**15.05.2020**

**Zestawienie zgłoszonych uwag do projektu rozporządzenia Ministra Cyfryzacji w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług**

**III TURA OPINIOWANIA – konferencja uzgodnieniowa**

Uwagi zgłoszone przez:

1. Komisja Nadzoru Finansowego (KNF) – nie było przedstawiciela na konferencji uzgodnieniowej
2. Najwyższa Izba Kontroli (NIK) – nie było przedstawiciela na konferencji uzgodnieniowej
3. Rada ds. Cyfryzacji (RdC)
4. Urząd Komunikacji Elektronicznej (UKE)
5. Urząd Ochrony Konkurencji i Konsumentów (UOKIK)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **l.p.** | **Jednostka redakcyjna projektu** | | **Zgłaszający** | | **Treść uwagi** | **Stanowisko MC** |
|  | Ogólne | | NIK | | NIK zauważa możliwe trudności w stosowaniu projektowanego rozporządzenia po jego przyjęciu, jak również niewystarczalność oceny skutków regulacji, w tym w szczególności oszacowania wpływu projektowanej regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców.  W powyższym zakresie w pierwszej kolejności należy zasygnalizować, że obowiązki przedsiębiorców telekomunikacyjnych (§ 2 projektowanego rozporządzenia) zakreślone są w sposób dość ogólnikowy. W przyszłej praktyce stosowania rozporządzenia może pojawić się wobec tego wątpliwość, czy działanie danego przedsiębiorcy telekomunikacyjnego będzie adekwatne i wystarczające – a zatem, czy określony przyjęty przez danego przedsiębiorcę środek techniczny lub organizacyjny bądź metoda zapobiegania zagrożeniom, o których mowa w art. 175a ust. 1 i art. 175c ust. 1 *ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U.  z 2019 r. poz. 2460, ze zm.*), są właściwe i realizują wymogi wynikające z rozporządzenia.  Projektowane rozporządzenie nie różnicuje również obowiązków (zakresu koniecznych rozwiązań technicznych lub organizacyjnych bądź metod) podlegających wdrożeniu przez poszczególnych przedsiębiorców telekomunikacyjnych. Wydaje się, iż zakres minimalnych środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom mógłby być uzależniony czy to od wielkości przedsiębiorcy telekomunikacyjnego czy też od istoty prowadzonej działalności. Jakkolwiek możliwość taką wydaje się przewidywać sam projektodawca, sposób realizacji tego założenia budzi wątpliwości. Jak wskazał bowiem projektodawca w uzasadnieniu projektu rozporządzenia, „*(…) różnice w stosowaniu rozporządzenia będą miały charakter faktyczny, a nie prawny. Środki proponowane w projekcie są skalowalne i sposób ich wdrożenia będzie zależny od wielkości i profilu działania przedsiębiorcy. Upoważnienie ustawowe odnosi się do dostawców i operatorów bez rozróżnienia na wielkość działalności przedsiębiorcy, zatem nie jest możliwe rozróżnianie obowiązków w samej treści rozporządzenia*”.  W świetle powyższego wskazać należy, iż jeżeli w ocenie samego projektodawcy nie daje się ustalić obowiązków poszczególnych, rodzajowo określonych, przedsiębiorców na poziomie rozporządzenia, to tym bardziej problematyczne będzie ustalenie przez adresatów tych norm zakresu ich faktycznych obowiązków, a następnie wzorca postępowania, który będzie od nich wymagany i będzie mógł podlegać weryfikacji. | Uwaga nieuwzględniona.  W opinii projektodawcy środki i metody wskazane w § 2 projektu rozporządzenia nie są określone w sposób ogólnikowy. Są one wskazane co do celu, który ma być osiągnięty. Alternatywą jest wskazanie ściśle określonych środków (np. rodzaje i wysokość płotów zabezpieczających infrastrukturę), co jest niepożądanym modelem.