UTF8String OPTIONAL,
  buildingNumber [2] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  apartmentNumber [3] OCTET STRING (SIZE (1..10)) OPTIONAL,
  -- ASCII coded: 10 char
  postcode [4] OCTET STRING (SIZE (1..8)) OPTIONAL,
  city [5] UTF8String OPTIONAL,
  country [6] UTF8String OPTIONAL
}

CallingPartyNumber ::= CHOICE
{
  iSUP-Format [1] OCTET STRING (SIZE (1..25)),
  -- Encoded in the same format as the calling party number (parameter field)
  -- of the ISUP (see EN 300 356 [5]).
```

```
  dSS1-Format [2] OCTET STRING (SIZE (1..25)),
  -- Encoded in the format defined for the value part of the Calling party number
  -- information element of DSS1 protocol EN 300 403-1 [6].
  -- The DSS1 Information element identifier and the DSS1 length are not included.
  ...,

  mAP-Format [3] OCTET STRING (SIZE (1..25))
  -- Encoded as AddressString of the MAP protocol ETS 300 974 [32].
}

CalledPartyNumber ::= CHOICE
{
  iSUP-Format [1] OCTET STRING (SIZE (1..25)),
  -- Encoded in the same format as the called party number (parameter field)
  -- of the ISUP (see EN 300 356 [5]).

  mAP-Format [2] OCTET STRING (SIZE (1..25)),
  -- Encoded as AddressString of the MAP protocol ETS 300 974 [32].

  dSS1-Format [3] OCTET STRING (SIZE (1..25)),
  -- Encoded in the format defined for the value part of the Called party number
information
  -- element of DSS1 protocol EN 300 403-1 [6].
  -- The DSS1 Information element identifier and the DSS1 length are not included.
  ...
}

Location ::= SEQUENCE
{
  e164-Number [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
  -- Coded in the same format as the ISUP location number (parameter
  --field) of the ISUP (see EN 300 356 [5]).

  globalCellID [2] OCTET STRING (SIZE (5..7)) OPTIONAL,
  -- See MAP format (see ETS 300 974 [32]).
  -- Refers to Cell Global Identification defined in TS GSM 03.03.
  -- Octets are coded according to TS GSM 04.08.
  -- The internal structure is defined as follows:
  -- Mobile Country Code: 3 digits according to CCITT Rec E.212
  -- 1 digit filler (1111)
  -- Mobile Network Code: 2 digits according to CCITT Rec E.212
  -- Location Area Code: 2 octets according to TS GSM 04.08
  -- Cell Identity: 2 octets (CI) according to TS GSM 04.08

  tetraLocation [3] TetraLocation OPTIONAL,
```

```
  rAI [4] OCTET STRING (SIZE (6)) OPTIONAL,
  -- The Routeing Area Identifier (RAI) in the current SGSN is coded in accordance with
  -- TS 124 008 [41] without the Routing Area Identification IEI (only the
  -- last 6 octets are used).

  gsmLocation [5] GSMLocation OPTIONAL,

  umtsLocation [6] UMTSLocation OPTIONAL,

  sAI [7] OCTET STRING (SIZE (7)) OPTIONAL,
  -- format: PLMN-ID 3 octets (no. 1-3),
  -- LAC 2 octets (no. 4-5),
  -- SAC 2 octets (no. 6-7)
  -- (according to 3GPP TS 125 431 [62]).

  oldRAI [8] OCTET STRING (SIZE (6)) OPTIONAL,
  -- the "Routeing Area Identifier" in the old SGSN is coded in accordance with
  -- TS 124 008 (41) without the Routing Area Identification IEI
  -- (only the last 6 octets are used).
  -- This parameter is duplicated from TS 133 108 [61].

TetraLocation ::= CHOICE
{
  ms-Loc [1] SEQUENCE
  {
    mcc [1] INTEGER (0..1023),
    -- 10 bits EN 300 392-1 [40]
    mnc [2] INTEGER (0..16383),
    -- 14 bits EN 300 392-1 [40]
    lai [3] INTEGER (0..65535),
    -- 14 bits EN 300 392-1 [40]
    ci [4] INTEGER OPTIONAL
  },
  -- (to be completed)

  ls-Loc [2] INTEGER
  -- (to be confirmed and completed)
}

GSMLocation ::= CHOICE
{
  geoCoordinates [1] SEQUENCE
  {
    latitude [1] PrintableString (SIZE(7..10)),
    -- format: XDDMMSS.SS
```

```
    longitude [2] PrintableString (SIZE(8..11)),
    -- format: XDDDMMSS.SS

    mapDatum [3] MapDatum DEFAULT wGS84,
    ...,
    azimuth [4] INTEGER (0..359) OPTIONAL
    -- The azimuth is the bearing, relative to true north.
  },
  -- format: XDDDMMSS.SS
  -- X : N(orth), S(outh), E(ast), W(est)
  -- DD or DDD : degrees (numeric characters)
  -- MM : minutes (numeric characters)
  -- SS.SS : seconds, the second part (.SS) is optional
  -- Example:
  -- latitude short form N502312
  -- longitude long form E1122312.18

  utmCoordinates [2] SEQUENCE
  {
    utm-East [1] PrintableString (SIZE(10)),

    utm-North [2] PrintableString (SIZE(7)),
    -- Universal Transverse Mercator
    -- example utm-East 32U0439955
    -- utm-North 5540736

    mapDatum [3] MapDatum DEFAULT wGS84,
    ...,
    azimuth [4] INTEGER (0..359) OPTIONAL
    -- The azimuth is the bearing, relative to true north.
  },

  utmRefCoordinates [3] SEQUENCE
  {
    utmref-string PrintableString (SIZE(13)),
    mapDatum MapDatum DEFAULT wGS84,
    ...
  },
  -- example 32UPU91294045

  wGS84Coordinates [4] OCTET STRING
  -- format is as defined in TS 101 109 [57]; polygon type of shape is not allowed.
}

MapDatum ::= ENUMERATED
{
```

```
  wGS84,
  -- World Geodetic System 1984
  wGS72,
  eD50,
  -- European Datum 50
  ...
}

UMTSLocation ::= CHOICE
{
  point [1] GA-Point,

  pointWithUnCertainty [2] GA-PointWithUnCertainty,

  polygon [3] GA-Polygon,
  ...
}

GeographicalCoordinates ::= SEQUENCE
{
  latitudeSign ENUMERATED
  {
    north,
    south
  },

  latitude INTEGER (0..8388607),

  longitude INTEGER (-8388608..8388607),
  ...
}

GA-Point ::= SEQUENCE
{
  geographicalCoordinates GeographicalCoordinates,
  ...
}

GA-PointWithUnCertainty ::=SEQUENCE
{
  geographicalCoordinates GeographicalCoordinates,

  uncertaintyCode INTEGER (0..127)
}

maxNrOfPoints INTEGER ::= 15
```

```
GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF SEQUENCE
{
  geographicalCoordinates GeographicalCoordinates,
  ...
}

CallContentLinkCharacteristics ::= SEQUENCE
{
  cCLink-State [1] CCLink-State OPTIONAL,
  -- current state of the CCLink

  release-Time [2] TimeStamp OPTIONAL,
  -- date and time of the release of the Call Content Link.

  release-Reason [3] OCTET STRING (SIZE(2)) OPTIONAL,
  -- Release cause coded in Q.850 [31] format.

  lEMF-Address [4] CalledPartyNumber OPTIONAL,
  -- Directory number used to route the call toward the LEMF.
  ...
}

CCLink-State ::= ENUMERATED
{
  setUpInProcess(1),
  -- The set-up of the call is in process.
  callActive(2),
  callReleased(3),
  lack-of-resource(4),
  -- The lack-of-resource state is sent when a CC Link cannot
  -- be established because of lack of resource at the MF level.
  ...
}

Intercepted-Call-State ::= ENUMERATED
{
  idle(1),
  -- When the intercept call is released, the state is IDLE and the reason is provided
  -- by the release-Reason-Of-Intercepted-Call parameter.
  setUpInProcess(2),
  -- The set-up of the call is in process.
  connected(3),
  -- The answer has been received.
  ...
}
```

```
Services-Information ::= SEQUENCE
{
  iSUP-parameters [1] ISUP-parameters OPTIONAL,

  dSS1-parameters-codeset-0 [2] DSS1-parameters-codeset-0 OPTIONAL,
  ...,
  mAP-parameters [3] MAP-parameters OPTIONAL
}

ISUP-parameters ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one additional ISUP parameter TLV coded not already
defined in
-- the previous parameters. The Tag value is the one given in EN 300 356 [5].
-- In version 1 of the present document "iSUP-parameters" is defined as mandatory.
-- It might occur that no ISUP parameter is available. In that case in a version 1
-- implementation the value "zero" may be included in the first octet string of the SET.
-- The Length and the Value are coded in accordance with the parameter definition in
-- EN 300 356 [5]. Hereafter are listed the main parameters.
-- However other parameters may be added:
-- Transmission medium requirement: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "calling party".
-- Transmission medium requirement prime: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "calling party".

DSS1-parameters-codeset-0 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-0. The parameter is
coded as
-- described in EN 300 403-1 [6] (The DSS1 Information element identifier and the DSS1
length
-- are included). Hereafter are listed the main parameters
-- (However other parameters may be added):
-- Bearer capability: this parameter may be repeated. Format defined in EN 300 403-1 [6].
-- This parameter can be provided with the "Party Information" of the "calling party",
-- "called party" or "forwarded to party".
-- High Layer Compatibility: this parameter may be repeated. Format defined in EN 300
403-1 [6]
-- This parameter can be provided with the "Party Information" of the "calling party",
-- "called party" or "forwarded to party".
-- Low Layer capability: this parameter may be repeated. Format defined in EN 300 403-1
[6].
-- This parameter can be provided with the "Party Information" of the "calling party",
-- "called party" or "forwarded to party".

MAP-parameters ::= SET SIZE (1..256) OF OCTET STRING (SIZE(1..256))
-- Each "OCTET STRING" contains one MAP parameter. The parameter is coded as described in
```

```
-- ETS 300 974 [32] (The map-TS-Code is included).

Supplementary-Services ::= SEQUENCE
{
  standard-Supplementary-Services [1] Standard-Supplementary-Services OPTIONAL,
  non-Standard-Supplementary-Services [2] Non-Standard-Supplementary-Services OPTIONAL,
  other-Services [3] Other-Services OPTIONAL,
  ...
}

Standard-Supplementary-Services ::= SEQUENCE
{
  iSUP-SS-parameters [1] ISUP-SS-parameters OPTIONAL,
  dSS1-SS-parameters-codeset-0 [2] DSS1-SS-parameters-codeset-0 OPTIONAL,
  dSS1-SS-parameters-codeset-4 [3] DSS1-SS-parameters-codeset-4 OPTIONAL,
  dSS1-SS-parameters-codeset-5 [4] DSS1-SS-parameters-codeset-5 OPTIONAL,
  dSS1-SS-parameters-codeset-6 [5] DSS1-SS-parameters-codeset-6 OPTIONAL,
  dSS1-SS-parameters-codeset-7 [6] DSS1-SS-parameters-codeset-7 OPTIONAL,
  dSS1-SS-Invoke-components [7] DSS1-SS-Invoke-Components OPTIONAL,
  mAP-SS-Parameters [8] MAP-SS-Parameters OPTIONAL,
  mAP-SS-Invoke-Components [9] MAP-SS-Invoke-Components OPTIONAL,
  ...
}

Non-Standard-Supplementary-Services ::= SET SIZE (1..20) OF CHOICE
{
  simpleIndication [1] SimpleIndication,
  sciData [2] SciDataMode,
  ...
}

Other-Services ::= SET SIZE (1..50) OF OCTET STRING (SIZE (1..256))
-- Reference manufacturer manuals.

ISUP-SS-parameters ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- It must be noticed this parameter is retained for compatibility reasons.
-- It is recommended not to use it in new work but to use ISUP-parameters parameter.
-- Each "OCTET STRING" contains one additional ISUP parameter TLV coded not already
defined in
-- the previous parameters. The Tag value is the one given in EN 300 356 [5].
-- The Length and the Value are coded in accordance with the parameter definition in EN
300 356 [5].
-- Hereafter are listed the main parameters. However other parameters may be added:
-- Connected Number: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "called party" or "forwarded to party".
```

```
-- RedirectingNumber: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "originating
party".
-- Original Called Party Number: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "originating
party".
-- Redirection information: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "originating party", "forwarded to party" or/and "Terminating party".
-- Redirection Number: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "forwarded to party" or "Terminating party".
-- Call diversion information: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "forwarded to party" or "Terminating party".
-- Generic Number: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the
-- "calling party", "called party" or "forwarded to party".
-- This parameters are used to transmit additional identities (additional, calling party
-- number, additional called number, …).
-- Generic Notification: format defined in EN 300 356 [5].
-- This parameter may be provided with the "Party Information" of the
-- "calling party", "called party" or "forwarded to party".
-- This parameters transmit the notification to the other part of the call of the
supplementary
-- services activated or invoked by a subscriber during the call.
-- CUG Interlock Code: format defined in EN 300 356 [5].
-- This parameter can be provided with the "Party Information" of the "calling party".

DSS1-SS-parameters-codeset-0 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-0. The parameter is
coded as
-- described in EN 300 403-1 [6] (The DSS1 Information element identifier and the DSS1
length
-- are included). Hereafter are listed the main parameters (However other parameters may
be added):
-- Calling Party Subaddress: format defined in EN 300 403-1 [6].
-- This parameter can be provided with the "Party Information" of the "calling party".
-- Called Party Subaddress: format defined in EN 300 403-1 [6].
-- This parameter can be provided with the "Party Information" of the "calling party".
-- Connected Subaddress: format defined in recommendation (see EN 300 097-1 [14]).
-- This parameter can be provided with the "Party Information" of the
-- "called party" or "forwarded to party".
-- Connected Number: format defined in recommendation (see EN 300 097-1 [14]).
-- This parameter can be provided with the "Party Information" of the
-- "called party" or "forwarded to party".
```

```
-- Keypad facility: format defined in EN 300 403-1 [6].
-- This parameter can be provided with the "Party Information" of the
-- "calling party", "called party" or "forwarded to party".
-- Called Party Number: format defined in EN 300 403-1 [6].
-- This parameter could be provided with the "Party Information" of the "calling party"
-- when target is the originating party; it contains the dialled digits before
modification
-- at network level (e.g. IN interaction, translation, etc …).
-- User-user: format defined in EN 300 286-1 [23]).
-- This parameter can be provided with the "Party Information" of the
-- "calling party", "called party" or "forwarded to party".

DSS1-SS-parameters-codeset-4 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-4. The parameter is
coded as
-- described in the relevant recommendation.

DSS1-SS-parameters-codeset-5 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-5. The parameter is
coded as
-- described in the relevant national recommendation.

DSS1-SS-parameters-codeset-6 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset-6. The parameter is
coded as
-- described in the relevant local network recommendation.

DSS1-SS-parameters-codeset-7 ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one DSS1 parameter of the codeset-7. The parameter is
coded as
-- described in the relevant user specific recommendation.

DSS1-SS-Invoke-Components ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one DSS1 Invoke or Return Result component.
-- The invoke or return result component is coded as
-- described in the relevant DSS1 supplementary service recommendation.
-- Invoke or Return Result component (BeginCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (AddCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (SplitCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (DropCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (IsolateCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (ReattachCONF): EN 300 185-1 [19]
-- Invoke or Return Result component (PartyDISC): EN 300 185-1 [19]
-- Invoke or Return Result component (MCIDRequest): EN 300 130-1 [16]
-- Invoke or Return Result component (Begin3PTY): EN 300 188-1 [20]
-- Invoke or Return Result component (End3PTY): EN 300 188-1 [20]
```

```
-- Invoke or Return Result component (ECTExecute): EN 300 369-1 [25]
-- Invoke or Return Result component (ECTInform): EN 300 369-1 [25]
-- Invoke or Return Result component (ECTLinkIdRequest): EN 300 369-1 [25]
-- Invoke or Return Result component (ECTLoopTest): EN 300 369-1 [25]
-- Invoke or Return Result component (ExplicitECTExecute): EN 300 369-1 [25]
-- Invoke or Return Result component (ECT: RequestSubaddress): EN 300 369-1 [25]
-- Invoke or Return Result component (ECT: SubaddressTransfer): EN 300 369-1 [25]
-- Invoke or Return Result component (CF: ActivationDiversion): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: DeactivationDiversion): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: ActivationStatusNotification): EN 300 207-1
[21]
-- Invoke or Return Result component (CF: DeactivationStatusNotification): EN 300 207-1
[21]
-- Invoke or Return Result component (CF: InterrogationDiversion): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: InterrogationServedUserNumber): EN 300 207-1
[21]
-- Invoke or Return Result component (CF: DiversionInformation): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: CallDeflection): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: CallRerouteing): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: DivertingLegInformation1): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: DivertingLegInformation2): EN 300 207-1 [21]
-- Invoke or Return Result component (CF: DivertingLegInformation3): EN 300 207-1 [21]
-- other invoke or return result components ...

MAP-SS-Invoke-Components ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one MAP Invoke or Return Result component.
-- The invoke or return result component is coded as
-- described in the relevant MAP supplementary service recommendation.

MAP-SS-Parameters ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one MAP Parameter. The parameter is coded as
-- described in the relevant MAP supplementary service recommendation.

SimpleIndication ::= ENUMERATED
{
  call-Waiting-Indication(0),
  -- The target has received a call waiting indication for this call
  add-conf-Indication(1),
  -- this call has been added to a conference
  call-on-hold-Indication(2),
  -- indication that this call is on hold
  retrieve-Indication(3),
  -- indication that this call has been retrieved
  suspend-Indication(4),
  -- indication that this call has been suspended
  resume-Indication(5),
```

```
  -- indication that this call has been resumed
  answer-Indication(6),
  -- indication that this call has been answered
  ...
}

SciDataMode ::= OCTET STRING (SIZE (1..256))

SMS-report ::= SEQUENCE
{
  communicationIdentifier [1] CommunicationIdentifier,
  -- used to uniquely identify an intercepted call: the same used for the
  -- relevant IRI
  -- Called "callIdentifier" in Edition 1 (v.1.1.1) ES 201 671.

  timeStamp [2] TimeStamp,
  -- date and time of the report. The format is
  -- the one defined in case a) of the ASN.1 recommendation X.680 [33].
  -- (year month day hour minutes seconds)

  sMS-Contents [3] SEQUENCE
  {
    initiator [1] ENUMERATED
    {
      -- party which sent the SMS
      target(0),
      server(1),
      undefined-party(2),
      ...
    },

    transfer-status [2] ENUMERATED
    {
      succeed-transfer(0),
      --the transfer of the SMS message succeeds
      not-succeed-transfer(1),
      undefined(2),
      ...
    } OPTIONAL,

    other-message [3] ENUMERATED
    {
      -- In case of terminating call, indicates if the server will send other SMS.
      yes(0),
      no(1),
      undefined(2),
```

```
      ...
    } OPTIONAL,

    content [4] OCTET STRING (SIZE (1..270)) OPTIONAL,
    -- Encoded in the format defined for the SMS mobile.
    ...
  }
}

LawfulInterceptionIdentifier ::= OCTET STRING (SIZE (1..25))
-- It is recommended to use ASCII characters in "a"…"z", "A"…"Z", "-", "_", ".", and
"0"…"9".
-- For subaddress option only "0"..."9" shall be used.
-- 17 znakow numerycznych ASCII
-- format: LEAID + TARGET(SEQ)
-- TARGET - (15 znakow) nadawany sekwencyjnie dla kazdego LEAID
-- LEAID -(2 znaki) 00 – LEMF operatora, 01 - ABW, 02 - Policja, 03 - CBŚ, 04 - SG, 05 -
CBA, 06 - SKW

National-Parameters ::= SET SIZE (1..40) OF OCTET STRING (SIZE (1..256))
-- Content defined by national law.

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))

GPRSEvent ::= ENUMERATED
{
  pDPContextActivation(1),
  startOfInterceptionWithPDPContextActive(2),
  pDPContextDeactivation(4),
  gPRSAttach(5),
  gPRSDetach(6),
  cellOrRAUpdate(10),
  sMS(11),
  ...,
  pDPContextModification(13)
}
-- see TS 101 509 [42]

Services-Data-Information ::= SEQUENCE
{
  gPRS-parameters [1] GPRS-parameters OPTIONAL,
  ...
}

GPRS-parameters ::= SEQUENCE
{
```

```
  pDP-address-allocated-to-the-target [1] DataNodeAddress OPTIONAL,
  aPN [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
  pDP-type [3] OCTET STRING (SIZE(2)) OPTIONAL,
  ...
}

GPRSOperationErrorCode ::= OCTET STRING (SIZE(2))
-- Refer to TS 124 008 [41] for values (GMM cause or SM cause parameter).

DataNodeAddress ::= CHOICE
{
  ipAddress [1] IPAddress,
  x25Address [2] X25Address,
  ...
}

IPAddress ::= SEQUENCE
{
  iP-type [1] ENUMERATED
  {
    iPV4(0),
    iPV6(1),
    ...
  },

  iP-value [2] IP-value,

  iP-assignment [3] ENUMERATED
  {
    static(1),
    -- The static coding shall be used to report a static address.
    dynamic(2),
    -- The dynamic coding shall be used to report a dynamically allocated address.
    notKnown(3),
    -- The notKnown coding shall be used to report other then static or dynamically
    -- allocated IP addresses.
    ...
  } OPTIONAL,
  ...
}

IP-value ::= CHOICE
{
  iPBinaryAddress [1] OCTET STRING (SIZE(4..16)),
  iPTextAddress [2] IA5String (SIZE(7..45)),
  ...
```

```
}

X25Address ::= OCTET STRING (SIZE(1..25))

National-HI2-ASN1parameters ::= SEQUENCE
{
  countryCode [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [67],
  -- the country to which the parameters inserted after the extension marker apply.
  ...
  -- In case a given country wants to use additional national parameters according to its
law,
  -- these national parameters should be defined using the ASN.1 syntax and added after
the
  -- extension marker (...).
  -- It is recommended that "version parameter" and "vendor identification parameter" are
  -- included in the national parameters definition. Vendor identifications can be
  -- retrieved from the IANA web site (see annex H). Besides, it is recommended to avoid
  -- using tags from 240 to 255 in a formal type definition.
}

UmtsQos ::= CHOICE
{
  qosMobileRadio [1] OCTET STRING,
  -- The qosMobileRadio parameter shall be coded in accordance with the § 10.5.6.5 of
  -- document [9] without the Quality of service IEI and Length of
  -- quality of service IE (. That is, first
  -- two octets carrying 'Quality of service IEI' and 'Length of quality of service
  -- IE' shall be excluded).

  qosGn [2] OCTET STRING
  -- qosGn parameter shall be coded in accordance with § 7.7.34 of document [17]
}

IMSevent ::= ENUMERATED
{
  unfilteredSIPmessage (1),
  -- This value indicates to LEMF that the whole SIP message is sent.
  ...,
  sIPheaderOnly (2)
  -- If warrant requires only IRI then specific content in a 'sIPMessage'
  -- (e.g. 'Message', etc.) has been deleted before sending it to LEMF.
}

LDIevent ::= ENUMERATED
{
```

```
  targetEntersIA (1),
  targetLeavesIA (2),
  ...
}

CorrelationValues ::= CHOICE
{
  iri-to-CC [0] IRI-to-CC-Correlation,
  -- correlates IRI to Content(s)
  iri-to-iri [1] IRI-to-IRI-Correlation,
  -- correlates IRI to IRI
  both-IRI-CC [2] SEQUENCE
  {
    -- correlates IRI to IRI and IRI to Content(s)
    iri-CC [0] IRI-to-CC-Correlation,
    iri-IRI [1] IRI-to-IRI-Correlation
  }
}

IRI-to-CC-Correlation ::= SEQUENCE
{
  -- correlates IRI to Content
  cc [0] SET OF OCTET STRING,
  -- correlates IRI to multiple CCs

  iri [1] OCTET STRING OPTIONAL
  -- correlates IRI to CC with signaling
}

IRI-to-IRI-Correlation ::= OCTET STRING
-- correlates IRI to IRI


END -- of HI2Operations
```

Załącznik nr 3

Specyfikacja techniczna styku HI-3 interfejsu HI

I. Struktura Interfejsu HI3

1.Warstwa fizyczna

Warstwa fizyczna ma znaczenie lokalne pomiędzy dwoma urządzeniami sieciowymi i ma znaczenie tylko na styku systemów miedzy operatorem a uprawnionym podmiotem.

2. Warstwa sieciowa

Dla każdego podmiotu uprawnionego określone są dedykowane adresy publiczne IPv4 dla DF (HI2). Służby określają adresację publiczną IPv4 po swojej stronie. Adresy IP nie mogą być takie same dla wszystkich operatorów w danym systemie LEMF, jak i nie mogą być takie same dla uprawnionych podmiotów w danym systemie ADMF/DF.

3. Warstwa transportowa

3.1 Circuit Switched (CS)

Interfejs będzie konstruowany w sposób umożliwiający w przyszłości wysyłanie 2 strumieni PCM (stereo) w przypadku voice. Interfejs umożliwia wysyłanie 2 strumieni PCM w przypadku transmisji data i fax.

3.2 Offline

Pliki przesyłane protokołem FTP (podobnie jak w przypadku HI2). Połączenie jest nawiązywane tylko w kierunku DF ► LEMF. Stosowany również dla sesji dla których zażądano trybu online. Pliki audio powinny być kodowane w formacie wave: PCM, 8 kHz, 16 bitów, mono. Nazwa pliku po przesłaniu składa się z LIID i CIN (LIID_CIN.ext),
Wysyłanie 2 strumieni audio w offline CS będzie rozróżniane po rozszerzeniu zgodnie z metodą A (2 – CC(MO), 4 – CC(MT), 6 - CC (MO+MT)).

3.3 Online

Tryb wykorzystywany na żądanie. Protokóły SIP (RFC 3261), SDP, RTP. Wykrywamy czy jest to głos. W przypadku głosu kodowanie z mniejszym wymaganiem na pasmo (G.711A (PCMA) 8kHz). Kodowanie – PCM 64kb w przypadku przesyłania danych lub faxu.

3.4 Packet Switched (PS)

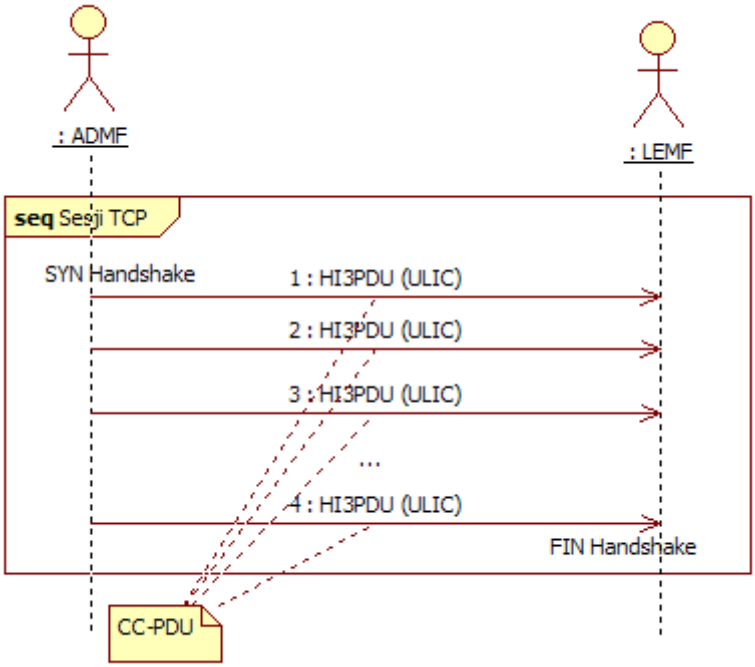
Protokół ULIC (TCP). Połączenie jest nawiązywane tylko w kierunku MF → LEMF.

3.5 IPAccess (WLAN, xDSL)

Protokół TCP zgodnie z ETSI TS 102 232-1.
Połączenie jest nawiązywane tylko w kierunku MF → LEMF

Warstwa aplikacyjna

Opis



Rysunek 1: Schemat Operacji - Packet Switched (PS)

W celu uzyskania jak największej wydajności, LEMF nie potwierdza odebrania PDU w warstwie aplikacyjnej.

II. Szczegółowa specyfikacja HI3 (PS only)

```
Umts-HI3-PS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulintercept(2) threeGPP(4) hi3(2) r6(6) version-3(3)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Object Identifier Definitions
-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4)
etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3DomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi3(2) r6(6) version-3(3)}
```

```
CC-PDU ::= SEQUENCE
{
  uLIC-header [1] ULIC-header,
  payload [2] OCTET STRING
}

ULIC-header ::= SEQUENCE
{
  hi3DomainId [0] OBJECT IDENTIFIER, -- 3GPP HI3 Domain

  version [1] Version,

  lIID [2] LawfulInterceptionIdentifier OPTIONAL,

  correlation-Number [3] GPRSCorrelationNumber,

  timeStamp [4] TimeStamp OPTIONAL,

  sequence-number [5] INTEGER (0..65535),

  t-PDU-direction [6] TPDU-direction,
  ...,
  national-HI3-ASN1parameters [7] National-HI3-ASN1parameters OPTIONAL,
  -- encoded per national requirements

  ice-type [8] ICE-type OPTIONAL
  -- The ICE-type indicates the applicable Intercepting Control Element(see ref [19]) in
which
  -- the T-PDU is intercepted.
}

Version ::= ENUMERATED
{
  version1(1),
  ...,
  version3(3)
}

TPDU-direction ::= ENUMERATED
{
  from-target (1),
  to-target (2),
  unknown (3)
}
```

```
National-HI3-ASN1parameters ::= SEQUENCE
{
  countryCode [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [39],
  -- the country to which the parameters inserted after the extension marker apply
  ...
  -- In case a given country wants to use additional national parameters according to its
law,
  -- these national parameters should be defined using the ASN.1 syntax and added after
the
  -- extension marker (...).
  -- It is recommended that "version parameter" and "vendor identification parameter" are
  -- included in the national parameters definition. Vendor identifications can be
  -- retrieved from IANA web site.
}

ICE-type ::= ENUMERATED
{
  sgsn (1),
  ggsn (2),
  ...
}

LocalTimeStamp ::= SEQUENCE
{
  generalizedTime [0] GeneralizedTime,
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.

  winterSummerIndication [1] ENUMERATED
  {
    notProvided(0),
    winterTime(1),
    summerTime(2),
    ...
  }
}

TimeStamp ::= CHOICE
{
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.
  localTime [0] LocalTimeStamp,
```

```
  utcTime [1] UTCTime
}

LawfulInterceptionIdentifier ::= OCTET STRING (SIZE (1..25))
-- It is recommended to use ASCII characters in "a"…"z", "A"…"Z", "-", "_", ".", and
"0"…"9".
-- For subaddress option only "0"..."9" shall be used.