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólne | | NIK | | Wreszcie zasygnalizować należy, iż zgodnie z treścią oceny skutków regulacji projektowane w rozporządzeniu regulacje nie będą mieć w okresie 10 lat od wejścia  w życie aktu normatywnego wpływu – w ujęciu pieniężnym – na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców. W zakresie wpływu w ujęciu niepieniężnym przewidziano z kolei, iż „*zastosowanie środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom wskazanych w projekcie może wymusić zmiany w organizacji oraz aktualizację istniejących rozwiązań technicznych*”. Już tylko to wskazuje, iż nastąpi zwiększenie obciążeń regulacyjnych, a przedsiębiorcy staną przed koniecznością przedsięwzięcia również nowych działań oczekiwanych przez projektodawcę. Budzi wobec tego wątpliwości również dalsze stwierdzenie, iż „*projekt rozporządzenia nie ma wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców (…)*”. Jakkolwiek w pełni zgodzić należy się z działaniami zwiększającymi szeroko pojęte bezpieczeństwo telekomunikacyjne i sieciowe, co musi wiązać się z określonymi nakładami inwestycyjnymi i działaniami organizacyjnymi, co z kolei nie zawsze jest mierzalne w pieniądzu i możliwe do precyzyjnego skwantyfikowania na poziomie oceny skutków regulacji, postulować należy doprecyzowanie analizy skutków projektowanych rozwiązań. | Uwaga nieuwzględniona.  Należy wskazać, że projekt rozporządzenia wskazuje jedynie na środki i metody, które mają być stosowane.  Obowiązek zabezpieczania sieci istnieje od 2004 r. i jego wpływ na gospodarkę był badany wówczas.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólne | | Rada ds. Cyfryzacji  (uwaga zaktualizowana) | | Ponadto warto rozważyć, czy nie uwzględnić kwestii zapewnienia udziału polskich firm w projektach realizowanych w oparciu o 5 G.  **Warto uwzględnić konieczność zapewnienia otwartych i powszechnie dostępnych standardów**, inaczej polskie firmy będą zbierać tylko niewielką część z tego obszaru oferowanego przez 3 głównych dostawców i nie zlikwidujemy, a nawet nie zmniejszymy ich "vendor lock".  Rada uważa, że powinniśmy nadążać za najnowszymi trendami w branży telekomunikacyjnej, a w szczególności w ramach ORAN (https://www.o-ran.org/), TIP (https://telecominfraproject.com/) czy ONF (https://www.opennetworking.org/). Model, w którym cały sprzęt, oprogramowanie i integracja do danego elementu infrastruktury sieciowej dostarczane są od jednego dostawcy, jest sukcesywnie wypierany przez zakupy od niezależnych od siebie dostawców, z zachowaniem interoperacyjności opartej na standardach telekomunikacyjnych. | Wyjaśnienie.  W zakresie wykorzystywanych standardów, projekt rozporządzenia jest neutralny technologicznie i nie promuje żadnego rozwiązania krajowego - MC promuje stosowanie otwartych standardów.  Na konferencji:  Przedstawiciel Rady ds. Cyfryzacji przyjął wyjaśnienia MC. |
|  | Ogólne | | UOKIK | | W nawiązaniu do naszej wcześniejszej korespondencji i uwag zgłoszonych przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów do *projektu rozporządzenia Ministra Cyfryzacji w  sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług*, chcieliśmy zwrócić uwagę, że nie jest dla nas jasne jaka jest podstawa materialnoprawna do zawierania ewentualnych porozumień.  Jak wynika, z informacji przez Państwo przekazanych przypuszczają Państwo, że w celu realizacji postanowień rozporządzenia, przedsiębiorcy będą zawierać porozumienia, które mogą naruszać konkurencję, jednak przy spełnieniu warunków z art. 8 u.o.k.k. będą najprawdopodobniej podlegały wyłączeniu indywidualnemu.  Jednakże wskazujemy, że aktualne uzasadnienie błędnie sugeruje, że podstawą do zawarcia porozumienia jest art. 8 ustawy o ochronie konkurencji i konsumentów (fragment uzasadnienia: "Legalność tego rozwiązania opiera się na art. 8 ust. 1 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369, z późn. zm.), zwanej dalej „uokik”. Na podstawie tego przepisu przedsiębiorcy zawierają między sobą porozumienie.")  Wskazany przepis u.o.k.k. daje jedynie możliwość wyłączenia indywidualnego (przy spełnieniu określonych przesłanek) porozumienia spod zakazu wyrażonego w art. 6 uokik, nie jest jednak podstawą do zawarcia porozumienia. Taką podstawę mogłoby ewentualnie zawierać rozporządzenie. | Uwaga uwzględniona.  Oczywiście, podstawą do zawarcia porozumienia będzie potrzeba zabezpieczenia sieci, a nie art. 8 ustawy o ochronie konkurencji i konsumentów.  Uzasadnienie zostanie zmienione.  Na konferencji:  Ustalono, że treść uzasadnienia zostanie poprawiona w porozumieniu z UOKiK na odrębnym spotkaniu.  Po uzgodnieniu z UOKiK zdecydowano uwzględnić uwagę w ten sposób, że fragment uzasadnienia dotyczący ochrony konkurencji zostanie usunięty. |