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))

END -- OF Umts-HI3-PS
```

IPAccess – WLAN, xDSL (HI2, HI3)

```
PS-PDU ::= SEQUENCE
{
pSHeader [1] PSHeader,
payload [2] Payload
}
```

```
PSHeader ::= SEQUENCE
{
li-psDomainId [0] OBJECT IDENTIFIER,
lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
authorizationCountryCode [2] PrintableString (SIZE (2)) OPTIONAL,
-- see clause 5.2.3
communicationIdentifier [3] CommunicationIdentifier,
sequenceNumber [4] INTEGER (0..4294967295),
timeStamp [5] GeneralizedTime OPTIONAL,
-- see clause 5.2.6
...,
interceptionPointID [6] PrintableString (SIZE (1..8)) OPTIONAL,
-- see clause 5.2.11
```

```
Payload ::= CHOICE
{
iRIPayloadSequence [0] SEQUENCE OF IRIPayload,
cCPayloadSequence [1] SEQUENCE OF CCPayload,
...
}
```

```
CommunicationIdentifier ::= SEQUENCE
{
networkIdentifier [0] NetworkIdentifier,
communicationIdentityNumber [1] INTEGER (0..4294967295) OPTIONAL,
-- in case of transport of HI1 messages not required
-- Mandatory for CC and IRI, with certain exceptions (see 5.2.4)
deliveryCountryCode [2] PrintableString (SIZE (2)) OPTIONAL,
-- see clause 5.2.4
...
}
```

```
NetworkIdentifier ::= SEQUENCE
{
operatorIdentifier [0] OCTET STRING (SIZE(1..16)),
networkElementIdentifier [1] OCTET STRING (SIZE(1..16)) OPTIONAL,
...,
```

```
eTSI671NEID [2] Network-Element-Identifier OPTIONAL
-- For Network Element Identifier, use either OCTET STRING or ETSI671 definition
}
```

```
IRIPayload ::= SEQUENCE
{
iRIType [0] IRIType OPTIONAL,
-- See clause 5.2.10
timeStamp [1] GeneralizedTime OPTIONAL,
-- For aggregated payloads (see clause 6.2.3)
iRIContents [2] IRIContents,
...
}
```

```
IRIType ::= ENUMERATED
{
iRI-Begin(1),
iRI-End(2),
iRI-Continue(3),
iRI-Report(4)
}
```

```
IRIContents ::= CHOICE
-- Any of these choices may be commented out if they are not being used (see clause A.3)
{
undefinedIRI [0] OCTET STRING,
emailIRI [1] EmailIRI,
iPIRI [2] IPIRI,
iPIRIOnly [3] IPIRIOnly, --NOT USED
uMTSIRI [4] UMTSIRI,
eTSI671IRI [5] ETSI671IRI,
...,
l2IRI [6] L2IRI,
l2IRIOnly [7] L2IRIOnly,
tARGETACTIVITYMONITOR-1 [8] TS101909201.TARGETACTIVITYMONITOR-1,
tARGETACTIVITYMONITOR-2 [9] TS101909202.TARGETACTIVITYMONITOR,
pstnIsdnIRI [10] PstnIsdnIRI,
iPMMIRI [11] IPMMIRI
}
```

```
UMTSIRI ::= CHOICE
-- not used
{
iRI-Parameters [0] UmtsHI2Operations.IRI-Parameters,
umtsIRIsContent [1] UmtsIRIsContent,
...
}
```

```
ETSI671IRI ::= CHOICE
-- not used
{
iRI-Parameters [0] HI2Operations.IRI-Parameters,
iRIsContent [1] IRIsContent,
...
}
```

```
IPIRI ::= SEQUENCE
{
iPIRIObjId [0] RELATIVE-OID,
iPIRIContents [1] IPIRIContents,
...
```

```
}
```

```
IPIRIContents ::= SEQUENCE
{
accessEventType [0] AccessEventType,
targetUsername [1] OCTET STRING,
-- in ASCII-characters
internetAccessType [2] InternetAccessType,
iPVersion [3] IPVersion,
targetIPAddress [4] IPAddress OPTIONAL,
-- IP address may not be available in case of failed logon attempts.
-- If it is available, it must be sent.
targetNetworkID [5] UTF8String (SIZE (1..20)) OPTIONAL,
-- Target network ID (e.g. MAC address, PSTN number)
targetCPEID [6] UTF8String (SIZE (1..128)) OPTIONAL,
-- CPEID (e.g. Relay Agent info, computer name)
targetLocation [7] UTF8String (SIZE (1..64)) OPTIONAL,
-- When internetAccessType is Wireless LAN, this field should contain a string which
-- uniquely identifies the wireless accesspoint within the SvP domain
pOPPortNumber [8] INTEGER (0..4294967295) OPTIONAL,
-- The POP port number used by the target.
callBackNumber [9] UTF8String (SIZE (1..20)) OPTIONAL,
-- The number used to call-back the target
startTime [10] GeneralizedTime OPTIONAL,
-- The start date-time of the session or lease
endTime [11] GeneralizedTime OPTIONAL,
-- The actual end date-time of the session or lease
endReason [12] EndReason OPTIONAL,
-- The reason for the session to end
octetsReceived [13] INTEGER (0..18446744073709551615) OPTIONAL,
-- The number of octets the target received
octetsTransmitted [14] INTEGER (0..18446744073709551615) OPTIONAL,
-- The number of octets the target transmitted
rawAAAData [15] OCTET STRING OPTIONAL,
-- Content of the raw AAA record
...,
expectedEndTime [16] GeneralizedTime OPTIONAL,
-- The expected end date-time of the session or lease
pOPPhoneNumber [17] UTF8String (SIZE (1..20)) OPTIONAL,
-- The phone number dialed by the target for dial-up
pOPIdentifier [18] IPIRIIDType OPTIONAL,
-- The identifier or name of the POP
pOPIPAddress [19] IPAddress OPTIONAL
-- The IP address of the POP
partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity OPTIONAL,
-- The same as in HI2 for CS and PS
}
```

```
AccessEventType ::= ENUMERATED
{
accessAttempt(0),
-- A target requests access to the IAS
accessAccept(1),
-- IAS access is granted to the target, the session begins
accessReject(2),
-- IAS access is refused to the target
accessFailed(3),
-- The Access_attempt timed-out or failed otherwise
sessionStart(4),
-- A target starts using the IAS; not in use anymore from version 4(4).
sessionEnd(5),
-- A target stops using the IAS; not in use anymore from version 4(4).
interimUpdate(6),
-- Intermediate status report on service status or usage
...,
startOfInterceptionWithSessionActive(7),
-- LI is started on a target who already has an active session
```

```
accessEnd(8)
-- A target stops using the IAS, the session ends.
}
```

```
InternetAccessType ::= ENUMERATED
{
undefined(0),
dialUp(1),
-- IAS via DialUp access
xDSL(2),
-- IAS via DSL access
cableModem(3),
-- IAS via Cable access
lAN(4),
-- IAS via LAN access
...,
wirelessLAN(5)
-- IAS via Wireless LAN access
}
```

```
IPVersion ::= ENUMERATED
{
iPV4(1),
-- The IPv4 protocol is used
iPV6(2)
-- The IPv6 protocol is used
}
```

```
EndReason ::= ENUMERATED
{
undefined(0),
regularLogoff(1),
-- The target logged off
connectionLoss(2),
-- The connection was lost
connectionTimeout(3),
-- The connection timed-out
leaseExpired(4),
-- The DHCP lease expired
...
}
```

```
IPIRIIDType ::= CHOICE
{
printableIDType [0] UTF8String (SIZE (1..128)),
-- For printable userIDs, such as the Radius username, phonenumbers
macAddressType [1] OCTET STRING (SIZE (6)),
-- For MAC address types, raw binary format as in RFC 2132 [15]
ipAddressType [2] IPAddress,
-- For IP address types
...
}
```

```
IPIROnly ::= SEQUENCE
{
iPIROnlyObjId [0] RELATIVE-OID,
iPInformation [1] IPInformation,
protocolInformation [2] ProtocolInformation,
iPAggregatedNbrOfPackets [3] INTEGER OPTIONAL,
iPAggregatedNbrOfBytes [4] INTEGER OPTIONAL,
...
partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity OPTIONAL,
-- The same as in HI2 for CS and PS
}
```

```
IPInformation ::= CHOICE
{
iPv4Information [0] IPv4Information,
iPv6Information [1] IPv6Information
}
```

```
ProtocolInformation ::= CHOICE
{
none [0] NULL,
-- No layer 4 protocol information is provided
tCPInformation [1] TCPInformation,
uDPInformation [2] UDPInformation,
...
}
```

```
IPv4Information ::= SEQUENCE
{
headerLength [0] OCTET STRING OPTIONAL,
typeOfService [1] OCTET STRING OPTIONAL,
totalLength [2] OCTET STRING (SIZE (2))OPTIONAL,
identification [3] OCTET STRING (SIZE (2))OPTIONAL,
fragment [4] OCTET STRING (SIZE (2))OPTIONAL,
ttl [5] OCTET STRING OPTIONAL,
protocol [6] OCTET STRING OPTIONAL,
headerChecksum [7] OCTET STRING (SIZE (2))OPTIONAL,
source [8] OCTET STRING (SIZE (4)),
destination [9] OCTET STRING (SIZE (4)),
options [10] OCTET STRING (SIZE (0..40))OPTIONAL
}
```

```
IPv6Information ::= SEQUENCE
{
trafficClass [0] OCTET STRING OPTIONAL,
flowLabel [1] OCTET STRING (SIZE (20))OPTIONAL,
payloadLength [2] OCTET STRING (SIZE (4))OPTIONAL,
nextHeader [3] OCTET STRING OPTIONAL,
hopLimit [4] OCTET STRING OPTIONAL,
source [5] OCTET STRING (SIZE (16)),
destination [6] OCTET STRING (SIZE (16))
}
```

```
TCPInformation ::= SEQUENCE
{
sourcePort [0] OCTET STRING (SIZE (2))OPTIONAL,
destinationPort [1] OCTET STRING (SIZE (2))OPTIONAL,
sequenceNumber [2] OCTET STRING (SIZE (4))OPTIONAL,
ackNumber [3] OCTET STRING (SIZE (4))OPTIONAL,
dataOffset [4] BIT STRING (SIZE (4))OPTIONAL,
-- First 4 bits
controlBits [5] BIT STRING (SIZE (6))OPTIONAL,
-- Last 6 bits
windowSize [6] OCTET STRING (SIZE (2))OPTIONAL,
checkSum [7] OCTET STRING (SIZE (2))OPTIONAL,
urgentPointer [8] OCTET STRING (SIZE (2))OPTIONAL,
options [9] OCTET STRING (SIZE (0..40))OPTIONAL
}
```

```
UDPInformation ::= SEQUENCE
{
sourcePort [0] OCTET STRING (SIZE (2))OPTIONAL,
destinationPort [1] OCTET STRING (SIZE (2))OPTIONAL,
length [2] OCTET STRING (SIZE (2))OPTIONAL,
checkSum [3] OCTET STRING (SIZE (2))OPTIONAL
}
```

```
CCPayload ::= SEQUENCE
{
payloadDirection [0] PayloadDirection OPTIONAL,
timeStamp [1] GeneralizedTime OPTIONAL,
-- For aggregated payloads (see clause 6.2.3)
cCContents [2] CCContents,
...,
microSecondTimeStamp [3] MicroSecondTimeStamp OPTIONAL
-- For aggregated payloads (see clause 6.2.3)
}
```

```
PayloadDirection ::= ENUMERATED
{
fromTarget(0),
toTarget(1),
...,
indeterminate(2),
-- Indication whether intercepted CC was travelling to or from the target
-- or that the direction was indeterminate
combined(3),
-- Indication applicable to some services that the traffic is actually a combination
-- of To and From
notapplicable(4)
-- Indication that direction of interceptable service does not make sense
}
```

```
CCContents ::= CHOICE
-- Any of these choices may be commented out if they are not being used, see clause A.3
{
undefinedCC [0] OCTET STRING,
emailCC [1] EmailCC,
iPCC [2] IPCC,
uMTSCC [4] OCTET STRING,
eTSI671CC [5] OCTET STRING,
...,
l2CC [6] L2CC,
tTRAFFIC-1 [7] TS101909201.TTRAFFIC,
cTTRAFFIC-1 [8] TS101909201.CTTRAFFIC,
tTRAFFIC-2 [9] TS101909202.TTRAFFIC,
cTTRAFFIC-2 [10] TS101909202.CTTRAFFIC,
pstnIsdnCC [11] PstnIsdnCC,
iPMMCC [12] IPMMCC
}
```

```
MicroSecondTimeStamp ::= SEQUENCE
{
seconds [0] INTEGER (0..18446744073709551615),
-- number of seconds since 1970-1-1 00:00Z also known as unix time epoch
microSeconds [1] INTEGER (0..999999),
...
}
```

```
IPCC ::= SEQUENCE
{
iPCCObjId [0] RELATIVE-OID,
iPCCContents [1] IPCCContents
}
```

```
IPCCContents ::= CHOICE
{
iPPackets [0] OCTET STRING,
...
}
```

IV. HI3 (PS only)

```
Umts-HI3-PS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulintercept(2) threeGPP(4) hi3(2) r6(6) version-3(3)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Object Identifier Definitions
-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4)
etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3DomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi3(2) r6(6) version-3(3)}

CC-PDU ::= SEQUENCE
{
  uLIC-header [1] ULIC-header,
  payload [2] OCTET STRING
}

ULIC-header ::= SEQUENCE
{
  hi3DomainId [0] OBJECT IDENTIFIER, -- 3GPP HI3 Domain

  version [1] Version,

  lIID [2] LawfulInterceptionIdentifier OPTIONAL,

  correlation-Number [3] GPRSCorrelationNumber,

  timeStamp [4] TimeStamp OPTIONAL,

  sequence-number [5] INTEGER (0..65535),

  t-PDU-direction [6] TPDU-direction,
  ...,
  national-HI3-ASN1parameters [7] National-HI3-ASN1parameters OPTIONAL,
  -- encoded per national requirements

  ice-type [8] ICE-type OPTIONAL
```

```
  -- The ICE-type indicates the applicable Intercepting Control Element(see ref [19]) in
which
  -- the T-PDU is intercepted.
}

Version ::= ENUMERATED
{
  version1(1),
  ...,
  version3(3)
}

TPDU-direction ::= ENUMERATED
{
  from-target (1),
  to-target (2),
  unknown (3)
}

National-HI3-ASN1parameters ::= SEQUENCE
{
  countryCode [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [39],
  -- the country to which the parameters inserted after the extension marker apply
  ...
  -- In case a given country wants to use additional national parameters according to its
law,
  -- these national parameters should be defined using the ASN.1 syntax and added after
the
  -- extension marker (...).
  -- It is recommended that "version parameter" and "vendor identification parameter" are
  -- included in the national parameters definition. Vendor identifications can be
  -- retrieved from IANA web site.
}

ICE-type ::= ENUMERATED
{
  sgsn (1),
  ggsn (2),
  ...
}

LocalTimeStamp ::= SEQUENCE
{
  generalizedTime [0] GeneralizedTime,
  -- The minimum resolution required is one second.
```

```
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.

  winterSummerIndication [1] ENUMERATED
  {
    notProvided(0),
    winterTime(1),
    summerTime(2),
    ...
  }
}

TimeStamp ::= CHOICE
{
  -- The minimum resolution required is one second.
  -- "Resolution" is the smallest incremental change that can be measured for time and
  -- is expressed with a definite number of decimal digits or bits.
  localTime [0] LocalTimeStamp,

  utcTime [1] UTCTime
}

LawfulInterceptionIdentifier ::= OCTET STRING (SIZE (1..25))
-- It is recommended to use ASCII characters in "a"…"z", "A"…"Z", "-", "_", ".", and
"0"…"9".
-- For subaddress option only "0"..."9" shall be used.

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))

END -- OF Umts-HI3-PS
```

Załącznik nr 4

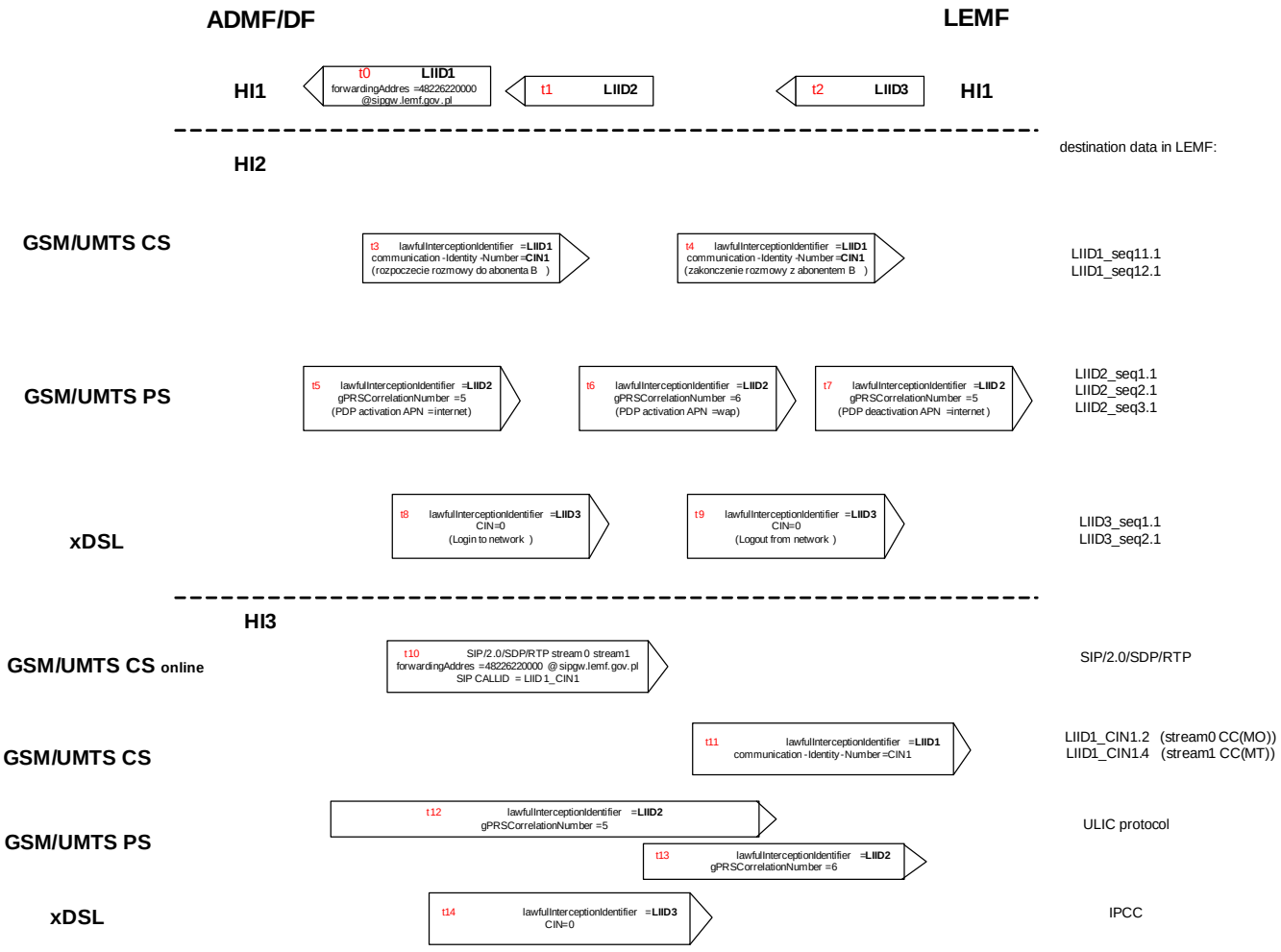
Specyfikacja techniczna styku HI-2 i 3 interfejsu HI w zakresie IPAccess

(WLAN,WiFi, xDSL)

Aktywność abonenta powodująca przesył danych pakietowych w sieci operatora powoduje, że system ADMF/DF wysyła informacje skojarzone interfejsem HI2 oraz treść przekazu interfejsem HI3.
Za korelacje informacji skojarzonych przekazu (HI2) z jego treścią (HI3) odpowiada pole Communication Identity Number (CIN) umieszczone w strukturze ASN.1 interfejsu HI2 oraz HI3. CIN unikalny jest w ramach jednej sesji użytkownika.

Przyklad

abonent Jan Kowalski o numerze PESEL xxx przypisane ma trzy LIID w systemach LI:
LIID1 – abonent Jan Kowalski o numerze 48501000000, usługa monitorowana GSM/UMTS CS
LIID2 – abonent Jan Kowalski o numerze 48501000000, usługa monitorowana GSM/UMTS PS
LIID3 – abonent Jan Kowalski o login-ie SDFG56DDSX, usługa monitorowana xDSL



Rysunek 1: Przepływ wiadomości w interfejsach HI.

Przykładowy przepływ wiadomości w interfejsach HI, gdzie abonentowi założono monitorowanie trzech usług: CS z opcja online, PS oraz xDSL.

t0 – założenie dedykacji abonentowi X dla usługi GSM/UMTS CS z opcja online
t1 – założenie dedykacji abonentowi X dla usługi GSM/UMTS PS
t2 - założenie dedykacji abonentowi X dla usługi xDSL

Po założeniu i zaktywowaniu dedykacji w CN sieci operatora, dedykacje są aktywne i w zależności od aktywności abonenta pojawiają się informacje skojarzone oraz sama treść przekazu.

t3 – rozpoczęcie rozmowy
t4 – zakończenie rozmowy
t5 – aktywowanie PDP kontekst do punktu dostępowego „Internet”
t6 – aktywowanie drugiego PDP kontekst do punktu dostępowego „Wap”
t7 – dezaktywacja PDP kontekstu do punktu dostępowego „Internet”
t8 – zalogowanie się do sieci dostęp xDSL
t9 – wylogowanie się z sieci dostęp xDSL

Treść przekazu zostaje przesłana zgodnie z informacjami skojarzonymi, z którymi są powiązane.

t10 – zestawienie połączenia SIP do uprawnionego podmiotu z treścią rozmowy w trybie online
t11 – dodatkowo treść rozmowy przesłania w trybie offline (stereo)
t12 – treść przekazu (dane IP) generowane do punktu dostępowego „Internet”
t13 - treść przekazu (dane IP) generowane do punktu dostępowego „Wap”
t14 – treść przekazu (dane IP) przez xDSL

Informacje skojarzone zostały dostarczone FTP w postaci plików o określonych nazwach kojarzonych z zawartością do systemu LEMF. Treści przekazu zostały dostarczone wykorzystując różne techniki przesyłu informacji w zależności rodzaju danych.

```
PS-PDU ::= SEQUENCE
{
pSHeader [1] PSHeader,
payload [2] Payload
}
```

```
PSHeader ::= SEQUENCE
{
li-psDomainId [0] OBJECT IDENTIFIER,
lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
authorizationCountryCode [2] PrintableString (SIZE (2)) OPTIONAL,
-- see clause 5.2.3
communicationIdentifier [3] CommunicationIdentifier,
sequenceNumber [4] INTEGER (0..4294967295),
timeStamp [5] GeneralizedTime OPTIONAL,
-- see clause 5.2.6
...,
interceptionPointID [6] PrintableString (SIZE (1..8)) OPTIONAL,
-- see clause 5.2.11
```

```
Payload ::= CHOICE
{
iRIPayloadSequence [0] SEQUENCE OF IRIPayload,
cCPayloadSequence [1] SEQUENCE OF CCPayload,
...
}
```

```
CommunicationIdentifier ::= SEQUENCE
{
networkIdentifier [0] NetworkIdentifier,
communicationIdentityNumber [1] INTEGER (0..4294967295) OPTIONAL,
-- in case of transport of HI1 messages not required
-- Mandatory for CC and IRI, with certain exceptions (see 5.2.4)
deliveryCountryCode [2] PrintableString (SIZE (2)) OPTIONAL,
-- see clause 5.2.4
...
}
```

```
NetworkIdentifier ::= SEQUENCE
{
operatorIdentifier [0] OCTET STRING (SIZE(1..16)),
networkElementIdentifier [1] OCTET STRING (SIZE(1..16)) OPTIONAL,
...,
eTSI671NEID [2] Network-Element-Identifier OPTIONAL
-- For Network Element Identifier, use either OCTET STRING or ETSI671 definition
}
```

```
IRIPayload ::= SEQUENCE
{
iRIType [0] IRIType OPTIONAL,
-- See clause 5.2.10
timeStamp [1] GeneralizedTime OPTIONAL,
-- For aggregated payloads (see clause 6.2.3)
iRIContents [2] IRIContents,
...
}
```

```
IRIType ::= ENUMERATED
{
iRI-Begin(1),
iRI-End(2),
iRI-Continue(3),
iRI-Report(4)
}
```

```
IRIContents ::= CHOICE
-- Any of these choices may be commented out if they are not being used (see clause A.3)
{
undefinedIRI [0] OCTET STRING,
emailIRI [1] EmailIRI,
iPIRI [2] IPIRI,
iPIRIOnly [3] IPIRIOnly, --NOT USED
uMTSIRI [4] UMTSIRI,
eTSI671IRI [5] ETSI671IRI,
...,
l2IRI [6] L2IRI,
l2IRIOnly [7] L2IRIOnly,
tARGETACTIVITYMONITOR-1 [8] TS101909201.TARGETACTIVITYMONITOR-1,
tARGETACTIVITYMONITOR-2 [9] TS101909202.TARGETACTIVITYMONITOR,
pstnIsdnIRI [10] PstnIsdnIRI,
```

```
iPMMIRI [11] IPMMIRI
}
```

```
UMTSIRI ::= CHOICE
-- not used
{
iRI-Parameters [0] UmtsHI2Operations.IRI-Parameters,
umtsIRIsContent [1] UmtsIRIsContent,
...
}
```

```
ETSI671IRI ::= CHOICE
-- not used
{
iRI-Parameters [0] HI2Operations.IRI-Parameters,
iRIsContent [1] IRIsContent,
...
}
```

```
IPIRI ::= SEQUENCE
{
iPIRIObjId [0] RELATIVE-OID,
iPIRIContents [1] IPIRIContents,
...
}
```

```
IPIRIContents ::= SEQUENCE
{
accessEventType [0] AccessEventType,
targetUsername [1] OCTET STRING,
-- in ASCII-characters
internetAccessType [2] InternetAccessType,
iPVersion [3] IPVersion,
targetIPAddress [4] IPAddress OPTIONAL,
-- IP address may not be available in case of failed logon attempts.
-- If it is available, it must be sent.
targetNetworkID [5] UTF8String (SIZE (1..20)) OPTIONAL,
-- Target network ID (e.g. MAC address, PSTN number)
targetCPEID [6] UTF8String (SIZE (1..128)) OPTIONAL,
-- CPEID (e.g. Relay Agent info, computer name)
targetLocation [7] UTF8String (SIZE (1..64)) OPTIONAL,
-- When internetAccessType is Wireless LAN, this field should contain a string which
-- uniquely identifies the wireless accesspoint within the SvP domain
pOPPortNumber [8] INTEGER (0..4294967295) OPTIONAL,
-- The POP port number used by the target.
callBackNumber [9] UTF8String (SIZE (1..20)) OPTIONAL,
-- The number used to call-back the target
startTime [10] GeneralizedTime OPTIONAL,
-- The start date-time of the session or lease
endTime [11] GeneralizedTime OPTIONAL,
-- The actual end date-time of the session or lease
endReason [12] EndReason OPTIONAL,
-- The reason for the session to end
octetsReceived [13] INTEGER (0..18446744073709551615) OPTIONAL,
-- The number of octets the target received
octetsTransmitted [14] INTEGER (0..18446744073709551615) OPTIONAL,
-- The number of octets the target transmitted
rawAAAData [15] OCTET STRING OPTIONAL,
-- Content of the raw AAA record
...,
expectedEndTime [16] GeneralizedTime OPTIONAL,
-- The expected end date-time of the session or lease
pOPPhoneNumber [17] UTF8String (SIZE (1..20)) OPTIONAL,
-- The phone number dialed by the target for dial-up
pOPIdentifier [18] IPIRIIDType OPTIONAL,
-- The identifier or name of the POP
```

```
pOPIPAddress [19] IPAddress OPTIONAL
-- The IP address of the POP
partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity OPTIONAL,
-- The same as in HI2 for CS and PS
}
```