|  | § 2 pkt 9 | KNF | | Dodanie nowego punktu, przesunięcie numeracji w paragrafie +1  Propozycje zmiany:  Identyfikuje i klasyfikuje kategorie danych oraz odpowiednio dane wg ich wrażliwości  Uzasadnienie:  W odniesieniu do obecnego pkt 9 (po aktualizacji pkt 10) kategorie danych, o których mowa muszą zostać najpierw określone, a dane zidentyfikowane | | Uwaga nieuwzględniona.  Identyfikacja i klasyfikacja kategorii danych to ważny element bezpieczeństwa informacji. Jest ot jednak środek, który ma największe znaczenie dla bezpieczeństwa informacji wewnątrz danej instytucji, a nie dla bezpieczeństwa i integralności sieci.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 11 i 12 | NIK | | Uzupełniająco, z legislacyjno-redakcyjnego punktu widzenia, należy wskazać na zasadność sprecyzowania w § 2 pkt 11 i 12 projektowanego rozporządzenia jednostki redakcyjnej art. 175a *ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,* do której następuje odwołanie w tych punktach. | | Uwaga nieuwzględniona.  Cały art. 175a odnosi się do incydentów, a nie tylko do jednego z jego ustępów. Stąd potrzeba do wskazania całego artykułu.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 13 | KNF | | Tekst aktualny  przeprowadza ocenę bezpieczeństwa sieci i usług telekomunikacyjnych:   1. co najmniej raz na dwa lata, 2. po każdym:   – stwierdzonym naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym naruszeniem oraz  – wykryciu podatności zwiększającej poziom ryzyka wystąpienia naruszenia  bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o  istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym  wykrytą podatnością.  Propozycja zmiany  przeprowadza ocenę bezpieczeństwa sieci i usług telekomunikacyjnych:   1. w formie audytu, co najmniej raz na rok ~~dwa lata~~, 2. w formie udokumentowanej analizy ryzyka każdorazowo po ~~każdym~~:   - istotnej modyfikacji przebiegu realizowanych procesów,  - istotnej zmianie komponentów środowiska teleinformatycznego,  – stwierdzonym naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym naruszeniem oraz  – wykryciu podatności zwiększającej poziom ryzyka wystąpienia naruszenia  bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o  istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym wykrytą podatnością.  Uzasadnienie  Z uwagi na rosnącą liczbę zagrożeń i szybkość zmian technologicznych ocenę bezpieczeństwa sieci i usług powinno wykonywać się nie rzadziej niż raz w roku i zawsze przy wprowadzaniu nowych rozwiązań sprzętowych / systemowych | | Uwaga nieuwzględniona.  Proponowana zmiana byłaby korzystna dla dużych podmiotów, które wprowadzają dużo zmian w swojej sieci oraz dla których audyt bezpieczeństwa występuje niemal jako proces ciągły. Jednak projekt obejmuje także kilka tysięcy małych podmiotów (mikro i małych przedsiębiorców), które nie są w stanie tak często prowadzić ocen bezpieczeństwa i nie jest to w ich przypadku celowe.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 14 | KNF | | Dodanie nowego punktu  Testuje bezpieczeństwo sieci i usług pod kątem odporności na identyfikowane podatności, odpowiednio do przyjętych zasad zarządzania ryzykiem | | Uwaga nieuwzględniona.  Założeniem projektodawcy było podejście do bezpieczeństwa od strony audytu, a nie testów bezpieczeństwa (pentestów).  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 3 ust. 1 pkt. 1 | | UKE | | W projektowanym § 3 ust. 1 pkt 1 użyto względem przedsiębiorców telekomunikacyjnych dostarczających sieć piątej generacji (5G) zapisu „stosuje rekomendacje”, o których mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Kategoryczny charakter ww. zapisu oznacza, że przedsiębiorcy telekomunikacyjni dostarczający sieć piątej generacji (5G) będą obowiązani do bezwzględnego stosowania rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. Niniejszy przepis, w aktualnym brzmieniu, jest zatem niespójny z zawartym na str. 13 pkt 1 uzasadnieniem do projektowanej regulacji, zgodnie z którym „Rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotyczą stosowania urządzeń informatycznych lub oprogramowania […]. Ujęcie rekomendacji w tym punkcie nie oznacza, że przedsiębiorcy są włączani w procedurę dotyczącą uwzględniania stosowania rekomendacji i nadzoru określoną w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa”. | Uwaga częściowo uwzględniona.  Zmieniono przepis w ten sposób, że należy „uwzględniać” rekomendacje Pełnomocnika w ramach swojego procesu szacowania ryzyka. Nie będą obowiązani stosować rekomendacji na równi z podmiotami krajowego systemu cyberbezpieczeństwa.  Na konferencji:  UKE podtrzymało swoje uwagi z jednoczesnym skierowaniem zapytania do przedsiębiorców.  Przedstawiciele strony społecznej nie potwierdzili potrzeby zmiany w tym zakresie.  W dalszej części przedstawiciel UKE nie zgłosił dalszych zastrzeżeń. Uwagę uznano za uzgodnioną. |
|  | § 3 ust. 1 pkt 2 | | UKE | | Podobnie zamieszczony w projektowanym § 3 ust. 1 pkt 2 kategoryczny wymóg „gwarantuje brak uzależnienia od jednego producenta” jest niespójny ze stanowiskiem samego projektodawcy, który na str. 13 pkt 2 uzasadnienia do projektowanego przepisu twierdzi, że pełna dywersyfikacja elementów sieci może nie być możliwa: „[…] konieczne jest rozważenie dywersyfikacji elementów sieci telekomunikacyjnej. Oczywistym jest, że w niektórych przypadkach będzie to niemożliwe bądź bardzo utrudnione – stąd nie wskazuje się w procentowy sposób, ile urządzeń powinno być od różnych producentów”. Powyższe stanowisko korespondowało z poprzednio konsultowaną wersją rozporządzenia, w której przedmiotowy wymóg miał charakter kierunkowy, zaś decyzja co do stopnia jego uwzględnienia należała do przedsiębiorcy.  Przy obecnym zaostrzeniu przedmiotowego obowiązku konieczne jest dookreślenie w treści przepisu, na czym ów gwarantowany brak uzależnienia ma polegać, w tym czy i jakie odstępstwa są dopuszczalne. Powyższe jest istotne zwłaszcza w kontekście warsztatów z przedsiębiorcami MNO przeprowadzonych na poprzednich etapach procesu legislacyjnego, podczas których wskazywali oni na brak możliwości współpracy w ramach jednej sieci (w wybranych jej warstwach) urządzeń różnych dostawców.  Co więcej, projektowany w § 3 ust. 1 pkt 2 wymóg odwołuje się do jednoczesnego zapewnienia interoperacyjności usług. Interoperacyjność usług jest terminem dotyczącym współpracy różnych sieci, czyli zapewnienia świadczenia jednorodnych usług pomiędzy sieciami, nie zaś wzajemnej współpracy różnych urządzeń spełniających te same funkcje w sieci jednego przedsiębiorcy. | Uwaga częściowo uwzględniona.  Zmieniono brzmienie przepisu, nie będzie się odnosić do „gwarantowania braku uzależnienia”.  Na konferencji:  UKE podtrzymało swoje uwagi z jednoczesnym skierowaniem zapytania do przedsiębiorców.  Przedstawiciele strony społecznej nie potwierdzili potrzeby zmiany w tym zakresie.  W dalszej części przedstawiciel UKE nie zgłosił dalszych zastrzeżeń. Uwagę uznano za uzgodnioną. |
|  | § 3 ust. 1 pkt. 3 | | UKE | | Ponadto należy podkreślić, że zawarty w projektowanym § 3 ust. 1 pkt 3 wymóg zapewnienia przez przedsiębiorcę telekomunikacyjnego dostarczającego sieć piątej generacji (5G) podwyższania odporności na zakłócenia sieci i usług telekomunikacyjnych nie posiada dodatkowej wartości normatywnej. Podwyższanie odporności na zakłócenia nie jest bowiem środkiem, lecz celem osiąganym na skutek zastosowania każdego z pozostałych środków lub metod, o których mowa w projektowanym § 2 pkt 3-5. Co więcej, cel ten dotyczy wszystkich przedsiębiorców telekomunikacyjnych, nie zaś wyłącznie przedsiębiorców telekomunikacyjnych dostarczających sieć piątej generacji (5G). Jednocześnie należy zaznaczyć, że projektowany § 3 ust. 1 pkt 3 stanowi de facto zmodyfikowany odpowiednik projektowanego § 2 pkt 5. | Uwaga nieuwzględniona.  Przepis wskazuje element, którym ma się kierować przedsiębiorca telekomunikacyjny podczas szacowania ryzyka.  Na konferencji:  UKE podtrzymało swoje uwagi z jednoczesnym skierowaniem zapytania do przedsiębiorców.  Przedstawiciele strony społecznej nie potwierdzili potrzeby zmiany w tym zakresie.  W dalszej części przedstawiciel UKE nie zgłosił dalszych zastrzeżeń. Uwagę uznano za uzgodnioną. |
|  | § 3 ust. 1 pkt. 2 | | Rada ds. Cyfryzacji  (uwaga zaktualizowana) | | Biorąc pod uwagę dotychczasowy przebieg konsultacji i bardzo zróżnicowane stanowiska strony społecznej, a szczególnie grupy operatorów telekomunikacyjnych i jednego z dostawców rozwiązań dla sieci 5G, **Rada stoi na stanowisku, że kluczowym elementem jest, aby finalna treść rozporządzenia była maksymalnie precyzyjna i nie pozostawiała zbyt wiele pola do interpretacji jego kluczowych zapisów.**  Elementem budzącym wątpliwości jest w chwili obecnej par. 3, ust. 1 pkt. 2 projektu Rozporządzenia, który brzmi:  "2) gwarantuje brak uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług"  W ocenie Rady zaproponowany zapis jest nadal nieprecyzyjny. "Uzależnienie" nie jest terminem biznesowym, prawniczym czy też technologicznym, a przede wszystkim jest to pojęcie niemierzalne. **Stąd Rada jest zwolennikiem użycia w przedmiotowym zapisie sformułowania o potrzebie nałożenia na Przedsiębiorcę telekomunikacyjnego obowiązku (zagwarantowania) „dywersyfikacji” producentów poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług.**  Ponadto można rozważyć pójście drogą Kolegów Brytyjczyków, którzy w odpowiednich swoich regulacjach określili maksymalny udział jednego dostawcy w sieci (nazwanego Dostawcą Wysokiego Ryzyka)  (<https://www.reuters.com/article/us-health-coronavirus-britain-huawei/uk-made-a-firm-decision-on-huawei-in-5g-foreign-ministrys-top-official-idUSKCN22327E>).  Uzasadnienie stanowiska  *Rząd w UK przeprowadził ocenę ryzyka dostawcy i zidentyfikował go jako DWR (dostawca wysokiego ryzyka). Ograniczenie udziału w rynku dotyczy, więc wyłącznie dostawcy wysokiego ryzyka, a nie dostawców ogólnie! Ograniczenia zastosowane w Wielkiej Brytanii są następujące:*  *dopuszczony jest tylko jeden dostawca wysokiego ryzyka DWR (dlatego ten drugi jest automatycznie wykluczony). DWR nie może dostarczać sieci core’owej, a w dostępie tylko tam, gdzie nie ma w pobliżu infrastruktury krytyczne.*  *K*westia ta jest bardzo precyzyjnie zapisana w europejskim „Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures”, który Polska, jako państwo członkowskie UE powinna uwzględniać tworząc przepisy wykonawcze oraz procedury weryfikacji sposobu wdrożenia 5G w kraju.  „5G Toolbox” zaleca (str. 18), aby wszystkie państwa członkowskie zapewniły stosowanie zabezpieczeń (w tym silną rolę regulatorów krajowych) właściwych i proporcjonalnych w odpowiedzi do obecnie zidentyfikowanych, jak i przyszłych ryzyk. W szczególności w zakresie:  I. wzmocnienia wymagań bezpieczeństwa dla operatorów (np. dokładnego/precyzyjnego zarządzania dostępem, zasad bezpiecznych działań operacyjnych i monitorowania, ograniczenia outsourcingu specyficznych funkcji, itp.)  II. oszacowania profilu ryzyka dla dostawców, a jako konsekwencja wdrożenia właściwych restrykcji dla dostawców wysokiego ryzyka włącznie z ich wykluczeniem dla złagodzenia ryzyka dla kluczowych aktywów (np. funkcje szkieletu sieci, zarządzanie siecią i funkcje orkiestracji oraz funkcje dostępu do sieci)  III. zapewnienie, że każdy operator posiada właściwą strategię wielu źródeł (ang. multivendor) w celu ograniczenia uzależnienia od pojedynczego dostawcy. | Uwaga częściowo uwzględniona.  Zmieniono brzmienie przepisu, nie będzie się odnosić do „gwarantowania braku uzależnienia”.  Pragnę ponadto wskazać, że proponowane w uwadze rozwiązania wymagają zmian ustawowych i wykraczają poza upoważnienie ustawowe niniejszego rozporządzenia.  Na konferencji:  Przedstawiciel Rady ds. Cyfryzacji przyjął wyjaśnienia MC. Uwaga została uznana za uzgodnioną. |