```
AccessEventType ::= ENUMERATED
{
accessAttempt(0),
-- A target requests access to the IAS
accessAccept(1),
-- IAS access is granted to the target, the session begins
accessReject(2),
-- IAS access is refused to the target
accessFailed(3),
-- The Access_attempt timed-out or failed otherwise
sessionStart(4),
-- A target starts using the IAS; not in use anymore from version 4(4).
sessionEnd(5),
-- A target stops using the IAS; not in use anymore from version 4(4).
interimUpdate(6),
-- Intermediate status report on service status or usage
...,
startOfInterceptionWithSessionActive(7),
-- LI is started on a target who already has an active session
accessEnd(8)
-- A target stops using the IAS, the session ends.
}
```

```
InternetAccessType ::= ENUMERATED
{
undefined(0),
dialUp(1),
-- IAS via DialUp access
xDSL(2),
-- IAS via DSL access
cableModem(3),
-- IAS via Cable access
lAN(4),
-- IAS via LAN access
...,
wirelessLAN(5)
-- IAS via Wireless LAN access
}
```

```
IPVersion ::= ENUMERATED
{
iPV4(1),
-- The IPv4 protocol is used
iPV6(2)
-- The IPv6 protocol is used
}
```

```
EndReason ::= ENUMERATED
{
undefined(0),
regularLogoff(1),
-- The target logged off
connectionLoss(2),
-- The connection was lost
connectionTimeout(3),
-- The connection timed-out
leaseExpired(4),
-- The DHCP lease expired
...
}
```

```
IPIRIIDType ::= CHOICE
{
printableIDType [0] UTF8String (SIZE (1..128)),
-- For printable userIDs, such as the Radius username, phonenumbers
macAddressType [1] OCTET STRING (SIZE (6)),
-- For MAC address types, raw binary format as in RFC 2132 [15]
ipAddressType [2] IPAddress,
-- For IP address types
...
}
```

```
IPIROnly ::= SEQUENCE
{
iPIROnlyObjId [0] RELATIVE-OID,
iPInformation [1] IPInformation,
protocolInformation [2] ProtocolInformation,
iPAggregatedNbrOfPackets [3] INTEGER OPTIONAL,
iPAggregatedNbrOfBytes [4] INTEGER OPTIONAL,
...
partyExtendedIdentity [PRIVATE 1] PartyExtendedIdentity OPTIONAL,
-- The same as in HI2 for CS and PS
}
```

```
IPInformation ::= CHOICE
{
iPv4Information [0] IPv4Information,
iPv6Information [1] IPv6Information
}
```

```
ProtocolInformation ::= CHOICE
{
none [0] NULL,
-- No layer 4 protocol information is provided
tCPInformation [1] TCPInformation,
uDPInformation [2] UDPInformation,
...
}
```

```
IPv4Information ::= SEQUENCE
{
headerLength [0] OCTET STRING OPTIONAL,
typeOfService [1] OCTET STRING OPTIONAL,
totalLength [2] OCTET STRING (SIZE (2))OPTIONAL,
identification [3] OCTET STRING (SIZE (2))OPTIONAL,
fragment [4] OCTET STRING (SIZE (2))OPTIONAL,
ttl [5] OCTET STRING OPTIONAL,
protocol [6] OCTET STRING OPTIONAL,
headerChecksum [7] OCTET STRING (SIZE (2))OPTIONAL,
source [8] OCTET STRING (SIZE (4)),
destination [9] OCTET STRING (SIZE (4)),
options [10] OCTET STRING (SIZE (0..40))OPTIONAL
}
```

```
IPv6Information ::= SEQUENCE
{
trafficClass [0] OCTET STRING OPTIONAL,
flowLabel [1] OCTET STRING (SIZE (20))OPTIONAL,
payloadLength [2] OCTET STRING (SIZE (4))OPTIONAL,
nextHeader [3] OCTET STRING OPTIONAL,
hopLimit [4] OCTET STRING OPTIONAL,
source [5] OCTET STRING (SIZE (16)),
destination [6] OCTET STRING (SIZE (16))
}
```

```
TCPInformation ::= SEQUENCE
{
sourcePort [0] OCTET STRING (SIZE (2))OPTIONAL,
destinationPort [1] OCTET STRING (SIZE (2))OPTIONAL,
sequenceNumber [2] OCTET STRING (SIZE (4))OPTIONAL,
ackNumber [3] OCTET STRING (SIZE (4))OPTIONAL,
dataOffset [4] BIT STRING (SIZE (4))OPTIONAL,
-- First 4 bits
controlBits [5] BIT STRING (SIZE (6))OPTIONAL,
-- Last 6 bits
windowSize [6] OCTET STRING (SIZE (2))OPTIONAL,
checkSum [7] OCTET STRING (SIZE (2))OPTIONAL,
urgentPointer [8] OCTET STRING (SIZE (2))OPTIONAL,
options [9] OCTET STRING (SIZE (0..40))OPTIONAL
}
```

```
UDPInformation ::= SEQUENCE
{
sourcePort [0] OCTET STRING (SIZE (2))OPTIONAL,
destinationPort [1] OCTET STRING (SIZE (2))OPTIONAL,
length [2] OCTET STRING (SIZE (2))OPTIONAL,
checkSum [3] OCTET STRING (SIZE (2))OPTIONAL
}
```

```
CCPayload ::= SEQUENCE
{
payloadDirection [0] PayloadDirection OPTIONAL,
timeStamp [1] GeneralizedTime OPTIONAL,
-- For aggregated payloads (see clause 6.2.3)
cCContents [2] CCContents,
...,
microSecondTimeStamp [3] MicroSecondTimeStamp OPTIONAL
-- For aggregated payloads (see clause 6.2.3)
}
```

```
PayloadDirection ::= ENUMERATED
{
fromTarget(0),
toTarget(1),
...,
indeterminate(2),
-- Indication whether intercepted CC was travelling to or from the target
-- or that the direction was indeterminate
combined(3),
-- Indication applicable to some services that the traffic is actually a combination
-- of To and From
notapplicable(4)
-- Indication that direction of interceptable service does not make sense
}
```

```
CCContents ::= CHOICE
-- Any of these choices may be commented out if they are not being used, see clause A.3
{
undefinedCC [0] OCTET STRING,
emailCC [1] EmailCC,
iPCC [2] IPCC,
uMTSCC [4] OCTET STRING,
eTSI671CC [5] OCTET STRING,
...,
l2CC [6] L2CC,
tTRAFFIC-1 [7] TS101909201.TTRAFFIC,
cTTRAFFIC-1 [8] TS101909201.CTTRAFFIC,
tTRAFFIC-2 [9] TS101909202.TTRAFFIC,
cTTRAFFIC-2 [10] TS101909202.CTTRAFFIC,
pstnIsdnCC [11] PstnIsdnCC,
iPMMCC [12] IPMMCC
```

```
}
```

```
MicroSecondTimeStamp ::= SEQUENCE
{
seconds [0] INTEGER (0..18446744073709551615),
-- number of seconds since 1970-1-1 00:00Z also known as unix time epoch
microSeconds [1] INTEGER (0..999999),
...
}
```

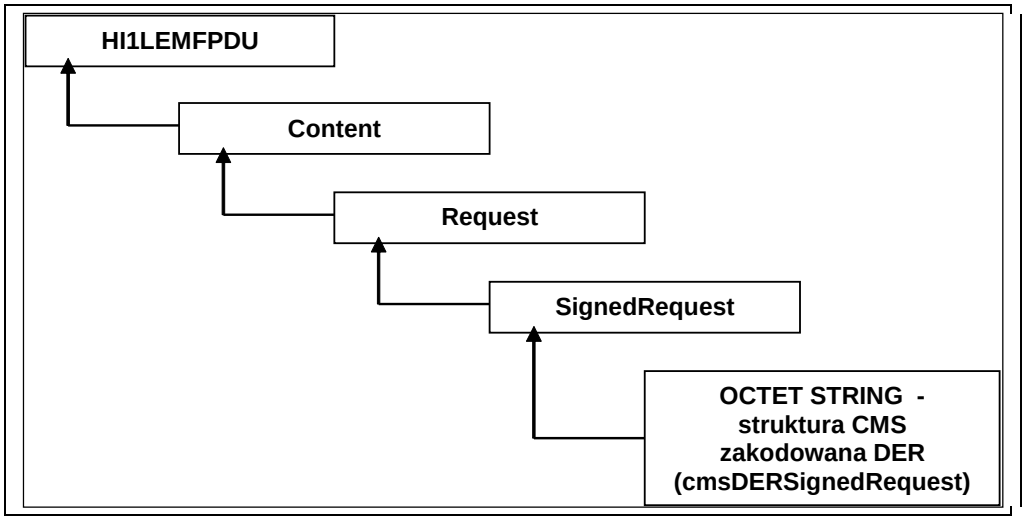
```
IPCC ::= SEQUENCE
{
iPCCObjId [0] RELATIVE-OID,
iPCCContents [1] IPCCContents
}
```

```
IPCCContents ::= CHOICE
{
iPPackets [0] OCTET STRING,
...
}
```

Załącznik nr 5

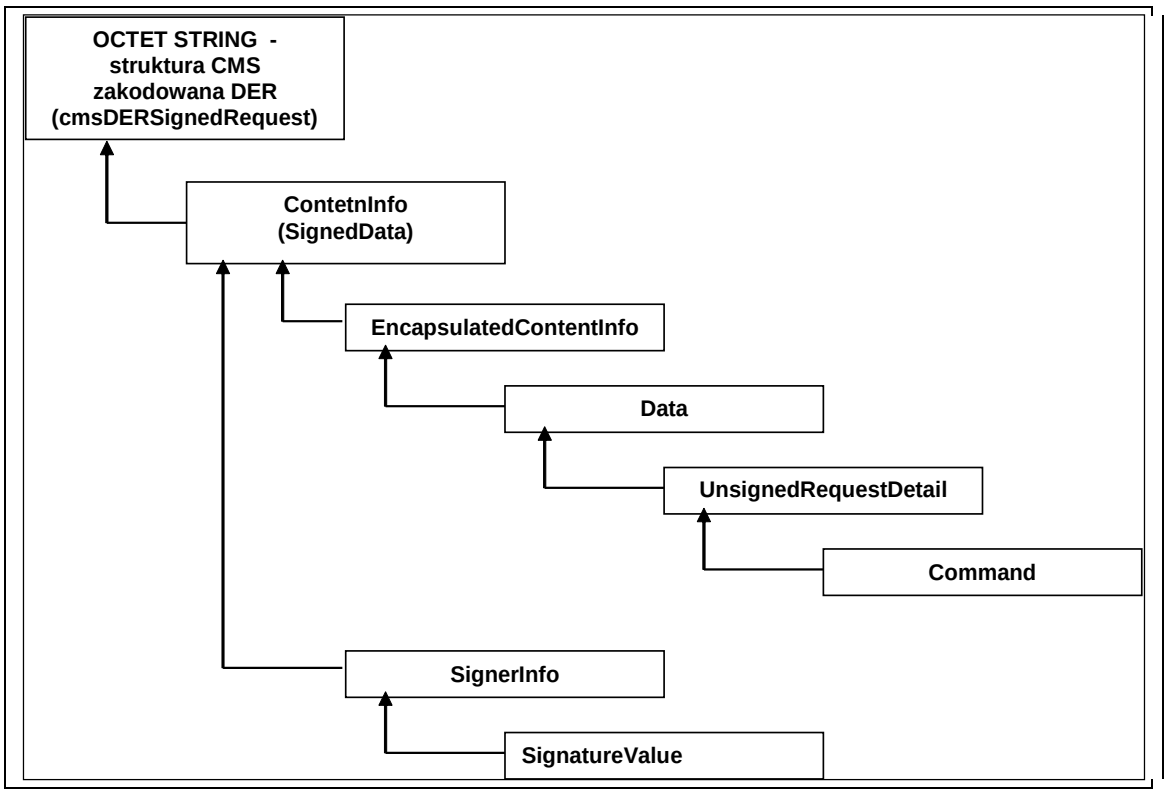
Koncepcja Podpisu Elektronicznego

Wybrane żądania HI1, po ich przygotowaniu w LEMF, są podpisywane elektronicznie przez użytkownika LEMF. Użytkownik do podpisu żądania wykorzystuje swój indywidualny klucz prywatny oraz certyfikat X.509, który przyporządkowuje dane identyfikujące użytkownika do jego klucza publicznego. Enkapsulowane żądanie HI1, wraz z podpisem elektronicznym jest przesyłane do ADMF.
By ADMF mógł sprawdzić podpis elektroniczny żądania HI1 złożony przez użytkownika LEMF konieczne jest by obie strony: LEMF i ADMF, wykorzystywały ten sam format (składnie) podpisu elektronicznego. Formatem tym jest CMS (Cryptographics Message Syntax) zdefiniowany w [RFC3852].
Podpisywanie żądania HI1 przez użytkownika LEMF jest możliwe pod warunkiem posiadania przez niego indywidualnego klucza prywatnego oraz certyfikatu X.509. Również ADMF musi posiadać pewną wiedzę o certyfikatach użytkowników LEMF, by móc sprawdzać poprawność podpisów elektronicznych. Dla tego celu wykorzystuje się infrastrukturę klucza publicznego PKI. Indywidualne certyfikaty X.509 użytkowników systemu LEMF są wystawiane przez CA (urząd ds. certyfikatów) w instytucji, która administruje i użytkuje dany system LEMF. Certyfikat tego CA jest jednocześnie dostępny w systemie ADMF administrowanego przez operatora. Zarządzanie certyfikatami X.509, listami CRL oraz infrastrukturą klucza publicznego PKI zostało opisane w osobnym punkcie.
Poniższy rysunek poglądowo przedstawia enkapsulowanie w HI1LEMFPDU struktury CMS zawierającej treść żądania HI1 oraz podpis, zakodowane z wykorzystaniem DER (cmsDERSignedRequest).



Rysunek 1: Enkapsulowanie podpisanego żądania HI1 w Hi1LEMFPDU

Poniższy rysunek poglądowo przedstawia enkapsulowanie żądania HI1 (Command) i jego podpisu (SignatureValue) w cmsDERSignedRequest:



Rysunek 2: Enkapsulowanie żądania HI1 i jego podpisu w strukturze CMS

Wykorzystywane standardy

[RFC3852] Housley, R., „Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

[RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, August 2002.

[RFC3279] Bassham, L., Polk, W., R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation Lists CRL Profile", RFC 3279, April 2002.

[RFC3280] Housley, R., Polk, T, Ford, W., Solo, D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC3281] Farrell, S., Housley, R., "An Internet Attribute Certificate Profile for Authorization", RFC3281, April 2002.

[RFC4055] Housley, R., Kaliski, B., Schaad, J., "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, June 2005.

[RFC3447] Jonsson, J., Kaliski, B., "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC3126] Pinkas D., Ross J., Pope N. "Electronic Signature Formats for long term electronic signatures", RFC 3126, September 2001

Wiadomości przesyłane w Hi1, które wymagają podpisania

Następujące żądania, przesyłane z LEMF do ADMF, mogą i muszą być podpisane elektronicznie:

- activate,
- deactivate,
- modificate.

Żądania te są polami wyboru typu Command:

```
Command ::= CHOICE
{
activate [1] Activate,
deactivate [2] Deactivate,
modificate [3] Modificate,
...
}
```

Pole command oraz pole time, które określa czas złożenia podpisu, wchodzą w skład typu UnsignedRequestDetail:

```
UnsignedRequestDetail ::= SEQUENCE
{
time [1] TimeStamp,
command [3] Command,
...
}
```

Zawartość pola typu UnsignedRequestDetail wraz z podpisem tego pola jest zapisywane w strukturze CMS.

Format podpisanego żądania Hi1

Na potrzeby podpisu elektronicznego stosuje się format Cryptographics Message Syntax (CMS) zdefiniowany w [RFC3852]. Struktura CMS jest identyfikowana przez następujący OID:

```
CryptographicMessageSyntax2004 OBJECT IDENTIFIER ::= { iso(1)
member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
smime(16) modules(0) cms-2004(24) }.
```

Struktura CMS zapisywana jest, z wykorzystaniem kodowania DER, w polu cmsDERSignedRequest typu SignedRequest:

```
SignedRequest ::= SEQUENCE
{
version                [1] SignedRequestVersion,
signStandard           [2] OBJECT IDENTIFIER,
-- CryptographicMessageSyntax2004 { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0)
cms-2004(24) }
cmsDERSignedRequest    [3] OCTET STRING
-- cmsDERSignedRequest [3] ANY DEFINED BY signStandard
}
```

```
SignedRequestVersion ::= INTEGER
{
v1 (0)
}
```

W kolejnych punktach przybliżono najważniejsze elementy struktury CMS. Pełny opis specyfikacji znajduje się w [RFC3852].

Typ ContentInfo

Podstawowym typem dla CMS jest ContentInfo. Typ ten jest identyfikowany przez następujący OID:

```
id-ct-contentInfo OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16)
ct(1) 6 }
```

Typ ContentInfo został zdefiniowany następująco:

```
ContentInfo ::= SEQUENCE
{
contentType ContentType,
content [0] EXPLICIT ANY DEFINED BY contentType
}

ContentType ::= OBJECT IDENTIFIER
```

Pole contentType musi identyfikować typ SignedData, określony przez następujący identyfikator OID:

```
id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }
```

Typ ContentInfo zostało opisany w [RFC3852], pkt 3.

Typ SignedData

Typ SignedData struktury CMS składa się z zawartości dowolnego typu oraz podpisów elektronicznych tej zawartości. Typ SignedData został zdefiniowany następująco:

```
SignedData ::= SEQUENCE
{
version CMSVersion,
digestAlgorithms DigestAlgorithmIdentifiers,
encapContentInfo EncapsulatedContentInfo,
certificates [0] IMPLICIT CertificateSet OPTIONAL,
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
signerInfos SignerInfos
}
```

Pole digestAlgorithms zawiera zbiór identyfikatorów algorytmów funkcji skrótu. Wymagania dotyczące tych algorytmów zostały opisana w pkt. 0
Pole encapContentInfo zawiera treść żądania Hi1, która wymaga podpisania.
Pole certificates zawiera zbiór certyfikatów niezbędnych do określenia poprawności podpisów znajdujących się w polu signersInfos.
Opcjonalne pole crls zawiera zbiór list unieważnionych i zawieszonych certyfikatów (ang.

Certificate Revocation List - CRL). Na potrzeby zarządzania certyfikatami i listami CRL wykorzystuje się infrastrukturę klucza publicznego PKI. PKI oraz formaty certyfikatów i list CRL zostały opisane w osobnym punkcie.
Pole signerInfos jest zbiorem podpisów elektronicznych.
Typ SignedData został opisany w [RFC3852], pkt 5.1.

EncapsulatedContentInfo

Typ EncapsulatedContentInfo został zdefiniowany następująco:

```
EncapsulatedContentInfo ::= SEQUENCE
{
eContentType ContentType,
eContent [0] EXPLICIT OCTET STRING OPTIONAL
}

ContentType ::= OBJECT IDENTIFIER
```

Pole eContentType musi identyfikować typ data:

```
id-data OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs7(7) 1 }
```

Pole eContent zawiera żądanie HI1 przeznaczone do podpisania w postaci UnsignedRequestDetail.
Typ EncapsulatedContentInfo został opisany w [RFC3852], pkt 5.2

Typ SignerInfo

Typ SignerInfo został zdefiniowany następująco:

```
SignerInfo ::= SEQUENCE
{
version CMSVersion,
sid SignerIdentifier,
digestAlgorithm DigestAlgorithmIdentifier,
signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
signatureAlgorithm SignatureAlgorithmIdentifier,
signature SignatureValue,
unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
}
```

Pole sid identyfikuje certyfikat podmiotu, który złożył podpis. Zgodnie z [RFC3852], pkt 5.3 muszą zostać zaimplementowane obie formy SignerIdentifier: issuerAndSerialNumber oraz subjectKeyIdentifier.
Pole digestAlgorithm zawiera identyfikator zastosowanego algorytmu funkcji skrótu. Wymagania dotyczące algorytmów funkcji skrótu zostały opisana w pkt. 0
Pole signedAttrs zawiera zbiór atrybutów, które są podpisywane. Zalecane jest, by wykorzystywany był atrybut określający czas złożenia podpisu. Ponadto w polu tym zostanie zawarta informacja o rodzaju zobowiązania (ang. *commitment type*) poprzez umieszczenie identyfikatora obiektu:
commitmentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 1 } wskazującego, że podpisujący pracownik LEA stworzył, zaaprobował i wysłał podpisaną wiadomość ([RFC3126], pkt 3.12.1).
Pole signatureAlgorithm zawiera identyfikator zastosowanego algorytmu podpisu elektronicznego. Wymagania dotyczące algorytmów podpisów elektronicznych zostały opisane w pkt 0
Pole signature typu SignatureValue zawiera wyliczoną wartość podpisu elektronicznego dla treści

żądania Hi1.
Opcjonalne pole unsignedAttrs zawiera zbiór atrybutów, które nie są podpisywane.
Typ SignerInfo został opisany w [RFC3852], pkt 5.3

Algorytmy kryptograficzne

Algorytmy funkcji skrótu

Identyfikatory stosowanych algorytmów funkcji skrótu określone są w polu digestAlgorithms typu SignedData oraz w polu digestAlgorithm typu SignerInfo. Alogorytmy funkcji skrótu, które muszą być obsługiwane przez ADMF w celu zapewnienia możliwości wyliczenia skrótu na potrzeby sprawdzenia podpisu elektronicznego zostały wyspecyfikowane w tabeli poniżej:

lp.	Algorytm	Identyfikator obiektu OID	Dokument określający OID
1.	SHA-1 (id-sha1)	{ iso(1) identified-organization(3) oiw(14) secsig(3) algorithms(2) 26 }	[RFC3370] [RFC4055]
2.	SHA-224 (id-sha224)	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 4 }	[RFC4055]
3.	SHA-256 (id-sha256)	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }	[RFC4055]
4.	SHA-384 (id-sha348)	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 }	[RFC4055]
5.	SHA-512 (id-sha512)	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }	[RFC4055]
6.	RIPEMD-160 (id-ripemd160)	{ iso(1) identifiedOrganization(3) teletrust(36) algorithm(3) hashAlgorithm(2) 1 }	http://homes.esat.kuleuven.be/~bosselae/ripemd160.html http://www.teletrust.de/index.php?id=513
7.	RIPEMD-256 (id-ripemd256)	{ iso(1) identified-organization(3) teletrust(36) algorithm(3) hashAlgorithm(2) ripemd256(3) }	http://homes.esat.kuleuven.be/~bosselae/ripemd160.html http://www.teletrust.de/index.php?id=513

ADMF może posiadać zaimplementowaną obsługę dodatkowych algorytmów funkcji skrótu.
LEMF na potrzeby podpisów elektronicznych powinien stosować algorytm funkcji skrótu SHA-512 (rozwiązanie preferowane) lub inny algorytm z rodziny SHA-2 (SHA-384, SHA-256, SHA-224) lub algorytm RIPEMD-256. Ze względu na znane słabości, algorytmu SHA-1 nie powinien być wykorzystywany przez LEMF.

Algorytmy podpisu

Identyfikator stosowanego algorytmu podpisu jest określony w polu signatureAlgorithm typu SignerInfo. Algorytmy podpisu, które muszą być obsługiwane przez ADMF w celu zapewnienia możliwości sprawdzenia podpisu zostały wyspecyfikowane w tabeli poniżej:

lp.	Algorytm	Identyfikator obiektu OID	Dokument określający OID	Długości klucza [bity]
1.	RSA (rsaEncryption)	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	[RFC3370]	1024, 2048, 4096
2.	DSA (id-dsa)	{ iso(1) member-body(2) us(840) x9-57 (10040) x9cm(4) 1 }	[RFC3370]	1024, 2048, 4096

ADMF może posiadać zaimplementowaną obsługę dodatkowych algorytmów podpisów.
LEMF na potrzeby podpisów elektronicznych powinien stosować algorytm podpisu RSA lub DSA o długości klucza przynajmniej 2048 bitów (zalecany jest algorytm RSA lub DSA o długości klucza 4096 bitów).

Składanie podpisu

Podpis składany jest indywidualnie, przez uprawnionego użytkownika systemu LEMF. Użytkownik ten wyposażony jest w indywidualną, imienną kartę inteligentną lub inny „komponent techniczny". Karta inteligentna jest nośnikiem klucza prywatnego oraz certyfikatu X.509 tego użytkownika. Generowanie podpisu dla zadanej wiadomości (żądania Hi1) odbywa się na karcie inteligentnej.
Generowanie (wyliczanie) podpisu odbywa się w sposób określony w [RFC3852].
Każde żądanie HI1 z podpisem w formacie CMS (cmsDERSignedRequest) powinno zawierać przynajmniej jeden poprawny podpis elektroniczny. Podpis ten powinien zawierać certyfikaty X.509 i może zawierać listy CRL.
LEMF musi zapewnić, że certyfikat użytkownika, który podpisuje żądanie jest ważny w chwili składania podpisu elektronicznego.

Sprawdzanie poprawności podpisu

Sprawdzenie poprawności podpisu żądania w HI1 odbywa się w ADMF i w sposób określony w [RFC3852]. W szczególności ADMF weryfikuje całą ścieżkę certyfikacji pomiędzy certyfikatem użytkownika LEMF, który złożył podpis i certyfikatem głównego urzędu ds. certyfikatów CA, który jest w LEA.
Realizowane są tylko te żądania, które zawierają przynajmniej jeden poprawny podpis elektroniczny. Sprawdzenie podpisu polega na znalezieniu pierwszego poprawnego podpisu elektronicznego w strukturze CMS. Oznacza to w szczególności, że żądanie, które zawiera jeden niepoprawny podpis elektroniczny (np certyfikat użytkownika stracił ważność) i jeden poprawny podpis elektroniczny zostanie obsłużone.
Poprawność podpisu elektronicznego sprawdzana jest przez ADMF tylko raz, po otrzymaniu podpisanego żądania Hi1.
Żądania w HI1 muszą być podpisane przez użytkownika (certyfikat wystawiony na osobę fizyczną). Żądania podpisane przez urząd ds. certyfikatów nie są realizowane.
W przypadku braku możliwości stwierdzenia poprawności podpisu (np. z powodu braku certyfikatu) podpis jest uznawany za niepoprawny i żądanie HI1 nie jest obsługiwane.

Załącznik nr 6

1.Struktura pliku z wykazem połączeń abonenta telefonii stacjonarnej

Poniżej zamieszczona została struktura pliku XML proponowana jako format danych, w którym przedsiębiorca telekomunikacyjny dostarczać powinien dane o usługach telekomunikacyjnych realizowanych na rzecz abonenta sieci stacjonarnej.

```
<?xml version="1.0" encoding="ISO-8859-2" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<!-- definicja formatu numeru telefonu (maks. 18 cyfr) -->
<xs:simpleType name="t_numer">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{1,18}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu wykorzystywanej daty -->
<xs:simpleType name="t_data">
<xs:restriction base="xs:dateTime"/>
</xs:simpleType>

<!-- definicja formatu nazwy abonenta -->
<xs:simpleType name="t_nazwa">
<xs:restriction base="xs:string">
<xs:maxLength value="50"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu adresu i lokalizacji aparatu abonenta -->
<xs:simpleType name="t_adres">
<xs:restriction base="xs:string">
<xs:maxLength value="200"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu długosci połaczenia w sekundach-->
<xs:simpleType name="t_dlugosc">
<xs:restriction base="xs:nonNegativeInteger"/>
</xs:simpleType>

<!-- definicja formatu identyfikatora operatora ( 4lub 5 cyfr)-->
<xs:simpleType name="t_operator">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{4,5}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja listy rodzajów połaczenia -->
<xs:simpleType name="t_lista_rodzajow">
<xs:restriction base="xs:string">
<xs:pattern value="audio|data|sms|faks"/>
</xs:restriction>
</xs:simpleType>
```

```
<!-- definicja listy usług -->
<xs:simpleType name="t_lista_uslug">
<xs:restriction base="xs:string">
<xs:pattern value="cfu|cfb|cfnr|konferencja"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu usług zwiazanych z połaczeniem -->
<xs:complexType name="t_usluga">
<xs:sequence>
<!-- nazwa us³ugi wykorzystywanej przy po³aczeniu -->
<xs:element name="nazwa_uslugi" type="t_lista_uslug" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<!-- definicja formatu pojedynczego połaczenia -->
<xs:complexType name="t_polaczenie">
<xs:all>
<!-- numer kolejny-->
<xs:element name="lp" type="xs:positiveInteger"/>
<!-- numer abonenta inicjujacego połączenie w formacie ITU-T E.164 -->
<xs:element name="nr_zrodlowy" type="t_numer"/>
<!-- numer wybrany w formacie ITU-T E.164 -->
<xs:element name="nr_wybrany" type="t_numer"/>
<!-- numer uzyskany w formacie ITU-T E.164 -->
<xs:element name="nr_uzyskany" type="t_numer" minOccurs="0"/>
<!-- data i czas rozpoczecia połaczenia -->
<xs:element name="czas_start" type="t_data"/>
<!-- czas trwania połaczenia -->
<xs:element name="dlugosc" type="t_dlugosc" minOccurs="0"/>
<!-- rodzaj połaczenia -->
<xs:element name="rodzaj" type="t_lista_rodzajow" minOccurs="0"/>
<!-- identyfikator operatora -->
<xs:element name="idop" type="t_operator"/>
<!-- us³ugi wykorzystywane przy po³aczeniu -->
<xs:element name="uslugi" type="t_usluga" minOccurs="0"/>
<!-- nazwa odbiorcy połaczenia -->
<xs:element name="nazwa_odb" type="t_nazwa" minOccurs="0"/>
<!-- adres odbiorcy połaczenia -->
<xs:element name="adres_odb" type="t_adres" minOccurs="0"/>
<!-- lokalizacja urzadzenia koncowego odbiorcy -->
<xs:element name="lok_odb" type="t_adres" minOccurs="0"/>
</xs:all>
</xs:complexType>

<!-- definicja formatu raportu dotyczacego połączeń -->
<xs:complexType name="t_polaczenia">
<xs:sequence>
<!-- numer abonenta inicjujacego połączenie w formacie ITU-T E.164 -->
<xs:element name="numer" type="t_numer"/>
<!-- data i czas poczatku zgromadzonych danych -->
<xs:element name="okres_od" type="t_data"/>
<!-- data i czas konca zgromadzonych danych -->
<xs:element name="okres_do" type="t_data"/>
<!-- nazwa abonenta -->
<xs:element name="nazwa" type="t_nazwa"/>
<!-- adres abonenta -->
<xs:element name="adres" type="t_adres"/>
<!-- lokalizacja urzadzenia koncowego abonenta -->
<xs:element name="lokalizacja" type="t_adres"/>
```

```
<!-- lista wykonanych połączeń -->
<xs:element name="polaczenie" type="t_polaczenie" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:element name="polaczenia" type="t_polaczenia"/>
</xs:schema>
```

2.Struktura pliku z wykazem połączeń abonenta telefonii komórkowej w zakresie połączeń rozpoczynanych

Poniżej zamieszczona została struktura pliku XML proponowana jako format danych, w którym przedsiębiorca telekomunikacyjny dostarczać powinien dane o usługach telekomunikacyjnych realizowanych na rzecz abonenta sieci komórkowej, w odniesieniu do połączeń rozpoczynanych.

```
<?xml version="1.0" encoding="ISO-8859-2" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<!-- definicja formatu numeru telefonu (maks. 18 cyfr) -->
<xs:simpleType name="t_numer">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{1,18}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu wykorzystywanej daty -->
<xs:simpleType name="t_data">
<xs:restriction base="xs:dateTime"/>
</xs:simpleType>
<!-- definicja formatu nazwy abonenta -->
<xs:simpleType name="t_nazwa">
<xs:restriction base="xs:string">
<xs:maxLength value="50"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu adresu i lokalizacji aparatu abonenta -->
<xs:simpleType name="t_adres">
<xs:restriction base="xs:string">
<xs:maxLength value="200"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu długosci połaczenia w sekundach-->
<xs:simpleType name="t_dlugosc">
<xs:restriction base="xs:nonNegativeInteger"/>
</xs:simpleType>
<!-- definicja formatu identyfikatora operatora (4 lub 5 cyfr)-->
<xs:simpleType name="t_operator">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{4,5}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja numeru IMEI (26 cyfr) -->
<xs:simpleType name="t_imei">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{26}"/>
```

```
</xs:restriction>
</xs:simpleType>

<!-- definicja numeru IMSI (15 cyfr) -->
<xs:simpleType name="t_imsi">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{15}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja identyfikatora kraju i operatora (6 cyfr) -->
<xs:simpleType name="t_idkraj">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{6}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja współrzednych geograficznych -->
<xs:simpleType name="t_wspolrzedne">
<xs:restriction base="xs:string">
<xs:maxLength value="50"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja listy rodzajów połaczenia -->
<xs:simpleType name="t_lista_rodzajow">
<xs:restriction base="xs:string">
<xs:pattern value="audio|faks|csd|sms|ems|mms|video"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja listy usług -->
<xs:simpleType name="t_lista_uslug">
<xs:restriction base="xs:string">
<xs:pattern value="cfu|cfb|cfnr|konferencja"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu usług zwiazanych z połaczeniem -->
<xs:complexType name="t_usluga">
<xs:sequence>
<!-- nazwa us³ugi wykorzystywanej przy po³aczeniu -->
<xs:element name="nazwa_uslugi" type="t_lista_uslug" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<!-- definicja formatu pojedynczego połaczenia -->
<xs:complexType name="t_polaczenie">
<xs:all>
<!-- numer kolejny-->
<xs:element name="lp" type="xs:positiveInteger"/>
<!-- numer abonenta inicjujacego połączenie w formacie ITU-T E.164 -->
<xs:element name="nr_zrodlowy" type="t_numer"/>
<!-- numer IMSI abonenta -->
<xs:element name="nr_imsi" type="t_imsi"/>
<!-- numer IMEI urzadzenia -->
<xs:element name="nr_imei" type="t_imei"/>
<!-- numer wybrany w formacie ITU-T E.164 -->
<xs:element name="nr_wybrany" type="t_numer"/>
<!-- numer uzyskany w formacie ITU-T E.164 -->
```

```
<xs:element name="nr_uzyskany" type="t_numer" minOccurs="0"/>
<!-- data i czas rozpoczecia połaczenia -->
<xs:element name="czas_start" type="t_data"/>
<!-- czas trwania połaczenia -->
<xs:element name="dlugosc" type="t_dlugosc" minOccurs="0"/>
<!-- rodzaj połaczenia -->
<xs:element name="rodzaj" type="t_lista_rodzajow" minOccurs="0"/>
<!-- identyfikator operatora -->
<xs:element name="idop" type="t_operator"/>
<!-- usługi wykorzystywane przy po³aczeniu -->
<xs:element name="uslugi" type="t_usluga" minOccurs="0"/>
<!-- nazwa odbiorcy połaczenia -->
<xs:element name="nazwa_odb" type="t_nazwa" minOccurs="0"/>
<!-- adres odbiorcy połaczenia -->
<xs:element name="adres_odb" type="t_adres" minOccurs="0"/>
<!-- poczatkowa aktywacja odbiorcy dla pre-paid -->
<xs:element name="akt_odb" type="t_data" minOccurs="0"/>
<!-- współrzedne geograficzne komórki w której dokonano poczatkowej aktywacji odbiorcy -->
<xs:element name="komorka_akt_odb" type="t_wspolrzedne" minOccurs="0"/>
<!-- współrzedne geograficzne komórki w której znajdował sie odbiorca -->
<xs:element name="wspolrzedne_kom_odb" type="t_wspolrzedne" minOccurs="0"/>
<!-- identyfikator kraju i operatora w której znajdowa³ sie abonent -->
<xs:element name="idkraj_odb" type="t_idkraj" minOccurs="0"/>
</xs:all>
</xs:complexType>

<!-- definicja formatu raportu dotyczacego połączeń -->
<xs:complexType name="t_polaczenia">
<xs:sequence>
<!-- numer abonenta inicjujacego połączenie w formacie ITU-T E.164 -->
<xs:element name="numer" type="t_numer"/>
<!-- data i czas poczatku zgromadzonych danych -->
<xs:element name="okres_od" type="t_data"/>
<!-- data i czas konca zgromadzonych danych -->
<xs:element name="okres_do" type="t_data"/>
<!-- nazwa abonenta -->
<xs:element name="nazwa" type="t_nazwa" minOccurs="0"/>
<!-- adres abonenta -->
<xs:element name="adres" type="t_adres" minOccurs="0"/>
<!-- poczatkowa aktywacja dla pre-paid -->
<xs:element name="aktywacja" type="t_data" minOccurs="0"/>
<!-- współrzedne geograficzne komórki w której dokonano poczatkowej aktywacji -->
<xs:element name="komorka_aktywacji" type="t_wspolrzedne" minOccurs="0"/>
<!-- lista wykonanych połączeń -->
<xs:element name="polaczenie" type="t_polaczenie" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:element name="polaczenia" type="t_polaczenia"/>
</xs:schema>
```

3.Struktura pliku z wykazem połączeń abonenta telefonii komórkowej w zakresie połączeń zakańczanych

Poniżej zamieszczona została struktura pliku XML proponowana jako format danych, w którym przedsiębiorca telekomunikacyjny dostarczać powinien dane o usługach telekomunikacyjnych realizowanych na rzecz abonenta sieci komórkowej, w odniesieniu do połączeń rozpoczynanych.

```
<?xml version="1.0" encoding="ISO-8859-2" ?>
```

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<!-- definicja formatu numeru telefonu (maks. 18 cyfr) -->
<xs:simpleType name="t_numer">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{1,18}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu wykorzystywanej daty -->
<xs:simpleType name="t_data">
<xs:restriction base="xs:dateTime"/>
</xs:simpleType>

<!-- definicja formatu nazwy abonenta -->
<xs:simpleType name="t_nazwa">
<xs:restriction base="xs:string">
<xs:maxLength value="50"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu adresu i lokalizacji aparatu abonenta -->
<xs:simpleType name="t_adres">
<xs:restriction base="xs:string">
<xs:maxLength value="200"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu długosci połaczenia w sekundach-->
<xs:simpleType name="t_dlugosc">
<xs:restriction base="xs:nonNegativeInteger"/>
</xs:simpleType>

<!-- definicja formatu identyfikatora operatora (4 lub 5 cyf)-->
<xs:simpleType name="t_operator">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{4,5}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja numeru IMEI (26 cyfr) -->
<xs:simpleType name="t_imei">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{26}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja numeru IMSI (15 cyfr) -->
<xs:simpleType name="t_imsi">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{15}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja numeru MSRN (maks. 18 cyfr) -->
<xs:simpleType name="t_msrn">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{1,18}"/>
</xs:restriction>
</xs:simpleType>
```

```
<!-- definicja identyfikatora kraju i operatora (6 cyfr) -->
<xs:simpleType name="t_idkraj">
<xs:restriction base="xs:string">
<xs:pattern value="[0-9]{6}"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja współrzednych geograficznych -->
<xs:simpleType name="t_wspolrzedne">
<xs:restriction base="xs:string">
<xs:maxLength value="50"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja listy rodzajów połaczenia -->
<xs:simpleType name="t_lista_rodzajow">
<xs:restriction base="xs:string">
<xs:pattern value="audio|faks|csd|sms|ems|mms|video"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja listy usług -->
<xs:simpleType name="t_lista_uslug">
<xs:restriction base="xs:string">
<xs:pattern value="cfu|cfb|cfnr|konferencja"/>
</xs:restriction>
</xs:simpleType>

<!-- definicja formatu usług zwiazanych z połaczeniem -->
<xs:complexType name="t_usluga">
<xs:sequence>
<!-- nazwa us³ugi wykorzystywanej przy po³aczeniu -->
<xs:element name="nazwa_uslugi" type="t_lista_uslug" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<!-- definicja formatu pojedynczego połaczenia -->
<xs:complexType name="t_polaczenie">
<xs:all>
<!-- numer kolejny-->
<xs:element name="lp" type="xs:positiveInteger"/>
<!-- numer abonenta inicjujacego połączenie w formacie ITU-T E.164 -->
<xs:element name="nr_zrodlowy" type="t_numer"/>
<!-- numer IMSI abonenta -->
<xs:element name="nr_imsi" type="t_imsi"/>
<!-- numer IMEI urzadzenia -->
<xs:element name="nr_imei" type="t_imei"/>
<!-- numer wybrany w formacie ITU-T E.164 -->
<xs:element name="nr_wybrany" type="t_numer"/>
<!-- numer uzyskany w formacie ITU-T E.164 -->
<xs:element name="nr_uzyskany" type="t_numer" minOccurs="0"/>
<!-- data i czas rozpoczecia połaczenia -->
<xs:element name="czas_start" type="t_data"/>
<!-- czas trwania połaczenia -->
<xs:element name="dlugosc" type="t_dlugosc" minOccurs="0"/>
<!-- rodzaj połaczenia -->
<xs:element name="rodzaj" type="t_lista_rodzajow" minOccurs="0"/>
<!-- identyfikator operatora -->
<xs:element name="idop" type="t_operator"/>
```

```
<!-- us³ugi wykorzystywane przy po³aczeniu -->
<xs:element name="uslugi" type="t_usluga" minOccurs="0"/>
<!-- nazwa odbiorcy połaczenia -->
<xs:element name="nazwa_odb" type="t_nazwa" minOccurs="0"/>
<!-- adres odbiorcy połaczenia -->
<xs:element name="adres_odb" type="t_adres" minOccurs="0"/>
<!-- poczatkowa aktywacja odbiorcy dla pre-paid -->
<xs:element name="akt_odb" type="t_data" minOccurs="0"/>
<!-- współrzedne geograficzne komórki w której dokonano poczatkowej aktywacji odbiorcy -->
<xs:element name="komorka_akt_odb" type="t_wspolrzedne" minOccurs="0"/>
<!-- współrzedne geograficzne komórki w której znajdowa³ sie odbiorca -->
<xs:element name="wspolrzedne_kom_odb" type="t_wspolrzedne" minOccurs="0"/>
<!-- identyfikator kraju i operatora w której znajdowa³ sie odbiorca -->
<xs:element name="idkraj_odb" type="t_idkraj" minOccurs="0"/>
<!-- numer MSRN odbiorcy -->
<xs:element name="msrn_odb" type="t_msrn" minOccurs="0"/>
</xs:all>
</xs:complexType>

<!-- definicja formatu raportu dotyczacego połączeń -->
<xs:complexType name="t_polaczenia">
<xs:sequence>
<!-- numer abonenta inicjujacego połączenie w formacie ITU-T E.164 -->
<xs:element name="numer" type="t_numer"/>
<!-- data i czas poczatku zgromadzonych danych -->
<xs:element name="okres_od" type="t_data"/>
<!-- data i czas konca zgromadzonych danych -->
<xs:element name="okres_do" type="t_data"/>
<!-- nazwa abonenta -->
<xs:element name="nazwa" type="t_nazwa" minOccurs="0"/>
<!-- adres abonenta -->
<xs:element name="adres" type="t_adres" minOccurs="0"/>
<!-- początkowa aktywacja dla pre-paid -->
<xs:element name="aktywacja" type="t_data" minOccurs="0"/>
<!-- współrzednych geograficzne komórki w której dokonano poczatkowej aktywacji -->
<xs:element name="komorka_aktywacji" type="t_wspolrzedne" minOccurs="0"/>
<!-- lista wykonanych połączeń -->
<xs:element name="polaczenie" type="t_polaczenie" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:element name="polaczenia" type="t_polaczenia"/>
</xs:schema>
```

4.Akronimy

BS-[Billing System] system bilingowy,
CDR-[Call Detailed Record] szczegółowy rekord o połaczeniu,
CFB-[Call Forwarding on Busy] usługa przekierowania połaczenia w przypadku zajetosci,
CFNR-[Call Forwarding on Replay] usługa przekierowania połaczenia w przypadku nie zgłaszania sie,
CFU-[Call Forwarding Unconditional] usługa bezwarunkowego przekierowania połaczenia,
HPLMN-[Home PLMN].macierzysta siec telefoni komórkowej,
IGR-[Incoming Gateway Rekord] rekord generowany na wejsciu centrali granicznej,
IMEI-[International Mobile Equipment Identity] miedzynarodowy numer identyfikacyjny terminala,
IMSI-[International Mobile Subscriber Identity] miedzynarodowy numer abonenta ruchomego, IMSI,

MCC-[Mobile country code] unikalny numer identyfikujacy kraj, w którym działa dana sieć telefonii bezprzewodowej,
MNC-[Mobile network code] unikalny w obrebie danego kraju numer, identyfikujacy sieć telefonii bezprzewodowej,
MOC-[Mobile Originating Call] rekord generowany w centrali wyjsciowej MSC,
MSISDN-[Mobile Station International ISDN Number] miedzynarodowy numer abonenta sieci ISDN,
MTC-[Mobile Terminating Call] rekord generowany w centrali przyjsciowej MSC,
OGR-[Outgoing Gateway Record].rekord generowany na wyjsciu centrali granicznej sieci wizytowanej do sieci macierzystej bilingowych miedzy systemami,
PLMN-[Public Land Mobile Network] publiczna siec komórkowa,
RGR-[Roaming Gateway Record] rekord generowany na wyjsciu centrali graniczne w przypadku połączeń skierowanych do abonenta przebywajacego w sieci wizytowanej,
SMS-MO-[Short Message Service – Mobile Originating] rekord generowany w centrali MSC wyjsciowej,
SMS-MT-[Short Message Service – Mobile Terminating] rekord generowany w centrali MSC przyjsciowej,
TAP-[Transffered Account Procedure] procedura transferu informacji taryfikacyjnych.

Projekt

ROZPORZĄDZENIE
MINISTRA SPRAWIEDLIWOŚCI

z dnia

w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji - do gromadzenia danych, niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji oraz sposobów zabezpieczania danych informatycznych

Na podstawie art. 218b ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. 1. Rozporządzenie określa:
1) sposób technicznego przygotowania systemów i sieci służących do przekazywania informacji - do gromadzenia danych , o których mowa w art. 218 § 1 Kodeks postępowania karnego, niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji;
2) sposoby zabezpieczania danych informatycznych w urządzeniach zawierających te dane oraz w systemach i na nośnikach danych informatycznych, zwanych dalej ”nośnikami”, mając na uwadze konieczność zabezpieczenia tych danych przed ich utratą, zniekształceniem lub nieuprawnionym ujawnieniem, zwanych dalej ”danymi zapisanymi”.

2. Ilekroć w rozporządzeniu jest mowa o:
1) "użytkowniku", rozumie się przez to użytkownika, w znaczeniu określonym ustawą z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[2)]);
2) "podmiocie uprawnionym", rozumie się przez to sąd lub prokuratora;
3) "podmiocie obowiązanym", rozumie się przez to urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną, o których mowa w art. 218a § 1 Kodeks postępowania karnego.

§ 2. Przygotowanie systemów i sieci służących do przekazywania informacji - do gromadzenia danych, o których mowa w § 1 ust. 1 pkt 1 polega na zapewnieniu przez podmiot obowiązany technicznych możliwości sporządzania wykazów tych danych , niezwłocznie w ciągu całej doby.

§ 3. Podmiot obowiązany gromadzi dane związane z przekazami informacji, przetwarzane przez ten podmiot w związku z prowadzoną działalnością telekomunikacyjną lub stanowiące przedmiot świadczonych usług w zakresie przekazu informacji.

§ 4. 1. Zabezpieczenia danych zapisanych dokonuje się przy użyciu środków technicznych, w sposób umożliwiający ich późniejsze odtworzenie przy użyciu urządzeń odtwarzających.

2. Zabezpieczenia danych zapisanych dokonuje osoba upoważniona przez podmiot obowiązany, przy użyciu środków technicznych podmiotu obowiązanego, w urządzeniach zawierających te dane, w systemie lub na nośniku.

3. W przypadku zabezpieczenia danych zapisanych na nośniku, osoba dokonująca tego zabezpieczenia zapisuje lub oznacza na tym nośniku:
1) sygnaturę akt sprawy, w której czynność ta została zlecona;
2) swoje imię, nazwisko i stanowisko służbowe;
3) dane dotyczące podstawy zabezpieczenia;
4) czas dokonania zabezpieczenia.

§ 5. Z czynności zabezpieczenia danych zapisanych osoba, o której mowa w § 4 ust. 2, sporządza notatkę, w której zamieszcza:
1) datę i miejsce sporządzenia notatki oraz sygnaturę akt sprawy;
2) swoje imię, nazwisko i stanowisko służbowe;
3) dane dotyczące podstawy zabezpieczenia;
4) imię i nazwisko użytkownika systemu lub sieci albo nazwę podmiotu będącego użytkownikiem, w stosunku do którego zarządzono zabezpieczenie danych zapisanych;
5) czas dokonania zabezpieczenia danych zapisanych;
6) dane identyfikujące miejsce zabezpieczenia danych zapisanych;
7) w miarę potrzeby inne dane dotyczące dokonywanej czynności.

§ 6. 1. Podmiot obowiązany gromadzi dane o dokonanych zabezpieczeniach danych zapisanych.
2. Gromadzone dane, o których mowa w ust. 1, obejmują:
1) sygnaturę akt sprawy i datę wydania postanowienia o zabezpieczeniu danych zapisanych;
2) nazwę podmiotu uprawnionego;
3) datę dokonania zabezpieczenia;
4) imię i nazwisko użytkownika systemu lub sieci albo nazwę podmiotu będącego użytkownikiem, w stosunku do którego zarządzono zabezpieczenie danych zapisanych;
5) czas trwania zabezpieczenia,
6) dane identyfikujące miejsce zabezpieczenia danych zapisanych.

§ 7. Zabezpieczone dane zapisane przechowuje się w warunkach zabezpieczających przed ich utratą, zniekształceniem lub nieuprawnionym ujawnieniem oraz zniszczeniem lub uszkodzeniem nośnika.

§ 8. Rozporządzenie wchodzi w życie z dniem ..... 2008 r.

Minister Sprawiedliwości

w porozumieniu

Minister Infrastruktury

Minister Obrony Narodowej

Minister Spraw Wewnętrznych i Administracji

---

1) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 50, poz. 580, Nr 62, poz. 717, Nr 73, poz. 852 i Nr 93, poz. 1027, z 2001 r. Nr 98, poz. 1071 i Nr 106, poz. 1149, z 2002 r. Nr 74, poz. 676, z 2003 r. Nr 17, poz. 155, Nr 111, poz. 1061 i Nr 130, poz. 1188, z 2004 r. Nr 51, poz. 514, Nr 69, poz. 62, Nr 93, poz. 889, Nr 240, poz. 2405 i Nr 264, poz. 2641, z 2005 r. Nr 10, poz. 70, Nr 48, poz. 461, Nr 77, poz. 680, Nr 96, poz. 821, Nr 141, poz. 1181, Nr 143, poz. 1203, Nr 163, poz. 1363, Nr 169, poz. 1416 i Nr 178, poz. 1479, z 2006 r. Nr 15, poz. 118, Nr 66, poz. 467, Nr 95, poz. 659, Nr 104, poz. 708 i 711, Nr 141, poz. 1009 i 1013, Nr 167, poz. 1192 i Nr 226, poz. 1647 i 1648, z 2007 r. Nr 20, poz. 116, Nr 64, poz. 432, Nr 80, poz. 539, Nr 89, poz. 589, Nr 99, poz. 664, Nr 112, poz. 766 i Nr 123, poz. 849 oraz z 2008 r. Nr 100, poz. 648 i Nr 107, poz. 686.

2) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556 oraz z 2008 r. Nr 17, poz. 101.

Uzasadnienie

Projekt ustawy o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw, w art. 5 projektu przewiduje nowelizację art. 218 §1 i art. 218b ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.), dalej kpk.

Projektowane zmiany wskazanych wyżej przepisów powodują konieczność zredagowania projektu aktu wykonawczego, uwzględniającego zmiany w siatce pojęciowej, który zastąpiłyby aktualne rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz. U. Nr 100, poz. 1023.).

Projekt nowego rozporządzenia Ministra Sprawiedliwości w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych, sprowadzono do zastąpienia treści tych przepisów obowiązujących, które odnoszą się do pojęć, które staną się nieaktualne z chwilą wejścia w życie projektowanych zmian ustawowych.

Przepis § 1 ust 1 pkt 1
- za projektem art. 218b kpk umieszczono odesłanie do treści art. 218 kpk;

Przepis § 1 ust 2 pkt 1
- określono pojęcie „nośników danych informatycznych” oraz na nowo zdefiniowano pojęcie „danych zapisanych”;

Przepis § 1 ust 2 pkt 1
- określono pojęcie „użytkownika”;

Przepis § 2
- zmiana, polegająca na zastąpieniu terminu „nośnik informatyczny” terminem „nośnik”, stanowi konsekwencję projektowanego brzmienia przepisu § 1 ust 1 pkt 2;

Przepis § 4
- zmiana, polegająca na zastąpieniu terminu „nośnik informatyczny” terminem „nośnik”, stanowi konsekwencję projektowanego brzmienia przepisu § 1 ust 1 pkt 2.

W pozostałej części projekt rozporządzenia zawiera propozycje przepisów w brzmieniu obowiązującym.

Ocena skutków regulacji

Podmioty na które oddziałuje rozporządzenie.

Projektowane rozporządzenia nie będzie oddziaływać na sądy powszechne.

Zakres konsultacji.

Przedmiotowy projekt zostanie przekazany do zaopiniowania (zakres konsultacji do ustalenia).

Wpływ aktu normatywnego na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego .

Wejście w życie projektowanego rozporządzenia nie powinno spowodować bezpośredniego zwiększenia lub zmniejszenia dochodów budżetu Państwa.

Wpływ aktu normatywnego na rynek pracy, konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorstw oraz na sytuację i rozwój regionalny.

Niniejsze rozporządzenie nie spowoduje skutków na rynku pracy, w sferze konkurencyjności wewnętrznej i zewnętrznej gospodarki a także pozostanie bez wpływu na rozwój regionalny. Wpływ pośredni natomiast, może wystąpić w wyniku podniesienia poziomu sprawności działania sądów powszechnych i współpracy z organami instytucji wymiaru sprawiedliwości w innych krajach.

Zgodność projektu z prawem Unii Europejskiej.

Rozporządzenie jest zgodne z prawem Unii Europejskiej.

Projekt niniejszego rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej, stosownie do przepisów ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414).

P R O J E K T

ROZPORZĄDZENIE RADY MINISTRÓW
z dnia
w sprawie trybu nieodpłatnego udostępniania radiowych urządzeń nadawczych lub nadawczo-odbiorczych stosowanych w służbach radiokomunikacyjnych przez podmioty niebędące przedsiębiorcami telekomunikacyjnymi

Na podstawie art. art. 177 ust. 6 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa tryb nieodpłatnego udostępniania radiowych urządzeń nadawczych lub nadawczo-odbiorczych zwanych dalej "urządzeniami", stosowanych w służbach radiokomunikacyjnych przez podmioty niebędące przedsiębiorcami telekomunikacyjnymi zwane dalej „podmiotami zobowiązanymi”, podmiotom i służbom wykonującym zadania: w zakresie ratownictwa, niesienia pomocy ludności, na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, a także podmiotom właściwymi w sprawach zarządzania kryzysowego, zwanym dalej „podmiotami uprawnionymi”.

§ 2. 1. Decyzję o udostępnieniu urządzenia wydaje wojewoda właściwy terytorialnie ze względu na miejsce zamieszkania lub siedzibę podmiotu zobowiązanego, na wniosek uprawnionego podmiotu.
2. Przed wydaniem decyzji wojewoda może zasięgnąć opinii Prezesa Urzędu Komunikacji Elektronicznej. Prezes Urzędu Komunikacji Elektronicznej niezwłocznie udziela informacji w zakresie posiadanych danych.
3. Decyzja, o której mowa w ust. 1, może być ogłoszona ustnie, bez uzasadnienia, w całości lub części, jeżeli wymagają tego względy obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

§ 3. Wniosek określony w § 2 powinien zawierać: nazwę uprawnionego podmiotu, dane adresowe podmiotu zobowiązanego, nazwę urządzenia, przewidywany czas udostępnienia oraz podpis i pieczęć podmiotu uprawnionego.

§ 4. W wypadku wpłynięcia kilku wniosków dotyczących tego samego urządzenia, decyzję o jego udostępnieniu podejmuje wojewoda, o którym mowa w § 2.

§ 5. Udostępnienie urządzenia uprawnionym podmiotom następuje przy udziale podmiotu zobowiązanego, chyba że korzystanie z urządzenia bez udziału podmiotu zobowiązanego uzasadnione jest szczególnymi okolicznościami.

§ 6. Zakończenie udostępnienia urządzenia następuje bez zbędnej zwłoki po ustąpieniu sytuacji szczególnych zagrożeń oraz stanów nadzwyczajnych.

§ 7. Podmiot uprawniony zwraca urządzenie w stanie nienaruszonym. W przypadku zniszczenia, uszkodzenia lub poniesienia dodatkowych kosztów eksploatacyjnych urządzenia podmiotowi zobowiązanemu przysługuje rekompensata na podstawie przepisów odrębnych.

§ 8. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331 i Nr 82, poz. 556 oraz z 2008 r. Nr 17, poz. 101.

UZASADNIENIE

Przedmiotowe rozporządzenie jest wykonaniem upoważnienia z art. 177 ust. 6 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Jego celem jest określenie trybu, w jakim podmioty obowiązane na podstawie tej ustawy udostępniają urządzenia radiowe nadawcze i nadawczo-odbiorcze podmiotom uprawnionym wykonującym zadania: w zakresie ratownictwa, niesienia pomocy ludności, na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, a także podmiotom właściwymi w sprawach zarządzania kryzysowego.

Udostępnianie urządzeń odbywa się na podstawie decyzji wojewody właściwego terytorialnie ze względu na miejsce zamieszkania lub siedzibę podmiotu zobowiązanego do udostępnienia, wydawanej na wniosek uprawnionego podmiotu.

OCENA SKUTKÓW REGULACJI

Skutkiem regulacji zawartej w projekcie jest nałożenie na podmioty niebędące przedsiębiorcami telekomunikacyjnymi, posługujące się radiowymi urządzeniami nadawczymi lub nadawczo-odbiorczymi, stosowanymi w służbach radiokomunikacyjnych, obowiązku udostępniania tych urządzeń służbom ustawowo odpowiedzialnym za bezpieczeństwo państwa oraz bezpieczeństwo i porządek publiczny. Regulacja zobowiązuje wojewodów do wydawania w uzasadnionych wypadkach decyzji administracyjnych w zakresie udostępnienia tych urządzeń. Zakłada również współuczestniczenie Prezesa UKE w procesie opracowywania tych decyzji.

Regulacja zawarta w rozporządzeniu nie będzie miała wpływu na rynek pracy, rozwój regionalny oraz konkurencyjność wewnętrzną i zewnętrzną gospodarki. Rozporządzenie nie spowoduje również skutków finansowych dla budżetu państwa oraz budżetów jednostek samorządu terytorialnego.

Projektowane rozporządzenie jest zgodne z prawem Unii Europejskiej.

Projekt rozporządzenia nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych oraz nie wymaga przedstawienia właściwym instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu.