Prezes
Rady Ministrów

Donald Tusk

Warszawa, dnia /elektroniczny znacznik czasu/

RM-0610-59-24
UC37

Pan Szymon HOŁOWNIA
Marszałek Sejmu

Szanowny Panie Marszałku,

na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.
Ma on na celu wykonanie prawa Unii Europejskiej.
Do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Spraw Wewnętrznych i Administracji.

Z poważaniem
Donald Tusk
/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
wnioskodawca

tel. +48 (22) 694 75 00
dkpl@kprm.gov.pl
gov.pl/premier

Al. Ujazdowskie 1/3; 00-583
Warszawa

Projekt

U S T A W A

z dnia

o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[1)]

Art. 1. W ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2024 r. poz. 92 i 1248) wprowadza się następujące zmiany:

1) do tytułu ustawy dodaje się odnośnik w brzmieniu:

„[1)] Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79);”;

2) w art. 2 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8–10 w brzmieniu:

„8) dostawcy usług hostingowych – należy przez to rozumieć dostawcę usług polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek, o którym mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79), zwanego dalej „rozporządzeniem 2021/784”;

9) dostawcy treści – należy przez to rozumieć użytkownika, o którym mowa w art. 2 pkt 2 rozporządzenia 2021/784;

10) treściach o charakterze terrorystycznym – należy przez to rozumieć materiały, o których mowa w art. 2 pkt 7 rozporządzenia 2021/784.”;

3) po rozdziale 5 dodaje się rozdział 5a w brzmieniu:

[1)] Niniejsza ustawa:

1) służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79);

2) w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW (Dz. Urz. UE L 88 z 31.03.2017, str. 6).

„Rozdział 5a

Przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym

Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.

Art. 26b. 1. Szef ABW wyznacza w Agencji Bezpieczeństwa Wewnętrznego punkt kontaktowy, o którym mowa w art. 12 ust. 2 rozporządzenia 2021/784, działający w systemie całodobowym przez 7 dni w tygodniu.

2. Informacje o siedzibie i danych kontaktowych punktu, o którym mowa w ust. 1, oraz sposobie składania wniosków o wyjaśnienie i informacje zwrotne w sprawie nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści o charakterze terrorystycznym, zwanych dalej „nakazami usunięcia", udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej Agencji Bezpieczeństwa Wewnętrznego.

Art. 26c. 1. Szef ABW sprawuje nadzór nad wdrażaniem środków szczególnych, o których mowa w art. 5 ust. 1–3 rozporządzenia 2021/784, przez:

1) dokonywanie kontroli środków szczególnych, które podjął dostawca usług hostingowych, w tym pod kątem ich zgodności z art. 5 ust. 2 i 3 rozporządzenia 2021/784;
2) wydawanie dostawcy usług hostingowych pisemnych zaleceń, mających na celu usunięcie stwierdzonych nieprawidłowości i dostosowanie jego działalności do przepisów rozporządzenia 2021/784.

2. Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego, przeprowadzając czynności, o których mowa w ust. 1, ma prawo:

1) wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych;
2) żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia bądź wglądu w dokumentację techniczną i operacyjną wynikającą ze stosowania środków szczególnych.

3. Dostawca usług hostingowych narażony na treści o charakterze terrorystycznym usuwa naruszenia przepisów prawa i nieprawidłowości stwierdzone w ramach nadzoru sprawowanego przez Szefa ABW w terminie określonym w zaleceniu.

Art. 26d. 1. Nakaz usunięcia lub stwierdzenie naruszenia, o których mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej. Do postępowań w tych sprawach w zakresie nieuregulowanym w rozporządzeniu 2021/784 i niniejszej ustawie stosuje się przepisy art. 6, art. 7, art. 7b, art. 8, art. 12, art. 14, art. 16, art. 24, art. 26 § 1 i 2, art. 28–30, art. 32, art. 33, art. 35 § 1, art. 50, art. 54–56, art. 63–65, art. 72, art. 75 § 1, art. 77, art. 97 § 1 pkt 4 i § 2, art. 104, art. 105 § 1, art. 112, art. 113 § 1, art. 156–158, art. 217 oraz art. 268a ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572).

2. Wskazywanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, o których mowa w art. 5 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej. Do postępowań w tych sprawach stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, o których mowa w ust. 1, oraz art. 107 tej ustawy.

3. Decyzje, o których mowa w ust. 1 i 2, są ostateczne i podlegają natychmiastowemu wykonaniu.

4. Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał nakaz usunięcia, lub dostawcy treści, którego treści obejmuje nakaz usunięcia, przysługuje prawo do wniesienia na ten nakaz skargi do sądu administracyjnego w terminie 30 dni od dnia:

1) jego dostarczenia w trybie, o którym mowa w art. 3 ust. 5 rozporządzenia 2021/784 – w przypadku dostawcy usług hostingowych;
2) otrzymania informacji, o której mowa w art. 11 ust. 1 rozporządzenia 2021/784 – w przypadku dostawcy treści.

5. Dostawcy usług hostingowych lub dostawcy treści, w stosunku do którego Szef ABW wydał decyzję, o której mowa w art. 4 ust. 4 rozporządzenia 2021/784, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego w terminie 30 dni od dnia otrzymania powiadomienia o tej decyzji.

6. Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał decyzję, o której mowa w art. 5 ust. 4, 6 lub 7 rozporządzenia 2021/784, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego.

7. Skargi, o których mowa w ust. 4 –6, mogą być rozpoznawane w trybie uproszczonym, o którym mowa w art. 120 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2024 r. poz. 935), o ile strona

nie zawnioskuje o przeprowadzenie rozprawy, a sąd uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione i przeprowadzenie rozprawy jest zbędne. Przepis art. 122 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi stosuje się.

Art. 26e. Dostawca usług hostingowych, w stosunku do którego został wydany nakaz usunięcia, w terminie do dnia 1 marca każdego roku przekazuje Szefowi ABW dane, o których mowa w art. 21 ust. 1 lit. b i d rozporządzenia 2021/784, za rok poprzedni.

Art. 26f. 1. Dostawca usług hostingowych, który nie dopełnia obowiązku, o którym mowa w art. 3 ust. 3 lub 6, art. 4 ust. 2 lub 7, art. 5 ust. 1–3, 5 lub 6, art. 6, art. 7, art. 10, art. 11, art. 14 ust. 5, art. 15 ust. 1 lub art. 17 rozporządzenia 2021/784, podlega karze pieniężnej.

2. Karę pieniężną, o której mowa w ust. 1, nakłada Szef ABW, w drodze decyzji administracyjnej, biorąc pod uwagę warunki i okoliczności określone w art. 18 rozporządzenia 2021/784 w wysokości do 4% całkowitych obrotów uzyskanych przez dostawcę usług hostingowych w poprzednim roku obrotowym.

3. Decyzje, o których mowa w ust. 2, są ostateczne.

4. Środki z kar pieniężnych, o których mowa w ust. 1, stanowią dochód budżetu państwa.

Art. 26g. 1. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej dostawca usług hostingowych jest obowiązany do dostarczenia Szefowi ABW, na każde jego żądanie, w terminie 30 dni od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej.

2. W przypadku niedostarczenia przez dostawcę usług hostingowych danych lub gdy dostarczone przez tego dostawcę dane uniemożliwiają ustalenie podstawy wymiaru kary pieniężnej, Szef ABW ustala podstawę wymiaru tej kary w sposób szacunkowy, uwzględniając ogólnie dostępne dane finansowe dotyczące tego dostawcy, w tym kryteria, o których mowa w art. 7 ust. 1 pkt 1–3 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236 i 1222).

Art. 26h. Karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja Szefa ABW, o której mowa w art. 26f ust. 2, stała się prawomocna.”.

Art. 2. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812 i 1222) art. 32c otrzymuje brzmienie:

„Art. 32c. 1. W celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa oraz ścigania ich sprawców sąd, na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, w drodze postanowienia, może zarządzić:

1) usunięcie lub zablokowanie dostępności w systemie teleinformatycznym przez usługodawcę świadczącego usługi drogą elektroniczną,
2) zablokowanie dostępności w systemie teleinformatycznym przez przedsiębiorcę telekomunikacyjnego

– określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa, lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa, zwane dalej odpowiednio „usunięciem” lub „blokadą dostępności”.

2. Wniosek, o którym mowa w ust. 1, może obejmować blokadę dostępności określonych danych informatycznych, jeżeli ich usunięcie jest lub może okazać się niewykonalne.

3. Wniosek, o którym mowa w ust. 1, przedstawia się wraz z materiałami uzasadniającymi potrzebę usunięcia lub blokady dostępności.

4. Przepisu ust. 1 nie stosuje się do dostawców usług hostingowych i treści o charakterze terrorystycznym, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79).

5. Postanowienie, o którym mowa w ust. 1, wydaje Sąd Okręgowy w Warszawie.

6. W przypadkach niecierpiących zwłoki, w celu zapobieżenia zdarzeniu o charakterze terrorystycznym lub uprawdopodobniającemu popełnienie przestępstwa szpiegostwa, Szef ABW, po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, może zarządzić blokadę dostępności, zwracając się

jednocześnie do sądu, o którym mowa w ust. 5, z wnioskiem o wydanie postanowienia w tej sprawie.

7. Usługodawca świadczący usługi drogą elektroniczną lub przedsiębiorca telekomunikacyjny jest obowiązany do natychmiastowego dokonania czynności określonych w postanowieniu sądu lub przekazanym mu zarządzeniu Szefa ABW.

8. Wniosek Szefa ABW, o którym mowa w ust. 1, zawiera w szczególności:

1) numer sprawy i jej kryptonim, jeżeli został jej nadany;
2) opis zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej;
3) okoliczności uzasadniające potrzebę usunięcia lub blokady dostępności;
4) szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać usunięciu lub blokadzie dostępności;
5) dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowane będzie usunięcie lub blokada dostępności, ze wskazaniem sposobu stosowania tego usunięcia lub blokady dostępności;
6) cel usunięcia lub blokady dostępności;
7) czas prowadzonej blokady dostępności.

9. Blokadę dostępności zarządza się na okres nie dłuższy niż 30 dni. Sąd, o którym mowa w ust. 5, może, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, wydać postanowienie o jednorazowym przedłużeniu blokady dostępności na okres nie dłuższy niż 3 miesiące, jeżeli nie ustały przyczyny jej zarządzenia.

10. Do wniosku, o którym mowa w ust. 6 i 9, stosuje się odpowiednio przepisy ust. 3 i 8. Sąd przed wydaniem postanowienia, o którym mowa w ust. 1, 6 i 9, zapoznaje się z materiałami uzasadniającymi wniosek.

11. Wnioski, o których mowa w ust. 1, 6 i 9, sąd rozpoznaje jednoosobowo, przy czym czynności sądu związane z rozpoznawaniem tych wniosków są realizowane w warunkach przewidzianych dla przekazywania, przechowywania i udostępniania informacji niejawnych oraz z odpowiednim zastosowaniem przepisów wydanych na podstawie art. 181 § 2 Kodeksu postępowania karnego. W posiedzeniu sądu może wziąć udział wyłącznie prokurator i Szef ABW.

12. Na postanowienia sądu, o których mowa w ust. 1, 6 i 9, przysługuje zażalenie Szefowi ABW, Pierwszemu Zastępcy Prokuratora Generalnego Prokuratorowi Krajowemu, usługodawcy świadczącemu usługi drogą elektroniczną lub przedsiębiorcy telekomunikacyjnemu. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

13. Blokady dostępności zaprzestaje się w przypadku:

1) nieudzielenia przez sąd, w terminie 5 dni od złożenia wniosku w trybie ust. 6, zgody na zarządzenie przez Szefa ABW blokady dostępności;
2) nieudzielenia przez sąd zgody na przedłużenie blokady dostępności w trybie ust. 9;
3) upływu okresu, na który blokada dostępności została wprowadzona.

14. Sąd, Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy oraz Szef ABW prowadzą w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych, rejestry postanowień, pisemnych zgód, zarządzeń i wniosków dotyczących usunięcia lub blokady dostępności.

15. O zastosowaniu usunięcia lub blokady dostępności Szef ABW powiadamia ministra właściwego do spraw informatyzacji, jeżeli usługodawca świadczący usługi drogą elektroniczną lub przedsiębiorca telekomunikacyjny ma siedzibę na terytorium Rzeczypospolitej Polskiej.

16. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób dokumentowania usunięcia lub blokady dostępności oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków, a także wzory stosowanych druków i rejestrów, uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów.”.

Art. 3. Do blokad dostępności, o których mowa w art. 32c ust. 1 ustawy zmienianej w art. 2, zarządzonych i niezakończonych przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.

Art. 4. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 32c ust. 14 ustawy zmienianej w art. 2 zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 32c ust. 16 ustawy zmienianej w art. 2, w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 5. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

UZASADNIENIE

W związku z wejściem w życie z dniem 7 czerwca 2021 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79), zwanego dalej „rozporządzeniem 2021/784", zaistniała potrzeba zainicjowania prac legislacyjnych mających na celu dostosowanie polskiego porządku prawnego do uregulowań unijnych. Państwa członkowskie, w tym Polska, są zobowiązane do odpowiedniego dostosowania swoich regulacji i stosowania rozporządzenia 2021/784, począwszy od dnia 7 czerwca 2022 r. Projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu wprowadza do polskiego porządku prawnego stosowne przepisy, które to umożliwią.

Głównym motywem wydania rozporządzenia 2021/784 było zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego przez przeciwdziałanie wykorzystywaniu usług hostingowych do celów terrorystycznych oraz przyczynianie się do poprawy bezpieczeństwa publicznego w całej Unii Europejskiej, przy jednoczesnym zagwarantowaniu pełnego poszanowania praw podstawowych, takich jak wolność wypowiedzi i informacji. Nowe uregulowania – co do zasady – ustanawiają we wszystkich państwach członkowskich UE spójny mechanizm umożliwiający skuteczne i legalne usuwanie z sieci oraz blokowanie wszelkich treści o charakterze terrorystycznym zamieszczanych z wykorzystywaniem usług hostingowych. Mając na uwadze transgraniczny charakter problemu oraz fakt, że treści o charakterze terrorystycznym są często publicznie rozpowszechniane za pośrednictwem usług świadczonych przez zagranicznych dostawców usług hostingowych, mechanizm ten ma zastosowanie wobec wszystkich dostawców, niezależnie od miejsca ustanowienia ich głównej jednostki organizacyjnej, jeżeli swoje usługi oferują w co najmniej jednym państwie członkowskim UE. W tym zakresie obowiązuje zasada równego traktowania, a działania podejmowane w celu stosowania przyjętych rozwiązań muszą być skuteczne, odpowiednie i proporcjonalne. Środki służące przeciwdziałaniu rozpowszechniania w internecie treści o charakterze terrorystycznym, w rozumieniu projektowanej regulacji, w przypadku gdy pozostają skuteczne i proporcjonalne, nie są sprzeczne z ochroną wolności wypowiedzi i informacji, lecz ochronę tę wzmacniają, przede wszystkim zapewniając bezpieczeństwo mediów cyfrowych przed działaniami grup terrorystycznych i ich zwolennikami.

Komisja Europejska, powołując się na dane Europolu, wskazuje na rosnące zainteresowanie wykorzystaniem internetu przez terrorystów, m.in. do szerzenia swoich

przesłań w celu zastraszania, radykalizacji, rekrutacji oraz ułatwiania przeprowadzania ataków terrorystycznych. W ocenie Komisji Europejskiej jest to szczególnie niebezpieczne w aktualnej sytuacji geopolitycznej w kontekście panujących konfliktów i niestabilności, które mają bezpośredni wpływ na bezpieczeństwo Europy. Jak wskazuje Komisja Europejska, cyt. „Rosyjska wojna napastnicza przeciwko Ukrainie i atak terrorystyczny przeprowadzony przez Hamas na Izrael 7 października 2023 r. doprowadziły do zwiększenia skali rozpowszechniania w internecie treści o charakterze terrorystycznym.”[1)].

W świetle rozporządzenia 2021/784 za treści o charakterze terrorystycznym należy uznać materiały, które:

- podżegają do popełnienia przestępstwa terrorystycznego (w rozumieniu dyrektywy 2017/541 z dnia 15 marca 2017 r.[2)]), w przypadku gdy takie materiały bezpośrednio lub pośrednio (np. przez pochwalanie aktów terrorystycznych) popierają popełnianie przestępstwa terrorystycznego, a tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw,
- nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia przestępstwa terrorystycznego,
- nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej,
- udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia przestępstwa terrorystycznego;
- stwarzają zagrożenie popełnienia przestępstwa terrorystycznego.

Treściami o charakterze terrorystycznym w rozumieniu rozporządzenia 2021/784 nie są natomiast materiały rozpowszechniane w celach: edukacyjnych, dziennikarskich, artystycznych, badawczych czy zwiększania świadomości na temat przeciwdziałania działalności terrorystycznej. Treściami o charakterze terrorystycznym nie powinny być również wyrażane w ramach debaty publicznej radykalne, polemiczne lub kontrowersyjne poglądy na drażliwe kwestie polityczne. Przepisy rozporządzenia 2021/784 nie będą miały także

[1)] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym z 14.02.2024 r. (COM(2024) 64 final), str. 1.

[2)] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/WSiSW (Dz. Urz. UE L 88 z 31.03.2017, str. 6).

zastosowania wobec usług poczty elektronicznej lub przesyłanych wiadomości prywatnych, a także do infrastruktury w chmurze, pod warunkiem że usługi te są świadczone na wniosek stron innych niż dostawcy treści i przynoszą korzyści dostawcom treści jedynie pośrednio. Natomiast rozporządzenie 2021/784 stosuje się do dostawców usług w zakresie mediów społecznościowych, usług wymiany materiałów video, obrazów i plików audio, a także usług wymiany plików i innych usług w chmurze, jeżeli usługi te są wykorzystywane do publicznego udostępnienia przechowywanych informacji na bezpośredni wniosek dostawcy treści.

W rezultacie państwa członkowskie zostały zobowiązane do wskazania w swoich porządkach prawnych takich organów, które bez względu na skalę zjawiska w danym państwie będą w stanie sprawnie i skutecznie zapewnić ochronę przed internetową propagandą terrorystyczną, mając przy tym do dyspozycji niezbędne do tego narzędzia zarówno na poziomie operacyjnym, jak i prawno-administracyjnym.

Zgodnie z internetowym rejestrem zawierającym wykaz takich organów obowiązek ten wypełniły 24 państwa, które tym samym zapewniły możliwość stosowania rozporządzenia[3)]. Z opublikowanego w 2024 r. przez Komisję Europejską raportu wynika, że do 31 grudnia 2023 r. Komisja Europejska otrzymała informację o co najmniej 349 nakazach usunięcia wysłanych przez właściwe organy Hiszpanii, Rumunii, Francji, Niemiec, Austrii i Czech m.in. do następujących podmiotów: Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net oraz Catbox. Przy czym hiszpański organ właściwy wysłał 62 nakazy, francuski 26 nakazów, natomiast tylko od czasu ataku terrorystycznego przeprowadzonego przez Hamas na Izrael w październiku 2023 r. do końca 2023 r. niemiecki organ takich nakazów wysłał blisko 250[4)].

Jednocześnie tylko w dziesięciu przypadkach dostawca usług hostingowych nie usunął treści o charakterze terrorystycznym lub nie zablokował dostępu do nich w czasie do jednej godziny, do czego zobowiązuje rozporządzenie 2021/784. W efekcie dzięki wdrożonym mechanizmom bardzo wzrosła szybkość reagowania na zgłoszenia dotyczące takich treści. W dziewięciu przypadkach EUROPOL otrzymał od dostawców usług hostingowych

[3)] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en (dostęp: 07.03.2024 r.)

[4)] „Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 (…) str. 6.

informacje na temat treści o charakterze terrorystycznym, które wiązały się z bezpośrednim zagrożeniem życia, zgodnie z art. 14 ust. 5 rozporządzenia[5)].

Tematyka rozporządzenia 2021/784 obecnie jest częściowo objęta regulacją krajową, która nie w pełni wdraża obowiązującą w tym zakresie dyrektywę Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW, zwaną dalej „dyrektywą 2017/541".

W świetle ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu , zwanej dalej „ustawą o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu", Szef Agencji Bezpieczeństwa Wewnętrznego, za zgodą sądu, może spowodować tzw. „blokadę dostępności" w internecie określonych danych powiązanych ze zdarzeniem o charakterze terrorystycznym. Zgodnie z art. 32c ww. ustawy, sąd, na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, w drodze postanowienia, może zarządzić zablokowanie dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa. Zaś w przypadkach niecierpiących zwłoki do zarządzenia takiej blokady uprawniony jest Szef ABW, po uzyskaniu pisemnej zgody od Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego. Jednocześnie w takiej sytuacji Szef ABW jest zobowiązany zwrócić się do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wydanie postanowienia w przedmiotowej sprawie. W przypadku gdy sąd w terminie 5 dni nie udzieli zgody na zarządzenie blokady, jest ona znoszona. W pozostałych przypadkach blokada dostępności danych teleinformatycznych jest zarządzana na okres nie dłuższy niż 30 dni z możliwością jej sądowego przedłużenia na okres nie dłuższy niż 3 miesiące.

Z kolei zgodnie z art. 21 dyrektywy 2017/541 państwa członkowskie są zobowiązane do wprowadzenia środków, które w pierwszej kolejności zapewnią natychmiastowe usunięcie treści internetowych nawołujących do popełnienia przestępstwa terrorystycznego. Natomiast jeżeli usunięcie takich treści nie jest możliwe, państwa członkowskie mogą podjąć środki w celu zablokowania dostępu do nich. Polskie ustawodawstwo zaś przewiduje jedynie możliwość zablokowania odpowiednich treści, co w ocenie Komisji Europejskiej nie jest wystarczające,

[5)] Str. 14 Sprawozdania, o którym mowa w odnośniku nr 4.

aby uznać transpozycję przepisów dyrektywy 2017/541 w tym zakresie za prawidłową. Brak jest bowiem podstawowego mechanizmu, który pozwalałby w pierwszej kolejności na usuwanie tych treści ze stron internetowych.

Projektując obowiązujące w tym zakresie rozwiązania krajowe, przyjęte ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych , zwaną dalej „ustawą o działaniach antyterrorystycznych", wzorowano się na wówczas już funkcjonujących przepisach dotyczących zarządzania kontroli operacyjnej w poszczególnych służbach. Ogólnie wynika z nich, że blokada treści o charakterze terrorystycznym w internecie wymaga – co do zasady – uprzedniej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego i sądu.

Z kolei mechanizm ustanowiony w rozporządzeniu 2021/784 jest znacznie szybszy i uproszczony. Unijne regulacje nie zakładają konieczności uzyskania sądowej zgody do jego zastosowania. Natomiast zapewniają wdrożenie procedury skargowej, do której będzie miała prawo każda ze stron, której wydany nakaz dotyczy, tj. zarówno dostawcy usług hostingowych, jak i dostawcy treści, które zostały usunięte.

W związku z tym jest konieczne dokonanie stosownej nowelizacji ustawy o działaniach antyterrorystycznych, która spowoduje, że również Polska znajdzie się w grupie państw członkowskich, które dysponują zwiększonym potencjałem zarówno w sferze prawnej, jak i funkcjonalnej w walce przeciwko wykorzystywaniu internetu do działań terrorystycznych. Obecnie, jak przedstawiono powyżej, aktualny stan prawny nie tylko nie przewiduje możliwości usuwania przez służby niebezpiecznych treści terrorystycznych ze stron internetowych, ale – co za tym idzie – nie pozwala na korzystanie z ustanowionych w tym celu narzędzi rynku cyfrowego. Należy wskazać, że od 3 lipca 2023 r. funkcjonuje opracowana przez EUROPOL platforma o nazwie „PERCI", która centralizuje, koordynuje i ułatwia przekazywanie nakazów usunięcia i zgłoszeń do dostawców usług hostingowych. Jest to rozwiązanie oparte na chmurze zapewniające bezpieczeństwo i ochronę danych zamieszczanych w chmurze. Obecnie oprócz roli, jaką pełni w odniesieniu do zgłoszeń, PERCI ułatwia przekazywanie nakazów usunięcia, sprawozdawczość państw członkowskich i koordynację, a także usuwanie konfliktów, w sytuacji gdy toczy się postępowanie przygotowawcze w sprawie treści, wobec których ma zostać wysłany nakaz usunięcia. Równocześnie trwają dalsze prace w kierunku wykorzystania tego systemu do realizacji kolejnych zadań wynikających z rozporządzenia 2021/784, np. weryfikacji transgranicznych nakazów usunięcia.

Mając powyższe na uwadze, niniejszym projektem proponuje się wprowadzenie zmian do ustawy o działaniach antyterrorystycznych przez dodanie do słownika ustawy definicji pojęć: „dostawcy usług hostingowych", „dostawcy treści" oraz „treści o charakterze terrorystycznym" przez odesłanie do odpowiednich definicji zawartych w rozporządzeniu 2021/784 (art. 1 pkt 1 projektu). W obecnym brzmieniu ustawy o działaniach antyterrorystycznych pojęcia te nie występują, w związku z tym ich wprowadzenie na grunt ustawowy wymaga odesłania w tym zakresie do przepisów prawa unijnego. Jest to niezbędne celem zapewnienia prawidłowego stosowania i jednolitego interpretowania projektowanych przepisów dotyczących przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym.

W rezultacie zgodnie z niniejszym projektem „treści o charakterze terrorystycznym" to materiały, które:

a) podżegają do popełnienia przestępstwa o charakterze terrorystycznym określonego w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (zgodnie z którym przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu), w przypadku gdy takie materiały bezpośrednio lub pośrednio (np. przez pochwalanie aktów terrorystycznych) popierają popełnianie przestępstwa o charakterze terrorystycznym i tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw,
b) nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia przestępstwa o charakterze terrorystycznym,
c) nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej,
d) udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia przestępstwa o charakterze terrorystycznym,

e) stwarzają zagrożenie popełnienia przestępstwa o charakterze terrorystycznym.

Z kolei za „dostawcę usług hostingowych" należy uznać dostawcę usług normalnie świadczonych za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług, polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek. Natomiast „dostawcą treści" jest użytkownik, który dostarczył informacje, które są lub były przechowywane i publicznie rozpowszechniane przez dostawcę usług hostingowych.

Równocześnie proponuje się dodanie do ustawy o działaniach antyterrorystycznych rozdziału 5a „Przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym", który umożliwi stosowanie unijnych rozwiązań, jednocześnie będąc komplementarnym z rozwiązaniami przyjmowanymi w tym zakresie przez pozostałe państwa członkowskie UE.

Celem dodania **art. 26a** ustawy jest ustanowienie na gruncie ustawowym Szefa ABW jako organu właściwego w rozumieniu rozporządzenia 2021/784. W rezultacie Szef ABW będzie odpowiedzialny m.in. za:

a) wydawanie nakazów zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich, zgodnie z art. 3 rozporządzenia 2021/784,
b) weryfikowanie nakazów usunięcia wydanych przez właściwe organy innych państw członkowskich oraz stwierdzania ewentualnych naruszeń w tym zakresie, zgodnie z art. 4 rozporządzenia 2021/784,
c) przedłużanie okresu zachowania treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony, na skutek wydanego nakazu usunięcia (art. 6 ust. 2 rozporządzenia 2021/784),
d) wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym oraz nadzoru nad wdrażaniem przez nich środków szczególnych, na podstawie art. 5 rozporządzenia 2021/784,
e) prowadzenie współpracy, w tym wymiany informacji, z innymi właściwymi organami ustanowionymi przez pozostałe państwa członkowskie, Europolem oraz dostawcami usług hostingowych, zgodnie z art. 14 rozporządzenia 2021/784,
f) nakładanie kar administracyjnych, na podstawie art. 18 rozporządzenia 2021/784,
g) publikację sprawozdania, na podstawie art. 8 rozporządzenia 2021/784,

h) przekazywanie do Komisji Europejskiej rocznej informacji, na podstawie art. 21 rozporządzenia 2021/784.

Nakazy usunięcia Szef ABW będzie mógł wydawać wszystkim dostawcom usług hostingowych obowiązanym do przestrzegania przepisów rozporządzenia 2021/784. Natomiast w pozostałym zakresie działania Szefa ABW wynikające ze stosowania rozporządzenia 2021/784 będą ograniczone wyłącznie do dostawców usług hostingowych, którzy mają główną jednostkę organizacyjną w Polsce lub których przedstawiciel prawny ma miejsce pobytu lub siedzibę w Polsce, i tylko w zakresie, o jakim mowa w rozporządzeniu 2021/784.

Mając na uwadze, że przepisy rozporządzenia stosuje się wprost, swoje zadania Szef ABW będzie realizował na zasadach określonych w art. 13 ust. 2 rozporządzenia 2021/784, a zatem w sposób obiektywny i niedyskryminacyjny, z pełnym poszanowaniem praw podstawowych. W kontekście wykonywania zadań, o których mowa w art. 12 ust. 1, nie będzie mógł też zwracać się o instrukcje do żadnego innego organu ani przyjmować takich instrukcji, co jednak nie wyklucza działań podejmowanych w ramach sprawowania nad nim konstytucyjnego nadzoru. Pozycja prawno-ustrojowa Szefa ABW, wynikająca przede wszystkim z ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zapewnia stosowanie przepisów unijnych w tym zakresie. Zgodnie z ww. ustawą Szef ABW jest centralnym organem administracji rządowej, podlegającym bezpośrednio Prezesowi Rady Ministrów oraz podlegającym kontroli Sejmu RP. Celem ustawowym samej Agencji jest z kolei ochrona bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

Zgodnie z projektowanym **art. 26b** Szef ABW wyznacza w ramach podległej mu służby punkt kontaktowy właściwy do rozpatrywania wniosków o wyjaśnienie i informacje zwrotne dotyczące nakazów wydanych przez ABW, który będzie funkcjonował całodobowo 7 dni w tygodniu. Dane dotyczące tego punktu, w tym dane kontaktowe oraz sposób składania ww. wniosków, będą publicznie dostępne za pośrednictwem Biuletynu Informacji Publicznej na stronie podmiotowej ABW, a także przekazane do wiadomości Komisji Europejskiej. W ten sposób zostanie wypełniony obowiązek, który unijny prawodawca nakłada na państwa członkowskie w art. 12 ust. 2 rozporządzenia 2021/784 w zakresie wyznaczenie punktu kontaktowego do spraw nakazów usunięcia wydanych w danym państwie.

W myśl **art. 26c** ustawy nadzór Szefa ABW nad dostawcami usług hostingowych w zakresie wdrażania przez nich środków szczególnych będzie polegał na dokonywaniu przez Szefa ABW kontroli środków szczególnych, które dostawca usług hostingowych zdecydował się zastosować, a także na wydawaniu zaleceń w przypadku stwierdzenia nieprawidłowości

w tym zakresie. W celu zapewnienia wykonania tych czynności upoważniony funkcjonariusz ABW będzie miał prawo wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych oraz prawo żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia bądź wglądu w dokumentację techniczną i operacyjną wynikającą ze stosowania środków szczególnych. W myśl projektowanych przepisów dostawca usług hostingowych będzie zobowiązany do terminowego usunięcia stwierdzonych nieprawidłowości. Podkreślenia wymaga, że do kontroli, w zakresie nieuregulowanym niniejszą ustawą, będą miały zastosowanie przepisy ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców , w tym art. 48, art. 49 ust. 1–3 i 6–9, a także art. 51–57.

Ponadto wskazać należy, że o ile decyzje Szefa ABW uznające dostawców usług hostingowych za narażonych na treści o charakterze terrorystycznym będą miały charakter natychmiastowej wykonalności, o tyle nie będzie to miało przełożenia na obowiązek natychmiastowego wdrożenia środków szczególnych przez tych dostawców. Zgodnie bowiem z art. 5 ust. 5 rozporządzenia 2021/784 dostawca usług hostingowych narażony na treści o charakterze terrorystycznym powiadamia właściwy organ (Szefa ABW) o środkach, które podjął lub zamierza podjąć w terminie do 3 miesięcy od otrzymania decyzji w tej sprawie. Z kolei w świetle art. 5 ust. 6 rozporządzenia 2021/784 działania kontrolne, o których mowa powyżej, Szef ABW będzie – co do zasady – podejmował nie wcześniej niż po otrzymaniu od dostawcy usług hostingowych tego powiadomienia, a zatem po upływie okresu do 3 miesięcy od wydania decyzji lub też bezpośrednio na wniosek samego dostawcy usług hostingowych.

Powyższe przepisy mają na celu zapewnienie stosowania art. 12 rozporządzenia 2021/784, które nakłada na państwa członkowskie obowiązek wyznaczenia organu właściwego w zakresie wydawania nakazów usunięcia i ich weryfikowaniu, nadzoru nad dostawcami usług hostingowych w zakresie wdrażania środków szczególnych, a także nakładania kar za naruszenia przedmiotowego rozporządzenia.

W świetle proponowanego brzmienia **art. 26d** ustawy do nakazów usunięcia oraz stwierdzania naruszeń, o których mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, zastosowanie będzie miała ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego we wskazanym w tym przepisie zakresie. Częściowe zastosowanie uregulowań Kodeksu postępowania administracyjnego w tym przypadku jest niezbędne. Stanowi o tym fakt, że tryb postępowania opisany w rozporządzeniu 2021/784 odnośnie do wydawania nakazów usunięcia ma zapewnić na poziomie unijnym (a zatem w wymiarze transgranicznym) spójny i efektywny mechanizm usuwania lub blokowania w sieci wszelkich

treści o charakterze terrorystycznym. Skuteczność tego mechanizmu jest natomiast mierzona szybkością reakcji i wykonania stosownych czynności. W rezultacie przyjęty w unijnym akcie sposób postępowania zarówno w odniesieniu do wydawania nakazów usunięcia, jak i stwierdzenia naruszeń, o których mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, znacząco odbiega od niektórych rozwiązań przyjętych na gruncie krajowych przepisów prawa administracyjnego. Ponadto większość elementów w rozumieniu postępowania administracyjnego zostało wprost określonych w samym rozporządzeniu, np. elementy decyzji, moment i skutek jej doręczenia, a zatem w takim przypadku jest niezbędne wyłączenie uregulowań krajowych.

Wymieniony w projektowanym art. 26d ust. 1 katalog przepisów Kodeksu postępowania administracyjnego jest po części wzorowany na funkcjonujących już w analogicznych przypadkach przepisach (np. w art. 4 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego), a po części stanowi niezbędne uzupełnienie i dostosowanie mechanizmu postępowania wynikającego wprost z przepisów rozporządzenia 2012/784. W rezultacie wskazane w niniejszym przepisie art. 50 oraz art. 54–56 k.p.a., dotyczące procedury wezwania, jak również art. 63–65 k.p.a., określające procedurę wnoszenia podania (żądania, wyjaśnienia, odwołania, zażalenia), będą mogły mieć *de facto* zastosowanie wyłącznie w odniesieniu do postępowań w sprawach stwierdzania naruszeń, o których mowa w art. 4 ust. 3 i 4. rozporządzenia 2021/784. Analogicznie do przypadku nakazów usunięcia oraz stwierdzania naruszeń, wskazanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, zgodnie z art. 5 rozporządzenia 2021/784, będzie następowało w formie decyzji. Do tych decyzji również będzie miał zastosowanie Kodeks postępowania administracyjnego tylko w zakresie wskazanym niniejszym projektem. Jednocześnie przewiduje się, że we wszystkich tych przypadkach postępowania będą jednoinstancyjne, a wydane decyzje będą podlegały natychmiastowej wykonalności. Tryb jednoinstancyjny jest w tym przypadku niezbędny w celu zapewnienia sprawności i efektywności prowadzenia takich postępowań. Takie rozwiązanie pozostaje zgodne z Konstytucją RP, która w art. 78 przewiduje możliwość ustawowego odstępstwa od zaskarżenia orzeczeń i decyzji wydanych w pierwszej instancji. Zgodnie z ustawą zasadniczą tego rodzaju ograniczenia mogą być ustanawiane wyłącznie ustawą i gdy jest to konieczne m.in. z uwagi na kwestie bezpieczeństwa i porządku publicznego. Kontekst i *ratio legis* projektu wpisują się zatem w te przesłanki. Natomiast mając na uwadze, że dostawcy usług hostingowych i dostawcy treści będzie każdorazowo

przysługiwało prawo wniesienia skargi do sądu, istota wolności i praw pozostanie w tym przypadku zachowana.

Prawo do zaskarżenia będzie przysługiwało dostawcom usług hostingowych również w odniesieniu do decyzji Szefa ABW wydanych na podstawie art. 5 ust. 6 lub 7 rozporządzenia 2021/784 . Wskazać należy, że projektowany art. 26d w tym zakresie stanowi wypełnienie art. 9 rozporządzenia 2021/784, który m.in. przewiduje prawo do zaskarżania wydanych nakazów usunięcia oraz pozostałych decyzji wydanych przez organ właściwy.

W przypadku gdy strona nie zawnioskuje o przeprowadzenie rozprawy, sąd – jeżeli uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione – będzie mógł zdecydować o jej rozpoznaniu w trybie uproszczonym. Nie wyklucza to jednak sytuacji, że rozpoznając sprawę w trybie uproszczonym, sąd ostatecznie zdecyduje o jej rozpoznaniu na rozprawie. Tryb uproszczony będzie mógł mieć zatem zastosowanie jedynie fakultatywnie po spełnieniu łącznie obu przesłanek i ma – co do zasady – zapewnić, że rozpatrywanie środków prawnych od nakazów usunięcia oraz od decyzji o wskazaniu dostawcy usług hostingowych narażonych na treści o charakterze terrorystycznym będzie realizowane w sposób sprawny i efektywny, ale z zachowaniem wszelkich gwarancji prawa do sądu.

W postępowaniach, o których mowa powyżej, właściwy pozostaje sąd administracyjny, co wynika z faktu, że postępowania te będą dotyczyły wyłącznie kwestii prawno-administracyjnych. Należy zauważyć, że określone rozporządzeniem 2021/784 sankcje odnoszą się do sytuacji niespełnienia określonych obowiązków o charakterze administracyjnym przez dostawcę usług hostingowych, nie zaś dopuszczenia się przez nich czynów karalnych na gruncie przepisów prawa karnego materialnego. Samo usuwanie treści nie jest środkiem sankcyjnym, lecz środkiem ograniczającym. W związku z tym projektodawca przewiduje, że w tym zakresie jedynie sądy administracyjne będą kompetentnymi jednostkami sądownictwa do rozpatrywania skarg na decyzje Szefa ABW.

Mając na uwadze potrzebę zapewnienia wykonania art. 21 ust. 1 rozporządzenia 2021/784, który zobowiązuje państwa członkowskie do gromadzenia i przekazywania do Komisji Europejskiej informacji m.in. w zakresie podjętych środków szczególnych, liczby wszczętych procedur rozpatrywania skarg oraz innych działań podjętych przez dostawcę usług hostingowych w ramach ustanowionego mechanizmu skargowego, dostawcy usług hostingowych – na podstawie **art. 26e** ustawy – będą zobowiązani do cyklicznego przekazywania do Szefa ABW informacji, o których mowa w art. 21 ust. 1 lit. b i d

rozporządzenia 2021/784. Dane te następnie będą zbiorczo przesyłane do wiadomości Komisji Europejskiej.

Projektowane art. 26f–26h stanowią natomiast konsekwencję przepisów unijnych, które w art. 18 rozporządzenia 2021/784 zobowiązują państwa członkowskie do ustanowienia środków karnych mających zastosowanie w przypadku naruszeń tego rozporządzenia. Należy zauważyć, że przepisy unijne szczegółowo wskazują zarówno rodzaj naruszeń podlegających karze (art. 18 ust. 1), jak i okoliczności, które należy uwzględnić przy określeniu wysokości tej kary (art. 18 ust. 2 i 3).

W związku z powyższym proponuje się w **art. 26f ust. 1** bezpośrednie odesłanie do określonego w art. 18 ust. 1 rozporządzenia 2021/784 katalogu przypadków naruszeń, które będą sankcjonowane odpowiednimi karami. Z kolei w projektowanym art. 26f ust. 2 proponuje się przyznanie Szefowi ABW uprawnienia do nakładania na dostawców usług hostingowych, w drodze decyzji administracyjnej, kar pieniężnych za popełnienie tych naruszeń. Przy nakładaniu kar będą brane pod uwagę warunki i okoliczności określone w art. 18 rozporządzenia 2021/784 w wysokości do 4% całkowitych obrotów uzyskanych przez tego dostawcę w poprzednim roku obrotowym. W takiej wysokości kara będzie mogła zostać nałożona jednak wyłącznie w przypadku, gdy dostawca systematycznie lub uporczywie nie będzie wypełniał obowiązków w zakresie usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich.

Zgodnie bowiem z unijnymi regulacjami wysokość kar pieniężnych powinna być skuteczna, proporcjonalna i odstraszająca w zależności od zaistniałych okoliczności analizowanych w każdym przypadku indywidualnie. Mając na uwadze powyższe, organ właściwy, ustalając wysokość kary, będzie musiał wziąć pod uwagę szereg istotnych okoliczności, w tym te określone w art. 18 ust. 2 rozporządzenia 2021/784, tj.:

a) charakter, wagę i czas trwania naruszenia,
b) umyślny lub wynikający z zaniedbania charakter naruszenia,
c) wcześniejsze naruszenia popełnione przez dostawcę usług hostingowych,
d) kondycję finansową dostawcy usług hostingowych,
e) poziom współpracy dostawcy usług hostingowych z właściwymi organami,
f) charakter i rozmiary dostawców usług hostingowych, w szczególności, czy jest on mikro-, małym lub średnim przedsiębiorstwem,

g) stopień winy dostawcy usług hostingowych, z uwzględnieniem podjętych przez niego środków technicznych i organizacyjnych w celu spełnienia wymogów niniejszego rozporządzenia.

Jednocześnie proponuje się, aby należności z tytułu kar pieniężnych stanowiły dochód budżetu państwa, a postępowania w tych sprawach były jednoinstancyjne.

Uzupełnieniem powyższej regulacji będą przepisy prawa krajowego, w tym projektowany **art. 26g** ustawy, w którym proponuje się, aby przy ustalaniu wysokości kary Szef ABW miał możliwość zwrócenia się do dostawcy usług hostingowych, wobec którego prowadzone jest postępowanie w sprawie nałożenia kary pieniężnej, o dostarczenie odpowiednich informacji. Dostawca będzie miał ustawowo 30 dni na dostarczenie stosownej dokumentacji. W przypadku gdy w tym terminie nie poda żądanych informacji, Szef ABW ustali podstawę wymiaru kary pieniężnej w sposób szacunkowy, biorąc pod uwagę ogólnie dostępne dane finansowe tego przedsiębiorcy.

Wskazać też należy, że projekt w zakresie nakładania kar nie przewiduje wyłączenia przepisów powszechnie obowiązujących, czyli w tym przypadku Kodeksu postępowania administracyjnego, a zatem, wymierzając karę, organ będzie miał możliwość skorzystania z narzędzi łagodzących jej ostateczny wymiar, tj. np. z instytucji odroczenia albo rozłożenia na raty stosownie do popełnionego naruszenia oraz innych możliwości określonych przepisami (art. 189k k.p.a.). Dodatkowo podkreślenia wymaga, że chociaż projektodawca założył ustanowienie wyłącznie systemu kar pieniężnych, to jednak zasada proporcjonalności zostanie zachowana również dzięki możliwości zastosowania przez organ przepisów pozwalających na odstąpienie od kary pieniężnej na rzecz lżejszej formy ukarania, np. pouczenia, przy założeniu zaistnienia ku temu określonych prawem przesłanek – *vide* art. 189f k.p.a.

Natomiast w **art. 26h** przewiduje się uregulowanie terminu płatności administracyjnych kar pieniężnych.

Dodanie rozdziału 5a w ustawie o działaniach antyterrorystycznych wymaga modyfikacji dotychczasowych przepisów odnoszących się do kwestii zarządzania blokady dostępności w internecie. W związku z tym w art. 2 niniejszego projektu proponuje się wprowadzenie stosownych zmian do obowiązującego **art. 32c** ustawy Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, który przewiduje, że – co do zasady – w celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa oraz ścigania ich sprawców, sąd na pisemny

wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, w drodze postanowienia, może zarządzić zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa. Jednocześnie wskazać należy, że przepis ten stanowi wdrożenie art. 21 dyrektywy 2017/541 z dnia 15 marca 2017 r., który nakłada na państwa członkowskie obowiązek zapewnienia natychmiastowego usuwania treści internetowych publicznie nawołujących do popełnienia przestępstwa terrorystycznego, nie wskazując przy tym podmiotu zobowiązanego do usuwania takich treści. Z kolei rozporządzenie 2021/784 nakłada zobowiązania do usuwania treści o charakterze terrorystycznym wyłącznie na dostawców usług hostingowych, nie nakładając takich obowiązków na inne podmioty świadczące usługi drogą elektroniczną, w tym np. usługi tzw. cachingu, które należy rozumieć jako usługi polegające na automatycznym i krótkotrwałym przechowywaniu na serwerze pośredniczącym cudzych danych przez stworzenie ich kopii w celu ich szybszego udostępnienia użytkownikowi końcowemu. W tym kontekście podkreślenia wymaga również to, że przepisy ww. dyrektywy nie zostały uchylone rozporządzeniem 2021/784, co oznacza, że oba akty są względem siebie komplementarne i powinny być stosowane równolegle.

Mając powyższe na uwadze, niniejszy projekt zakłada utrzymanie w mocy art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu z jednoczesną jego modyfikacją, która zapewni, że przepis ten będzie miał zastosowanie w przypadkach publikowania lub prób publikowania w internecie treści o charakterze terrorystycznym przez podmioty niebędące dostawcami usług hostingowych w rozumieniu rozporządzenia 2021/784.

Jednocześnie, mając na uwadze zarzuty Komisji Europejskiej odnośnie do nieprawidłowej transpozycji art. 21 ust. 1 dyrektywy 2017/541, proponuje się uzupełnienie art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu o element usuwania treści o charakterze terrorystycznym. W art. 21 ust. 1 dyrektywa 2017/541 zobowiązuje państwa członkowskie do wprowadzenia niezbędnych środków w celu zapewnienia natychmiastowego usuwania treści internetowych o charakterze terrorystycznym, a przynajmniej tych, które znajdują się na serwerach na ich terytorium. Z kolei zgodnie z art. 21 ust. 2 tej dyrektywy państwa członkowskie mogą wprowadzić środki w celu zablokowania

użytkownikom korzystającym z internetu na ich terytorium dostępu do takich treści, jednakże tylko w przypadku, gdy usunięcie takich treści u źródła nie jest możliwe. W ocenie Komisji Europejskiej transpozycja art. 21 ust.1 dyrektywy przez Polskę jest nieprawidłowa. W swoim stanowisku Komisja Europejska stwierdza: „Polskie prawo nie przewiduje środków zapewniających natychmiastowe usuwanie takich treści internetowych, w szczególności gdy takie treści znajdują się na serwerach na terytorium Polski. Chociaż może się to różnić w niektórych indywidualnych przypadkach, nie ma powodu, aby sądzić, że usunięcie treści u źródła byłoby zasadniczo niewykonalne. Art. 21 ust. 2 nie może być rozumiany jako powód, dla którego państwo członkowskie nie dokonało transpozycji art. 21 ust. 1. Zgodnie z dyrektywą państwa członkowskie są bowiem zobowiązane do transpozycji obu przepisów, tak aby możliwe było usunięcie treści zgodnie z art. 21 ust. 1 jako zasada ogólna oraz zablokowanie dostępu zgodnie z art. 21 ust. 2, jeżeli w indywidualnych przypadkach usunięcie nie jest wykonalne.”[6)].

W rezultacie proponuje się w art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu ustanowienie podstawy prawnej do zarządzania wobec usługodawców świadczących usługi drogą elektroniczną usunięcia lub zablokowania dostępności określonych danych lub usług teleinformatycznych, a wobec przedsiębiorców telekomunikacyjnych – zablokowania dostępności takich danych lub usług. Wyłączenie przedsiębiorców telekomunikacyjnych z obowiązku usuwania danych lub usług telekomunikacyjnych wynika z braku ich uprawnienia do podejmowania tego rodzaju czynności.

Jednocześnie wyjaśnić należy, że rozszerzenie zakresu przedmiotowego art. 32c ust. 1 o mechanizm usunięcia określonych danych teleinformatycznych nie będzie miało istotnego przełożenia na zwiększenie zadań organów, o których mowa w tym przepisie. Obowiązek prowadzenia rejestru stosownych postanowień, pisemnych zgód, zarządzeń i wniosków wynika już z obowiązujących przepisów wydanych na podstawie upoważnienia ustawowego z art. 32c ust. 14 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Projektowane zmiany spowodują dodanie do tego katalogu jedynie dokumentacji, która będzie wytworzona na potrzeby zarządzenia usunięcia określonych danych informatycznych. Mając zaś na uwadze, że w świetle obowiązujących przepisów większość dokumentów jest wytwarzana przez przedstawicieli organów ścigania, proponowane zmiany nie wpłyną znacząco również na kognicję i obowiązki sądów.

[6)] Stanowisko Komisji Europejskiej z 9 czerwca 2021 r. (sygn. INFR(2021)2046, C(2021)3630 final, str. 7.

W celu uporządkowania stosowania przepisów prawa unijnego w zakresie usuwania i blokowania internetowych treści o charakterze terrorystycznym, w myśl dyrektywy 2017/541 oraz rozporządzenia 2021/784 proponuje się wskazanie przepisu wyłączającego stosowanie mechanizmów usuwania lub blokowania, o których mowa w art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, w odniesieniu do dostawców usług hostingowych oraz treści o charakterze terrorystycznym, o których mowa w rozporządzeniu 2021/784.

Mając na uwadze, że niniejszy projekt przewiduje modyfikację upoważnienia ustawowego do wydania rozporządzenia przez Prezesa Rady Ministrów dotychczas obowiązującego na podstawie art. 32c ust. 14, w art. 3 niniejszego projektu proponuje się wprowadzenie przepisu przejściowego, utrzymującego w mocy dotychczasowe rozwiązania do czasu przyjęcia nowego rozporządzenia.

Ponadto przewiduje się wprowadzenie przepisu przejściowego, który zapewni, że do blokad dostępności, już zarządzonych i niezakończonych przed dniem wejścia w życie projektowanej ustawy, stosuje się przepisy dotychczasowe.

Projekt uwzględnia wyrażone w art. 67 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców zasady proporcjonalności i adekwatności projektowanych rozwiązań, a zapewniając stosowanie prawa Unii Europejskiej, któremu służy niniejsza regulacja, dokonano nałożenia jedynie takich obowiązków administracyjnych, jakie wynikają bezpośrednio z przepisów rozporządzenia 2021/784. Ponadto, zgodnie ze wskazanym rozporządzeniem, umożliwiono realizację obowiązków informacyjnych w postaci elektronicznej.

Zgodnie z art. 24 rozporządzenia 2021/784 jest ono stosowane od dnia 7 czerwca 2022 r. Do tego dnia państwa członkowskie powinny powiadomić Komisję Europejską o właściwych wyznaczonych organach, a Komisja Europejska ma stworzyć internetowy wykaz tych organów oraz wyznaczonych w nich punktach kontaktowych.

Mając na względzie, że rozporządzenie 2021/784 weszło w życie z dniem 7 czerwca 2021 r., niezbędne jest, aby projektowane zmiany zostały wprowadzone do polskiego porządku prawnego jak najszybciej. Wobec powyższego przewiduje się, że projektowana ustawa wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

W dniu 7 lutego 2024 r. Komisja Europejska skierowała do Rzeczypospolitej Polskiej, na mocy art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, uzasadnioną opinię w związku

z niedopełnieniem niektórych obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. W opinii tej Komisja Europejska zobowiązała Polskę do przedsięwzięcia wymaganych środków w terminie dwóch miesięcy od wpływu opinii. W efekcie Polska musi zapewnić pilną realizację ciążących na niej obowiązków.

Projekt ustawy nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i w związku z tym nie podlega procedurze notyfikacji.

Projekt ustawy jest zgodny z przepisami prawa Unii Europejskiej i służy ich stosowaniu.

Projekt ustawy nie podlega przedstawieniu właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt ustawy stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348 oraz z 2024 r. poz. 757) został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny. W trybie ww. ustawy uwag do projektu nie zgłoszono.

Projekt ustawy nie podlegał dokonaniu oceny OSR przez koordynatora OSR w trybie § 32 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów.

Nazwa projektu Projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Spraw Wewnętrznych i Administracji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan Czesław Mroczek – Sekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji **Kontakt do opiekuna merytorycznego projektu** Pan Mariusz Cichomski – Zastępca Dyrektora Departamentu Porządku Publicznego MSWiA Tel. 47 728 40 70 e-mail: sekretariat.dpp@mswia.gov.pl	**Data sporządzenia** 20.08.2024 r. **Źródło:** dostosowanie przepisów krajowych do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79) **Nr w wykazie prac legislacyjnych i programowych Rady Ministrów:** **UC 37**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Z dniem 7 czerwca 2021 r. weszło w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, zwane dalej „rozporządzeniem", które ustanawia zharmonizowane ramy prawne na potrzeby zapobiegania wykorzystywaniu internetu do rozpowszechniania treści propagujących terroryzm przez wprowadzenie mechanizmu wydawania i weryfikowania nakazów usunięcia lub uniemożliwienia dostępu do treści o charakterze terrorystycznym.

Głównym motywem wydania rozporządzenia jest zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego przez przeciwdziałanie wykorzystywaniu usług hostingowych do celów terrorystycznych oraz przyczynianie się do poprawy bezpieczeństwa publicznego w całej Unii Europejskiej, przy jednoczesnym zagwarantowaniu pełnego poszanowania praw podstawowych, takich jak wolność wypowiedzi i informacji. Nowe uregulowania – co do zasady – zakładają wprowadzenie we wszystkich państwach członkowskich UE spójnego mechanizmu umożliwiającego skuteczne i legalne usuwanie z sieci oraz blokowanie wszelkich treści o charakterze terrorystycznym zamieszczanych z wykorzystywaniem usług hostingowych. Mając na uwadze transgraniczny charakter problemu oraz fakt, że treści o charakterze terrorystycznym są często publicznie rozpowszechniane za pośrednictwem usług świadczonych przez zagranicznych dostawców usług hostingowych, mechanizm ten będzie miał zastosowanie wobec wszystkich dostawców, niezależnie od miejsca ustanowienia ich głównej jednostki organizacyjnej, jeżeli swoje usługi oferują w co najmniej jednym państwie członkowskim UE. W tym zakresie obowiązuje zasada równego traktowania, a działania podejmowane w celu stosowania przyjętych rozwiązań muszą być skuteczne, odpowiednie i proporcjonalne. Środki służące przeciwdziałaniu rozpowszechniania w internecie treści o charakterze terrorystycznym, w rozumieniu przedmiotowej regulacji, w przypadku gdy pozostają skuteczne i proporcjonalne, nie są sprzeczne z ochroną wolności wypowiedzi i informacji, lecz ochronę tę wzmacniają, przede wszystkim zapewniając bezpieczeństwo mediów cyfrowych przed działaniami grup terrorystycznych i ich zwolennikami.

W świetle rozporządzenia za treści o charakterze terrorystycznym, które podlegają usunięciu lub blokowaniu, uznaje się materiały, które:

- podżegają do popełnienia przestępstwa terrorystycznego [w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW (Dz. Urz. UE L 88 z 31.03.2017, str. 6), zwanej dalej „dyrektywą 2017/541"], w przypadku gdy takie materiały bezpośrednio lub pośrednio (np. przez pochwalanie aktów terrorystycznych) popierają popełnianie przestępstwa terrorystycznego, a tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw,
- nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia przestępstwa terrorystycznego,
- nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej,
- udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia przestępstwa terrorystycznego,
- stwarzają zagrożenie popełnienia przestępstwa terrorystycznego.

Treściami o charakterze terrorystycznym w rozumieniu rozporządzenia nie są natomiast materiały rozpowszechniane w celach: edukacyjnych, dziennikarskich, artystycznych, badawczych czy zwiększania świadomości na temat przeciwdziałania działalności terrorystycznej.

Treści o charakterze terrorystycznym nie stanowią również wyrażane w ramach debaty publicznej radykalne, polemiczne lub kontrowersyjne poglądy na drażliwe kwestie polityczne. Przepisy rozporządzenia nie będą miały także zastosowania wobec usług poczty elektronicznej lub przesyłanych wiadomości prywatnych, a także do infrastruktury w chmurze, pod warunkiem że usługi te są świadczone na wniosek stron innych niż dostawcy treści i przynoszą korzyści dostawcom treści jedynie pośrednio.

Natomiast rozporządzenie stosuje się do dostawców usług w zakresie mediów społecznościowych, usług wymiany materiałów video, obrazów i plików audio, a także usług wymiany plików i innych usług w chmurze, jeżeli usługi te są wykorzystywane do publicznego udostępnienia przechowywanych informacji na bezpośredni wniosek dostawcy treści.

W świetle obowiązujących rozwiązań krajowych blokadę dostępności w systemie teleinformatycznym można zastosować wobec danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub wobec określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym. Blokada dostępności wymaga uprzedniej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego i sądu.

Zgodnie z art. 32c ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812, z późn. zm.), Szef ABW, po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, może wnioskować do sądu o zarządzenie blokady dostępności w internecie określonych danych powiązanych ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa. Zaś w przypadkach niecierpiących zwłoki do zarządzenia takiej blokady uprawniony jest Szef ABW, po uzyskaniu pisemnej zgody od Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego. W takiej sytuacji, równocześnie z wydaniem zarządzenia zablokowania strony, Szef ABW zwraca się do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wydanie postanowienia w przedmiotowej sprawie. W przypadku gdy sąd w terminie 5 dni nie udzieli zgody na zarządzenie blokady, jest ona znoszona. W pozostałych przypadkach blokada dostępności danych teleinformatycznych jest zarządzana na okres nie dłuższy niż 30 dni z możliwością jej sądowego przedłużenia na okres nie dłuższy niż 3 miesiące.

Mechanizm przyjęty w rozporządzeniu jest natomiast znacznie szybszy i uproszczony. Przewiduje również możliwość jego transgranicznego stosowania. Unijne regulacje nie zakładają konieczności uzyskania sądowej zgody do jego zainicjowania, natomiast zapewniają wdrożenie procedury skargowej, do której będzie miała prawo każda ze stron, której wydany nakaz dotyczy, tj. zarówno dostawcy usług hostingowych, jak i dostawcy treści, które zostały usunięte.

W związku z tym zaistniała potrzeba zainicjowania prac legislacyjnych mających na celu dostosowanie polskiego porządku prawnego do nowych uregulowań unijnych, zapewniając tym samym ich bezpośrednie stosowanie.

Konsekwentnie projekt przewiduje dokonanie modyfikacji obowiązującego art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, która zapewni, że przepis będzie miał zastosowanie w przypadkach nieobjętym reżimem rozporządzenia. Dodatkowo, mając na uwadze zarzuty Komisji Europejskiej odnośnie do nieprawidłowej transpozycji art. 21 ust. 1 dyrektywy 2017/541, proponuje się uzupełnienie art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zgodnie z oczekiwaniami Komisji Europejskiej przedstawionymi w tym zakresie.

W art. 21 ust. 1 dyrektywa 2017/541 zobowiązuje państwa członkowskie do wprowadzenia niezbędnych środków w celu zapewnienia natychmiastowego usuwania odnośnych treści internetowych, a przynajmniej tych, które znajdują się na serwerach na ich terytorium. Z kolei zgodnie z art. 21 ust. 2 tej dyrektywy państwa członkowskie mogą wprowadzić środki w celu zablokowania użytkownikom korzystającym z internetu na ich terytorium dostępu do takich treści, jednakże tylko w przypadku, gdy usunięcie takich treści u źródła nie jest możliwe. W ocenie Komisji Europejskiej transpozycja art. 21 ust. 1 dyrektywy przez Polskę jest nieprawidłowa. Art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu nie przewiduje środków zapewniających natychmiastowe usuwanie takich treści internetowych, a jedynie ich blokowanie.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rekomendowane rozwiązanie zakłada dokonanie nowelizacji ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2024 r. poz. 92, z późn. zm.) przez wskazanie organu właściwego w rozumieniu rozporządzenia.

W rezultacie proponuje się ustanowienie na gruncie ustawowym właściwości Szefa ABW jako organu właściwego w rozumieniu rozporządzenia. Tym samym Szef ABW będzie odpowiedzialny m.in. za:

a) wydawanie nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich, zgodnie z art. 3 rozporządzenia,
b) weryfikowanie nakazów usunięcia wydanych przez właściwe organy innych państw członkowskich oraz stwierdzanie ewentualnych naruszeń w tym zakresie, zgodnie z art. 4 rozporządzenia,
c) przedłużanie okresu zachowania treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony, na skutek wydanego nakazu usunięcia (art. 6 ust. 2 rozporządzenia),
d) wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym oraz nadzoru nad wdrażaniem przez nich środków szczególnych, na podstawie art. 5 rozporządzenia,
e) prowadzenie współpracy, w tym wymiany informacji, z innymi właściwymi organami ustanowionymi przez pozostałe państwa członkowskie, z Europolem oraz dostawcami usług hostingowych, zgodnie z art. 14 rozporządzenia,
f) nakładanie kar administracyjnych, na podstawie art. 18 rozporządzenia,
g) publikację sprawozdania, na podstawie art. 8 rozporządzenia,
h) przekazywanie do Komisji Europejskiej rocznej informacji, na podstawie art. 21 rozporządzenia.

Szef ABW wyznaczy, na podstawie art. 12 ust. 2 rozporządzenia, całodobowy punkt kontaktowy właściwy do rozpatrywania wniosków o wyjaśnienie i informacje zwrotne dotyczące nakazów wydanych przez ABW, którego dane będą publicznie dostępne za pośrednictwem Biuletynu Informacji Publicznej na stronie podmiotowej ABW, a także przekazane do wiadomości Komisji Europejskiej.

Wskazywanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, o których mowa w art. 5 rozporządzenia, będzie następowało w formie decyzji Szefa ABW. Natychmiastowa wykonalność tych decyzji jest uzasadniona potrzebą podjęcia działań w trybie niecierpiącym zwłoki z uwagi na charakter zagrożeń, jakie mogą powodować treści o charakterze terrorystycznym publikowane w internecie. W tym miejscu podkreślić należy, że zgodnie z art. 5 ust. 4 rozporządzenia, tego rodzaju decyzje będą dotyczyły dostawców usług hostingowych, którzy już co najmniej 2 razy w ciągu ostatnich 12 miesięcy otrzymali nakaz usunięcia, a zatem ich usługi były już wykorzystywane do działań terrorystycznych. Natychmiastowa wykonalność decyzji nie jest jednak tożsama z koniecznością natychmiastowego wdrożenia środków szczególnych przez dostawców usług hostingowych, ale z natychmiastowym podjęciem stosownych działań w tym kierunku oraz ich odpowiednim zaplanowaniem. Zgodnie z art. 5 ust. 5 rozporządzenia dostawca usług hostingowych narażony na treści o charakterze terrorystycznym powiadamia właściwy organ (Szefa ABW) o środkach, które podjął lub zamierza podjąć, w terminie do 3 miesięcy od otrzymania decyzji w tej sprawie.

Szef ABW będzie sprawował nadzór nad dostawcami usług hostingowych w zakresie wdrażania przez nich środków szczególnych. Nadzór będzie polegał na dokonywaniu przez Szefa ABW kontroli środków szczególnych, które dostawca usług hostingowych zdecydował się zastosować, a także na wydawaniu zaleceń w przypadku stwierdzenia nieprawidłowości w tym zakresie. W celu zapewnienia wykonania tych czynności upoważniony funkcjonariusz ABW będzie miał prawo wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych oraz prawo żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia bądź wglądu w dokumentację techniczną i operacyjną wynikającą ze stosowania środków szczególnych. W myśl projektowanych przepisów dostawca usług hostingowych będzie zobowiązany do terminowego usunięcia stwierdzonych nieprawidłowości. Należy jednak zauważyć, że w świetle art. 5 ust. 6 rozporządzenia przedmiotowe działania kontrolne Szef ABW będzie – co do zasady – podejmował najwcześniej dopiero po otrzymaniu od dostawcy usług hostingowych powiadomienia, o którym mowa w art. 5 ust. 5 rozporządzenia, a zatem po upływie okresu do 3 miesięcy od wydania decyzji o konieczności stosowania środków szczególnych lub też bezpośrednio na wniosek samego dostawcy usług hostingowych.

Nakazy usunięcia oraz stwierdzenie naruszeń, o których mowa w art. 4 ust. 3 i 4 rozporządzenia, będą wydawane w formie decyzji administracyjnych, do których będzie miała zastosowania ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572), zwanego dalej „k.p.a.”, jedynie we wskazanym zakresie, co wynika z faktu, że tryb postępowania opisany w rozporządzeniu odnośnie do wydawania nakazów usunięcia ma zapewnić na poziomie unijnym (a zatem w wymiarze transgranicznym) spójny i efektywny mechanizm usuwania lub blokowania w sieci wszelkich treści o charakterze terrorystycznym. Skuteczność tego mechanizmu jest natomiast mierzona szybkością reakcji i wykonania stosownych czynności. W rezultacie przyjęty w unijnym akcie sposób postępowania zarówno w odniesieniu do wydawania nakazów usunięcia, jak i stwierdzenia naruszeń, o których mowa w art. 4 ust. 3 i 4 rozporządzenia, znacząco odbiega od niektórych rozwiązań przyjętych na gruncie krajowych przepisów prawa administracyjnego. Ponadto większość elementów w rozumieniu postępowania administracyjnego zostało wprost określonych w samym rozporządzeniu, np. elementy decyzji, moment i skutek jej doręczenia, a zatem w takim przypadku jest niezbędne wyłączenie uregulowań krajowych. Analogicznie będą traktowane postępowania w sprawie wskazywania dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym. We wszystkich tych przypadkach postępowania będą jednoinstancyjne, a wydane decyzje będą podlegały natychmiastowej wykonalności. Tryb jednoinstancyjny jest w tym przypadku niezbędny w celu zapewnienia sprawności i efektywności prowadzenia takich postępowań. Takie rozwiązanie pozostaje zgodne z Konstytucją RP, która w art. 78 przewiduje możliwość ustawowego odstępstwa od zaskarżenia orzeczeń i decyzji wydanych w pierwszej instancji. Zgodnie z ustawą zasadniczą tego rodzaju ograniczenia mogą być ustanawiane wyłącznie ustawą i gdy jest to konieczne m.in. z uwagi na kwestie bezpieczeństwa i porządku

publicznego. Kontekst i *ratio legis* projektu wpisują się zatem w te przesłanki. Natomiast mając na uwadze, że dostawcy usług hostingowych i dostawcy treści będzie każdorazowo przysługiwało prawo wniesienia skargi do sądu, istota wolności i praw pozostanie w tym przypadku zachowana.

Prawo do zaskarżenia będzie przysługiwało dostawcom usług hostingowych również w odniesieniu do decyzji Szefa ABW wydanych na podstawie art. 5 ust. 6 lub 7 rozporządzenia. W przypadku gdy strona nie zawnioskuje o przeprowadzenie rozprawy, sąd – jeżeli uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione – będzie mógł zdecydować o jej rozpoznaniu w trybie uproszczonym. Tryb uproszczony będzie mógł mieć zastosowanie jedynie fakultatywnie po spełnieniu łącznie ww. warunków i ma – co do zasady – zapewnić, że rozpatrywanie środków prawnych od nakazów usunięcia oraz od decyzji o wskazaniu dostawcy usług hostingowych narażonych na treści o charakterze terrorystycznym będzie realizowane w sposób sprawny i efektywny, ale z zachowaniem wszelkich gwarancji prawa do sądu.

W postępowaniach, o których mowa powyżej, właściwy pozostaje sąd administracyjny, co wynika z faktu, że postępowania te będą dotyczyły wyłącznie kwestii prawno-administracyjnych. Należy zauważyć, że określone rozporządzeniem sankcje odnoszą się do sytuacji niespełnienia określonych obowiązków o charakterze administracyjnym przez dostawcę usług hostingowych, nie zaś dopuszczenia się przez nich czynów karalnych na gruncie przepisów prawa karnego materialnego. Samo usuwanie treści nie jest środkiem sankcyjnym, lecz środkiem ograniczającym. Celem rozporządzenia nie jest bowiem wykrywanie i ściganie przestępstw o charakterze terrorystycznym, jak ma to miejsce np. w odniesieniu do regulacji stanowiących podstawę prawną do zarządzenia blokady określonych danych informatycznych (art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu), ale zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego w otwartym i demokratycznym społeczeństwie przez przeciwdziałanie wykorzystywaniu usług hostingowych do celów terrorystycznych oraz przyczynianie się do poprawy bezpieczeństwa publicznego w całej Unii (motyw 1 rozporządzenia).

Mając na uwadze potrzebę zapewnienia wykonania art. 21 ust. 1 rozporządzenia, który zobowiązuje państwa członkowskie do gromadzenia i przekazywania do Komisji Europejskiej informacji m.in. w zakresie podjętych środków szczególnych, liczby wszczętych procedur rozpatrywania skarg oraz innych działań podjętych przez dostawcę usług hostingowych w ramach ustanowionego mechanizmu skargowego, dostawcy usług hostingowych będą zobowiązani do cyklicznego przekazywania do Szefa ABW informacji, o których mowa w art. 21 ust. 1 lit. b i d rozporządzenia. Dane te następnie będą zbiorczo przesyłane do wiadomości Komisji Europejskiej.

Proponuje się również uregulowanie kwestii związanej z nakładaniem przez Szefa ABW kar finansowych za naruszenia wskazane w rozporządzeniu. Podstawę prawną w tym zakresie stanowi art. 18 rozporządzenia. Zatem wysokość tych kar będzie ustalana w oparciu o przepisy unijne, które przewidują maksymalny ich wymiar w wysokości do 4% całkowitych obrotów dostawcy usług hostingowych w poprzednim roku obrotowym. Tak wysoki wymiar kary będzie mógł mieć zastosowanie jednak wyłącznie w przypadku systematycznego i uporczywego niedopełnienia obowiązków wynikających z art. 3 ust. 3 rozporządzenia, tj. nieusuwania lub nieblokowania w terminie treści o charakterze terrorystycznym. Zgodnie z rozporządzeniem wysokość kar pieniężnych powinna być skuteczna, proporcjonalna i odstraszająca w zależności od zaistniałych okoliczności, rozpatrywanych w każdym przypadku indywidualnie. W związku z tym proponuje się przyznanie Szefowi ABW prawa do żądania od dostawcy usług hostingowych, wobec którego prowadzone jest postępowanie, dostarczenia odpowiednich dokumentów, które pomogą określić odpowiednią, tj. zgodną z zasadą proporcjonalności, wysokość kary. W przypadku nieotrzymania takich danych Szef ABW będzie szacował wymiar kary m.in. w oparciu o posiadane dane oraz kryteria przewidziane w tym zakresie w ustawie z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm.). Stosowanie zasady proporcjonalności zapewniają również przepisy k.p.a., które w odniesieniu do postępowań dotyczących nakładania kary nie zostały wyłączone i mają zastosowanie w całości. W związku z tym, wymierzając karę, organ będzie miał możliwość skorzystania z narzędzi łagodzących jej ostateczny wymiar, tj. np. z instytucji odroczenia albo rozłożenia na raty stosownie do popełnionego naruszenia oraz innych możliwości określonych przepisami (art. 189k k.p.a.). Dodatkowo podkreślenia wymaga, że chociaż projektodawca założył ustanowienie wyłącznie systemu kar pieniężnych, to jednak zasada proporcjonalności zostanie zachowana również dzięki możliwości zastosowania przez organ przepisów pozwalających na odstąpienie od kary pieniężnej na rzecz lżejszej formy ukarania, np. pouczenia, przy założeniu zaistnienia ku temu określonych prawem przesłanek – *vide* art. 189f k.p.a.

Mając na uwadze brzmienie art. 16 rozporządzenia, który jednoznacznie rozstrzyga kwestie jurysdykcji, należy zauważyć, że zasadniczo Szef ABW będzie organem właściwym w zakresie nakładania kar przede wszystkim w odniesieniu do dostawców usług hostingowych, których jednostka organizacyjna albo siedziba ich przedstawiciela prawnego znajduje się na terenie Polski.

Należności z tytułu administracyjnych kar pieniężnych będą stanowiły dochód budżetu państwa.

Przyjęcie rozwiązań mających na celu zapewnienie stosowania rozporządzenia wymaga modyfikacji dotychczasowych przepisów odnoszących się do kwestii zarządzania blokady dostępności w internecie. W związku z tym proponuje się wprowadzenie stosownych zmian do obowiązującego art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, które zapewnią, że przepis ten będzie miał zastosowanie w przypadkach publikowania lub prób

publikowania w internecie treści o charakterze terrorystycznym przez podmioty niebędące dostawcami usług hostingowych w rozumieniu rozporządzenia. Jednocześnie w celu uporządkowania stosowania przepisów prawa unijnego w zakresie usuwania i blokowania internetowych treści o charakterze terrorystycznym, w myśl dyrektywy 2017/541 oraz rozporządzenia 2021/784 proponuje się dodanie odpowiedniego przepisu pozwalającego na równoległe stosowanie obu mechanizmów wynikających z ww. aktów unijnych. Ponadto proponuje się rozszerzenie tego przepisu o mechanizm usuwania treści o charakterze terrorystycznym, wypełniając tym samym zobowiązanie, jakie na państwa członkowskie narzuca w art. 21 ust. 1 dyrektywa 2017/541.

Jednocześnie rozszerzenie zakresu przedmiotowego art. 32c ust. 1 o mechanizm usunięcia określonych danych teleinformatycznych nie będzie miało istotnego przełożenia na zwiększenie zadań organów, o których mowa w tym przepisie. Obowiązek prowadzenia rejestru stosownych postanowień, pisemnych zgód, zarządzeń i wniosków wynika już z obowiązujących przepisów wydanych na podstawie upoważnienia ustawowego z art. 32c ust. 14 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Projektowane zmiany spowodują dodanie do tego katalogu jedynie dokumentacji, która będzie wytworzona na potrzeby zarządzenia usunięcia określonych danych informatycznych.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Na podstawie art. 12 ust. 4 rozporządzenia Komisja Europejska tworzy i na bieżąco aktualizuje internetowy rejestr zawierający wykaz właściwych organów, o których mowa w art. 12 ust. 1, oraz punktów kontaktowych wyznaczonych lub ustanowionych na podstawie art. 12 ust. 2 rozporządzenia. Zgodnie z rejestrem opublikowanym na stronie internetowej Komisji Europejskiej spośród 27 państw członkowskich 24 państwa członkowskie przekazały takie informacje. Są to:

1) Austria – Kommunikationsbehörde Austria (KommAustria),
2) Belgia – Federal prosecution service,
3) Bułgaria – Ministry of Interior - General Directorate Combating Organised Crime,
4) Chorwacja - Ministarstvo unutarnjih poslova,
5) Cypr – Cyprus Police i Ministry of Energy, Commerce and Industry,
6) Czechy – Police of the Czech Republic i Ministry of Interior of the Czech Republic
7) Dania – The Danish National Police,
8) Estonia – Estonian Internal Security Service,
9) Finlandia – National Bureau of Investigation
10) Francja – L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC),
11) Niemcy – Bundeskriminalamt (Federal Criminal Police Office),
12) Węgry – Nemzeti Média- és Hírközlési Hatóság,
13) Irlandia – An Garda Síochána,
14) Łotwa – State Security Service,
15) Litwa – Lithuanian Police,
16) Luksemburg – Police grand-ducale - Ministère de la Sécurité intérieure,
17) Malta – The Court of Justice as a Court of Criminal Judicature,
18) Holandia – Autoriteit online Terroristisch en Kinderpornografisch Materiaal,
19) Rumunia – Autoritatea Națională pentru Administrare și Reglementare în Comunicații,
20) Słowacja – Police Force of the Slovak Republic,
21) Hiszpania – The Centre for Intelligence against Terrorism and Organised Crime (CITCO), Secretariat of State for Security of the Ministry of the Interior,
22) Szwecja – Polismyndigheten,
23) Włochy – Uffici del Pubblico Ministero presso i Tribunali oraz Ministero dell'Interno – Dipartimento della Pubblica Sicurezza,
24) Grecja – Prosecutor of the Anti-terrorist Unit.

Podsumowując, 13 państw wyznaczyło organ właściwy pośród swoich wewnętrznych służb o charakterze policyjnym lub specjalnym, 4 państwa wskazały na właściwość komórki organizacyjnej funkcjonującej w ramach resortu odpowiedzialnego za sprawy wewnętrzne i tyle samo państw taką właściwość przewidziały w innych urzędach centralnych, np. w przypadku Węgier to Narodowy Urząd ds. Mediów i Komunikacji, w Austrii – Urząd do Spraw Łączności. W 2 państwach jest to organ prokuratorski, a w 1 państwie właściwy jest sąd.

Państwa, które nie przekazały jeszcze takich danych do Komisji Europejskiej to, oprócz Polski: Portugalia i Słowenia [1)].			
4. Podmioty, na które oddziałuje projekt			
Grupa	Wielkość	Źródło danych	Oddziaływanie
Szef ABW	1		– powierzenie zadań wynikających ze stosowania rozporządzenia, w tym dotyczących: a) wydawania nakazów zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, b) weryfikowania nakazów usunięcia wydanych przez właściwe organy innych państw członkowskich oraz stwierdzania ewentualnych naruszeń w tym zakresie, c) przedłużania okresu zachowania treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony, d) wydawania decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, e) nadzoru nad wdrażaniem środków szczególnych przez dostawców usług hostingowych; f) prowadzenia współpracy, w tym wymiany informacji, z innymi właściwymi organami oraz Europolem g) nakładania kar administracyjnych za naruszenia, o których mowa w rozporządzeniu; h) publikowania rocznych sprawozdań z przejrzystości, dotyczących działalności prowadzonej na podstawie rozporządzenia; i) przekazywania do Komisji Europejskiej rocznych informacji, o których mowa w rozporządzeniu; – obowiązek wyznaczenia punktu kontaktowego właściwego do przyjmowania wniosków i udzielania informacji dotyczących wydanych nakazów usunięcia; – wnioskowanie do sądu o zarządzenie usunięcia przez usługodawcę świadczącego usługi drogą elektroniczną lub zablokowania przez przedsiębiorcę telekomunikacyjnego dostępności określonych danych informatycznych lub określonych usług teleinformatycznych;
Wojewódzki Sąd Administracyjny w Warszawie	1		– rozpatrywanie skarg na decyzje Szefa ABW;
Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy	1		– wydawanie zgód w sprawie zarządzenia usunięcia lub blokady dostępności określonych danych informatycznych lub określonych usług teleinformatycznych;
Sąd Okręgowy w Warszawie	1		– wydawanie postanowień w sprawie zarządzenia usunięcia lub blokady dostępności określonych danych informatycznych lub określonych usług teleinformatycznych;

[1)] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en (dostęp: 12.06.2024 r.)

Sąd Apelacyjny w Warszawie	1		– rozpoznawanie zażaleń na postanowienia Sądu Okręgowego w Warszawie w sprawie zarządzenia usunięcia lub blokady dostępności określonych danych informatycznych lub określonych usług teleinformatycznych;
dostawcy usług hostingowych, których główna jednostka organizacyjna lub których przedstawiciel prawny ma siedzibę lub miejsce pobytu na terytorium Polski	brak danych		– prawo do skargi na decyzję Szefa ABW dotyczącą nakazu usunięcia treści o charakterze terrorystycznym albo decyzję, o której mowa w art. 4 ust. 4 rozporządzenia; – prawo do skargi na decyzję Szefa ABW o której mowa w art. 5 ust. 4, 6 lub 7 rozporządzenia; – obowiązek przekazywania do Szefa ABW danych, wynikających z realizacji rozporządzenia; – obowiązek wykonania decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym oraz nadzoru nad wdrażaniem przez nich środków szczególnych;
dostawcy treści	brak danych		– prawo do skargi na decyzję Szefa ABW dotyczącą nakazu usunięcia treści o charakterze terrorystycznym albo decyzję, o której mowa w art. 4 ust. 4 rozporządzenia.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt ustawy został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji, stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz zgodnie z § 52 ust. 1 uchwały Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348 oraz z 2024 r. poz. 757). W trybie ww. ustawy uwag nie zgłoszono.

Zakres zmian przepisów krajowych służących stosowaniu rozporządzenia 2021/784 został omówiony w ramach Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych, powołanego zarządzeniem nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, który jako organ pomocniczy Rady Ministrów zapewnia współdziałanie administracji rządowej w zakresie przygotowania do zapobiegania zdarzeniom o charakterze terrorystycznym, przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć oraz do reagowania na nie. W ramach Zespołu nie zgłoszono uwag co do zaproponowanego przez Ministerstwo Spraw Wewnętrznych i Administracji sposobu zapewnienia stosowania przepisów rozporządzenia na gruncie krajowym.

Projekt nie wywoła skutków dla budżetów jednostek samorządu terytorialnego, wobec czego nie wymagał konsultacji z Komisją Wspólną Rządu i Samorządu Terytorialnego.
Projekt został przekazany do rozpatrzenia przez Komitet do Spraw Europejskich.

Mimo że projekt będzie oddziaływał na branżę przedsiębiorstw świadczących usługi hostingowe, to jednak, zgodnie z informacją przekazaną przez Kancelarię Prezesa Rady Ministrów, nie jest możliwe oszacowanie wielkości tej branży, z tych względów nie było możliwe przeprowadzenie konsultacji projektu z tą branżą. Niemniej, w związku z udostępnieniem projektu w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji, dostęp do projektowanej regulacji był zapewniony dla nieograniczonego kręgu podmiotów. Korzystając z tej możliwości zapoznania się z projektem, uwagi zgłosiła Krajowa Izba Komunikacji Ethernetowej. Wyniki uzgodnień zostały opisane w załączonym raporcie z konsultacji. Ponadto stanowisko do projektu przestawiła Polska Izba Informatyki i Telekomunikacji.

W świetle dostępnych krajowych źródeł danych brak jest statystyk, które wskazują na liczbę podmiotów świadczących usługi hostingowe w Polsce, a w związku z tym brak jest również informacji określających estymację dotyczącą ewolucji tego rynku. Przyjęta formuła konsultacji i uzgodnień podyktowana jest koniecznością jak najszybszego dostosowania przepisów prawa krajowego do regulacji wynikających z rozporządzenia, które weszły w życie 7 czerwca 2021 r. i powinny być stosowane przez państwa członkowskie, począwszy od dnia 7 czerwca 2022 r.

Przygotowując ocenę skutków regulacji do projektu rozporządzenia 2021/784 także Komisja Europejska nie zaprezentowała dokładnych danych na temat wielkości branży hostingowej w Unii Europejskiej. Oszacowano wówczas, że obowiązkami wynikającymi z rozporządzenia będzie objętych 10,5 tys. dostawców usług hostingowych mających siedzibę w Europie i prawie 20 tys. mających siedzibę zarówno w Europie, jak i w Stanach Zjednoczonych i Kanadzie. Oszacowano, że w Unii Europejskiej ponad 90% hostingodawców to MŚP (9700 firm). Te szacunki nie były jednak oparte na danych zbieranych przez urzędy statystyczne, lecz wyliczono je w oparciu o komercyjną bazę danych DealRoom (https://dealroom.co/). Są to

jedynie przybliżone szacunki. Przedsiębiorstwa objęte bazą danych to przedsiębiorstwa na poziomie zalążkowym, otrzymujące kapitał venture lub publiczny i z założeniem, że są to firmy z dużym potencjałem wzrostu.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]										
	0	1	2	3	4	5	6	7	8	9	10
Dochody ogółem	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-
JST	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-
Wydatki ogółem	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-
JST	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-
Saldo ogółem	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-
Źródła finansowania											

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń

Wejście w życie ustawy nie wywoła skutków finansowych dla budżetów jednostek samorządu terytorialnego w rozumieniu art. 50 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270, z późn. zm.), jednocześnie będzie miało znikomy wpływ na budżet państwa.

Przedmiotowa nowelizacja nie pociągnie bowiem za sobą konieczności zwiększenia wydatków budżetu państwa w związku ze wskazaniem i prowadzeniem punktu kontaktowego właściwego do przyjmowania wniosków i udzielania informacji dotyczących wydanych nakazów usunięcia. Będzie on mieścił się w ramach istniejącej struktury etatowej Agencji Bezpieczeństwa Wewnętrznego.

Natomiast mając na uwadze, że projektowana ustawa przewiduje nakładanie przez Szefa ABW na dostawców usług hostingowych administracyjnych kar pieniężnych za naruszenia wynikające z rozporządzenia, które będą stanowiły dochód budżetu państwa, należy z tego tytułu prognozować przychód do budżetu państwa. Niemniej trzeba przyjąć, że będzie on znikomy, a ponadto niemożliwy na tym etapie do zwymiarowania. Prognozowany dochód jest trudny do oszacowania ze względu na brak danych, które posłużyłyby do dokonania stosownych obliczeń. Nie jest bowiem znana liczba przedsiębiorstw świadczących usługi hostingowe, których główna jednostka organizacyjna lub których przedstawiciel prawny ma siedzibę lub miejsce pobytu na terytorium Rzeczypospolitej Polskiej, jak również nie jest możliwe ustalenie częstotliwości naruszeń, za które będą nakładane przedmiotowe kary. Należy jednak zauważyć, że w Polsce, z uwagi na poziom zagrożenia terrorystycznego, działania podejmowane w celu przeciwdziałania temu rodzajowi zagrożeń pozostają proporcjonalne względem analiz ryzyka i nie zakładają wprowadzania szczególnych (nadmiernie restrykcyjnych) środków.

Jednocześnie, mając na uwadze prognozowaną niewielką liczbę spraw kierowanych do sądów, projektowane zmiany nie będą miały wpływu na funkcjonowanie Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Sądu Okręgowego w Warszawie w takim znaczeniu, że realizacja celów nowelizacji możliwa jest w ramach dotychczas posiadanych środków budżetowych w części 05 (Naczelny Sąd Administracyjny) oraz w części 15 (Sądy powszechne), bez potrzeby ich zwiększania w roku wejścia w życie regulacji oraz w latach następnych.

Zgodnie z informacją podaną przez Komisję Europejską w państwach członkowskich, które stosują rozporządzenie, do 31 grudnia 2023 r. żaden dostawca usług hostingowych nie zaskarżył przed właściwym sądem otrzymanego nakazu usunięcia[2)].

[2)] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym z 14.02.2024 r. (COM(2024) 64 final) str. 8-9.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, oraz na rodzinę, obywateli i gospodarstwa domowe												
Skutki												
Czas w latach od wejścia w życie zmian		1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa											
	sektor mikro-, małych i średnich przedsiębiorstw											
	rodzina, obywatele oraz gospodarstwa domowe											
	Przewoźnicy lotniczy z tytułu nakładanych kar pieniężnych											
W ujęciu niepieniężnym	duże przedsiębiorstwa											
	sektor mikro-, małych i średnich przedsiębiorstw	Mikro- i mali przedsiębiorcy będą mogli korzystać ze wsparcia oferowanego w ramach trzech projektów wybranych przez Komisję Europejską i finansowanych z Funduszu Bezpieczeństwa Wewnętrznego. Zgodnie z informacją przekazaną przez Komisję Europejską wsparcie to polega na zwiększaniu świadomości przedsiębiorców na temat przepisów i wymogów rozporządzenia, opracowywaniu, wdrażaniu i uruchamianiu narzędzi i mechanizmów niezbędnych do przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, a także na umożliwianiu wymiany doświadczeń i najlepszych praktyk w całym sektorze dostawców usług hostingowych.[3)]										
	rodzina, obywatele oraz gospodarstwa domowe											
	(dodaj/usuń)											
Niemierzalne	(dodaj/usuń)											
	(dodaj/usuń)											
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		Wpływ proponowanych zmian w przepisach na konkurencyjność gospodarki i przedsiębiorczość będzie znikomy i niemożliwy do zwymiarowania z tych samych powodów, które zostały wskazane w pkt 6 OSR w części dotyczącej dodatkowych informacji, w tym wskazania źródeł danych i przyjętych do obliczeń założeń. Jednocześnie, mając na uwadze, że przedmiotowa nowelizacja wprowadza przepisy, które, co do zasady, mają zapewnić ochronę przed internetową propagandą terrorystyczną, należy przyjąć pozytywny wpływ projektowanej regulacji na funkcjonowanie rodzin i obywateli w kontekście zwiększenia poziomu bezpieczeństwa przed działaniami grup terrorystycznych i ich zwolenników. Ze sprawozdania Komisji z wykonania rozporządzenia opublikowanego w lutym 2024 r. wynika, że dotychczasowe stosowanie rozporządzenia miało pozytywny wpływ na ograniczenie rozpowszechniania w internecie treści o charakterze terrorystycznym.[4)]										

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu	
☐ nie dotyczy	
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak X nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur X - skrócenie czasu na załatwienie sprawy ☐ inne:	X zwiększenie liczby dokumentów X zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	X tak ☐ nie ☐ nie dotyczy

[3)] Str. 12 Sprawozdania, o którym mowa w odnośniku nr 2.
[4)] Str. 3 Sprawozdania, o którym mowa w odnośniku nr 2.

Projektowana ustawa określa nowe kompetencje Szefa ABW dotyczące wydawania nakazów zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia do nich dostępu oraz realizowania – jako organ właściwy – pozostałych procedur wynikających ze stosowania rozporządzenia. Rozszerza również zakres obowiązku informacyjnego o publikację rocznych sprawozdań z przejrzystości dotyczących działalności prowadzonej w tym zakresie, a także przekazywania do Komisji Europejskiej rocznej informacji statystycznej, o której mowa w rozporządzeniu.

Jednocześnie projektowane przepisy zapewnią znacznie szybszy i uproszczony mechanizm usuwania ze stron internetowych treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich. Od 3 lipca 2023 r. funkcjonuje opracowana przez Europol i ustanowiona w tym celu platforma o nazwie „PERCI" (Platforme Européenne de Retraits des Contenus illégaux sur Internet). Jest to jednolity system komunikacji w czasie rzeczywistym oparty na chmurze, który przez zapewnienie centralnej koordynacji ułatwia szybkie przekazywanie nakazów usunięcia i zgłoszeń do dostawców usług hostingowych, w tym również pozwala na usuwanie konfliktów między państwami członkowskimi (właściwymi organami) w sytuacjach, w których właściwy organ państwa członkowskiego wysyła nakaz usunięcia treści będący przedmiotem trwającego już postępowania przygotowawczego w innym państwie członkowskim.

Projekt uwzględnia wyrażone w art. 67 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców zasady proporcjonalności i adekwatności projektowanych rozwiązań, a zapewniając stosowanie prawa Unii Europejskiej, któremu służy niniejsza regulacja, dokonano nałożenia jedynie takich obowiązków administracyjnych, jakie wynikają bezpośrednio z przepisów rozporządzenia 2021/784. Ponadto, zgodnie ze wskazanym rozporządzeniem, umożliwiona będzie realizacja obowiązków informacyjnych w postaci elektronicznej.

9. Wpływ na rynek pracy

Wejście w życie projektowanej nowelizacji ustawy nie będzie miało istotnego wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny X sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe X inne: bezpieczeństwo	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Internet pozostaje w zainteresowaniu zarówno indywidualnych przestępców, jak i zorganizowanych grup przestępczych oraz środowisk ekstremistycznych, w tym organizacji terrorystycznych, które wykorzystują cyberprzestrzeń do upowszechniania skrajnej ideologii, pozyskiwania zwolenników, prowadzenia instruktażu w zakresie podejmowania indywidualnych aktów terroru czy też konstruowania ładunków wybuchowych i pozyskiwania do nich komponentów. Należy mieć na uwadze, że upowszechnienie dostępu do internetu, w kontekście globalnego charakteru cyberprzestrzeni, pozwala na popełnianie tego rodzaju przestępstw ponad granicami państwowymi. Wykorzystując usługi hostingowe oferowane na terenie jednego państwa, sprawca może zamieścić treści o charakterze terrorystycznym, które za pośrednictwem sieci internet będą globalnie dostępne i rozpowszechniane w wielu państwach. Projektowane zmiany mają na celu w sposób systemowy wzmocnić bezpieczeństwo w internecie przed tego rodzaju działaniami propagandowymi grup terrorystycznych i ich zwolenników, w tym również działaniami pochodzącymi z zagranicy. Projekt zapewni możliwość stosowania przepisów rozporządzenia, które ustanawiają transgraniczny mechanizm szybkiego wydawania i weryfikowania nakazów usunięcia lub uniemożliwienia dostępu do zamieszczonych w internecie treści o charakterze terrorystycznym. Mając na uwadze, że projekt przewiduje przyznanie dostawcom usług hostingowych lub dostawcom treści, w stosunku do których Szef ABW wydał decyzje usunięcia treści lub uniemożliwienia do nich dostępu w internecie, prawo do wniesienia na te decyzje skargi do sądu administracyjnego, proponowane zmiany będą miały wpływ na sądy administracyjne. Niemniej doświadczenia wynikające ze stosowania art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu stanowiącego obecnie jedyną podstawę prawną do blokowania dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym wskazują co najwyżej na incydentalność takich przypadków w Polsce. W związku z tym zakłada się, że tego rodzaju skargi będą sporadyczne i nie będą w sposób istotny rzutowały na rozszerzenie kognicji sądów w tym zakresie.

	Od dnia stosowania rozporządzenia (7 czerwca 2022 r.) do 31 grudnia 2023 r. nie było prowadzone żadne postępowanie sądowe w sprawie otrzymanego nakazu usunięcia.[5)]

11. Planowane wykonanie przepisów aktu prawnego

Przewiduje się, że projektowana ustawa wejdzie w życie po upływie 14 dni od dnia jej ogłoszenia.
Proponowane w projekcie ustawy rozwiązania wynikają z konieczności stosowania rozporządzenia. W związku z tym, zgodnie z przyjętym regulacjami unijnymi, do dnia 31 marca każdego roku państwa członkowskie przedstawią Komisji Europejskiej informację na temat działań podjętych w poprzednim roku kalendarzowym wynikających ze stosowania rozporządzenia. Ponadto Komisja Europejska będzie prowadzić listę krajowych punktów kontaktowych po stronie właściwych organów krajowych.

W dniu 7 lutego 2024 r. Komisja Europejska skierowała do Rzeczypospolitej Polskiej, na mocy art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, uzasadnioną opinię w związku z niedopełnieniem niektórych obowiązków wynikających z rozporządzenia. W opinii tej Komisja Europejska zobowiązała Polskę do przedsięwzięcia wymaganych środków w terminie dwóch miesięcy od wpływu opinii. W efekcie Polska musi zapewnić pilną realizację ciążących na niej obowiązków.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Zgodnie z art. 23 rozporządzenia do dnia 7 czerwca 2024 r. Komisja Europejska dokona oceny rozporządzenia oraz przedstawi Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące jego stosowania.

Monitoring stosowania przepisów będzie prowadzony przez analizę:

a) liczby wydanych nakazów usunięcia oraz liczby przypadków usunięcia treści o charakterze terrorystycznym, a także szybkości, z jaką tego dokonano,
b) środków szczególnych podjętych na podstawie art. 5 rozporządzenia, w tym liczby przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkości, z jaką dokonano usunięcia lub uniemożliwiono dostępu,
c) liczby wniosków o dostęp, z którymi wystąpiły właściwe organy, w odniesieniu do treści zachowywanych przez dostawcę usług hostingowych na podstawie art. 6 rozporządzenia,
d) liczby wszczętych procedur rozpatrywania skarg oraz działań podjętych przez dostawców usług hostingowych na podstawie art. 10 rozporządzenia,
e) liczby wszczętych kontroli w postępowaniach administracyjnych lub sądowych oraz decyzji podjętych przez właściwy organ zgodnie z prawem krajowym.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

1. tabela zgodności
2. odwrócona tabela zgodności
3. raport z konsultacji

[5)] Sprawozdanie, o którym mowa w odnośniku nr 2.

Raport z konsultacji publicznych

projektu ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (UC 37)

1. Informacje ogólne

Projekt ustawy został zamieszczony, stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348, z późn. zm.) w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji.

2. Omówienie wyników konsultacji publicznych i opiniowania

Pismem z dnia 26 kwietnia 2024 r. Krajowa Izba Komunikacji Ethernetowej (KIKE) przedstawiła swoje stanowisko do projektu. Zgodnie z nim KIKE zgłasza zastrzeżenia do art. 2 projektu, który wprowadza zmiany do art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

W ocenie KIKE przedsiębiorcy telekomunikacyjni nie powinni być ujmowani w art. 32c ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, a tym samym zobowiązywani do usuwania lub blokowania danych informatycznych, o których mowa w tym przepisie. Powołując się na przepisy unijne, w tym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. *ustanawiające środki dotyczące dostępu do otwartego Internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenia (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii* KIKE stwierdza, że przedsiębiorcy telekomunikacyjni nie mają możliwości usuwania jakichkolwiek treści w systemie teleinformatycznym innych podmiotów, ponieważ nie mają takich uprawnień. Analogicznie przedsiębiorcy telekomunikacyjni nie mają możliwości blokowania dostępu do takich treści, a jedynie w wąskim zakresie mogą blokować dostęp do domeny internetowej, na której zakazane treści się znajdują. W swoim stanowisku KIKE podnosi brak przepisów konkretyzujących kwestie techniczne takiego obowiązku, co jest kluczowe do jego realizacji.

W związku z powyższym KIKE proponuje usunięcie z projektu art. 2 w całości, jako wykraczającego poza przepisy unijne jakie projekt ma wdrażać.

Projektodawca częściowo uwzględnił uwagę KIKE przez usunięcie z projektu przepisu nakładającego na przedsiębiorcę telekomunikacyjnego zobowiązania do usunięcia dostępności do określonych danych teleinformatycznych. Taki obowiązek będzie natomiast spoczywał na usługodawcy świadczącym usługi drogą elektroniczną. Przedsiębiorcy telekomunikacyjni będą zobligowani na żądanie sądu wyłącznie do blokowania dostępności określonych danych teleinformatycznych.

Należy zauważyć, że w art. 21 dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. *w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/WSiSW* wymaga się od państw członkowskich wprowadzenia środków zapewniających usuwanie lub blokowanie treści. W konsekwencji przepisy krajowe muszą się odnosić do treści. Nawiązując do praktyki jaka funkcjonuje w tym zakresie należy wskazać, że aktualnie w przypadku zarządzenia zablokowania dostępności w systemie teleinformatycznym określonych danych informatycznych, mających związek ze zdarzeniem o charakterze terrorystycznym lub usług teleinformatycznych służących lub wykorzystywanych

do spowodowania zdarzenia o charakterze terrorystycznym, wniosek Szefa Agencji Bezpieczeństwa Wewnętrznego w tym zakresie zawiera szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać zablokowaniu. Wynika to wprost z przepisów rozporządzenia Prezesa Rady Ministrów z dnia 18 lipca 2016 r. *w sprawie sposobu dokumentowania blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków* (Dz. U. poz. 1056). Analogiczne rozwiązania powinny być również wprowadzone w przypadku rozszerzenia zakresu przedmiotowego art. 32c ust. 1 ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.

Stanowisko przedstawiła również Polska Izba Informatyki i Telekomunikacji (PIIT), która w piśmie z dnia 24 czerwca 2024 r. (sygn. PIIT/595/24) zgłosiła zastrzeżenie do art. 2 projektu wprowadzającego zmiany do art. 32c ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,* w pierwszej kolejności wskazując, że projektowane zmiany do ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu uniemożliwią prawidłowe wykonanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. *w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*.

W odniesieniu do tej kwestii wskazać należy, że zmiany do ww. przepisu wynikają z potrzeby zapewnienia pełnej transpozycji art. 21 dyrektywy 2017/541 , który nakłada na państwa członkowskie obowiązek zapewnienia natychmiastowego usuwania treści internetowych publicznie nawołujących do popełnienia przestępstwa terrorystycznego, nie wskazując przy tym podmiotu zobowiązanego do usuwania takich treści. Z kolei rozporządzenie nakłada zobowiązania do usuwania treści o charakterze terrorystycznym wyłącznie na dostawców usług hostingowych, nie nakładając takich obowiązków na inne podmioty świadczące usługi drogą elektroniczną. W tym kontekście podkreślenia wymaga również to, że przepisy ww. dyrektywy nie zostały uchylone rozporządzeniem, co oznacza, że oba akty są względem siebie komplementarne i powinny być stosowane równolegle. Szczegółowo zostało to wyjaśnione w uzasadnieniu.

Ponadto wyjaśnić należy, że projektowana nowelizacja ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* nie koliduje również z pozostałymi przepisami unijnymi, w tym dyrektywą Parlamentu Europejskiego i Rady (UE) 2018/1972 ustanawiająca Europejski kodeks łączności elektronicznej. Należy wskazać, że prawo Unii Europejskiej tworzy oddzielny system regulacji dotyczących sieci i usług łączności elektronicznej oraz system regulacji dotyczących treści. Dyrektywa 2018/1972 należy do tej pierwszej kategorii i, jak wskazano w jej motywie 7, „nie obejmuje zatem zagadnień związanych z treścią usług świadczonych za pośrednictwem sieci łączności elektronicznej przy wykorzystaniu usług łączności elektronicznej". Znajduje to odzwierciedlenie także w art. 1 ust. 3 dyrektywy 2018/1972, który określa zakres wyłączeń (w zakresie blokowania treści terrorystycznych szczególnie istotne wydają się lit. b i c). W konsekwencji należy stwierdzić, że przepisy dyrektywy 2018/1972, w szczególności definicja „usługi łączności elektronicznej", nie mogą ograniczać przepisów prawa UE, dotyczących treści internetowych, jak art. 21 dyrektywy 2017/541. Przepis ten nakłada na państwa członkowskie obowiązek podjęcia środków zapewniających blokadę dostępności wskazanych treści. W konsekwencji przyjęcie rozwiązania, które wyłączałoby ten obowiązek wobec pewnej grupy podmiotów, mających techniczne możliwości w tym zakresie, stanowiłoby nieprawidłowe wdrożenie dyrektywy 2017/541 do polskiego porządku prawnego.

W swoim stanowisku PIIT wskazuje też, że cyt.: „Jednocześnie w dalszej części zmienianego art. 32c brakuje szczegółowych i precyzyjnych przepisów, wskazujących w jaki sposób (technicznie) przedsiębiorca telekomunikacyjny ma zablokować w swoim systemie teleinformatycznym dostępność

określonych danych informatycznych mających związek ze zdarzeniami o charakterze terrorystycznym lub uprawdopodabniającym.”.

Wobec powyższego niezbędne jest wyjaśnienie, że tego typu „uszczegółowienia techniczne” nie stanowią materii ustawowej i w związku z tym nie mogą być regulowane aktem prawnym tej rangi. Przywoływany z kolei przez PIIT art. 15f ustawy *o grach hazardowych*, jako przykład regulacji, która określa możliwości techniczne przedsiębiorców telekomunikacyjnych zablokowania takiej dostępności nie określa tak naprawdę szczegółowego sposobu takich technicznych kwestii. Wskazuje natomiast, że przedsiębiorcy telekomunikacyjni świadczący usługi dostępu do sieci Internet są ustawowo obowiązani do m.in. uniemożliwienia dostępu do określonych stron internetowych.

Ponadto w uzupełnieniu do powyższego wyjaśnić należy, że prawidłowe wykonanie projektowanych przepisów wdrażających dyrektywę 2017/541 będzie zapewnione w sposób analogiczny, jak ma to miejsce już w odniesieniu do obowiązujących przepisów ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*. Nawiązując do praktyki, jaka funkcjonuje w tym zakresie, należy wskazać, że aktualnie w przypadku zarządzenia zablokowania dostępności w systemie teleinformatycznym określonych danych informatycznych, mających związek ze zdarzeniem o charakterze terrorystycznym lub usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym, wniosek Szefa Agencji Bezpieczeństwa Wewnętrznego w tym zakresie zawiera szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać zablokowaniu. Wynika to wprost z przepisów rozporządzenia Prezesa Rady Ministrów z dnia 18 lipca 2016 r. *w sprawie sposobu dokumentowania blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków*. Analogiczne rozwiązania będą wprowadzone w przypadku rozszerzenia zakresu przedmiotowego art. 32c ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zgodnie z projektowaną nowelizacją.

3. Przedstawienie wyników zasięgnięcia opinii, dokonania konsultacji albo uzgodnienia projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym

Projekt ustawy nie wymagał zasięgnięcia opinii, dokonania konsultacji ani uzgodnienia projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym.

4. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa, wraz ze wskazaniem kolejności dokonania zgłoszeń albo informację o ich braku

Nie odnotowano zgłoszeń zainteresowanych podmiotów w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa.

Tabela zgodności

Tytuł projektu	Projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (UC37)
Tytuł wdrażanego aktu prawnego/ wdrażanych aktów prawych	**1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym;** **2) dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/WSiSW.**
wyjaśnienie terminu wejścia w życie projektu	Ze względu na wyznaczony w art. 24 rozporządzenia 2021/784 termin jego stosowania (od dnia 7 czerwca 2022 r.) ustawa wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Jedn. redakcyjna	Treść przepisu UE	Konieczność wdrożenia T/N	Jedn. redakcyjna	Treść przepisu projektu ustawy	Uzasadnienie
rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym					
Artykuł 1 Przedmiot i zakres stosowania	1. W niniejszym rozporządzeniu ustanawia się jednolite przepisy w celu przeciwdziałania wykorzystywaniu usług hostingowych do publicznego rozpowszechniania w internecie treści o charakterze terrorystycznym, w szczególności przepisy dotyczące: a) rozsądnych i proporcjonalnych obowiązków w zakresie staranności, których mają przestrzegać dostawcy usług hostingowych w celu przeciwdziałania publicznemu rozpowszechnianiu treści o charakterze terrorystycznym za pośrednictwem ich usług oraz zapewnienia, w razie potrzeby, niezwłocznego usuwania tych treści lub uniemożliwiania dostępu do nich; b) środków, które mają wdrożyć państwa członkowskie – zgodnie z prawem Unii i z zastrzeżeniem odpowiednich gwarancji w zakresie ochrony praw podstawowych, w szczególności wolności wypowiedzi i informacji w otwartym i demokratycznym społeczeństwie – w celu: (i) identyfikowania treści o charakterze terrorystycznym oraz zapewnienia ich niezwłocznego usuwania przez dostawców usług hostingowych; oraz (ii) ułatwienia współpracy między właściwymi organami państw członkowskich, dostawcami usług hostingowych oraz, w stosownych przypadkach, z Europolem.	N			

	2. Niniejsze rozporządzenie stosuje się do dostawców usług hostingowych oferujących usługi w Unii – niezależnie od miejsca ich głównej jednostki organizacyjnej – w zakresie, w jakim publicznie rozpowszechniają informacje. 3. Materiałów publicznie rozpowszechnianych w celach edukacyjnych, dziennikarskich, artystycznych lub badawczych lub w celach zapobiegania terroryzmowi lub zwalczania terroryzmu, w tym materiałów służących wyrażaniu polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej, nie uznaje się za treści o charakterze terrorystycznym. W drodze oceny ustala się, jaki jest rzeczywisty cel danego rozpowszechniania i czy materiały są publicznie rozpowszechniane do tych celów. 4. Niniejsze rozporządzenie nie ma wpływu na obowiązek poszanowania praw, wolności i zasad, o których mowa w art. 6 TUE, i stosuje się je bez uszczerbku dla podstawowych zasad odnoszących się do wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów. 5. Niniejsze rozporządzenie pozostaje bez uszczerbku dla dyrektyw 2000/31/WE i 2010/13/UE. W odniesieniu do audiowizualnych usług medialnych zdefiniowanych w art. 1 pkt 1 lit. a) dyrektywy 2010/13/UE pierwszeństwo ma dyrektywa 2010/13/UE.				
Artykuł 2 Definicje	Do celów niniejszego rozporządzenia stosuje się następujące definicje: 1) „dostawca usług hostingowych” oznacza dostawcę usług zdefiniowanych w art. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (14), polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek; 2) „dostawca treści” oznacza użytkownika, który dostarczył informacje, które są lub były przechowywane i publiczne rozpowszechnianie przez dostawcę usług hostingowych; 3) „publiczne rozpowszechnianie” oznacza udostępnianie informacji, na wniosek dostawcy treści, potencjalnie nieograniczonej liczbie osób; 4) „oferowanie usług w Unii” oznacza umożliwianie osobom fizycznym lub prawnym w co najmniej jednym państwie członkowskim korzystania z usług dostawcy usług hostingowych, którego łączy z danym państwem członkowskim istotny związek;	T	Art. 1 pkt 1 projektu ustawy dot. art. 2 pkt 8 – 10 ustawy o działaniach antyterrorystycznych	Art. 2. 8) dostawcy usług hostingowych – należy przez to rozumieć dostawcę usług, polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek, o którym mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79), zwanego dalej „rozporządzeniem 2021/784”; 9) dostawcy treści – należy przez to rozumieć użytkownika, o którym mowa w art. 2 pkt 2 rozporządzenia 2021/784;	

	5) „istotny związek” oznacza związek dostawcy usług hostingowych z co najmniej jednym państwem członkowskim, wynikający z posiadania jednostki organizacyjnej w Unii albo ze szczególnych kryteriów faktycznych, takich jak: a) posiadanie znacznej liczby użytkowników jego usług w co najmniej jednym państwie członkowskim; lub b) kierowanie jego działalności do co najmniej jednego państwa członkowskiego; 6) „przestępstwa terrorystyczne” oznaczają przestępstwa zdefiniowane w art. 3 dyrektywy (UE) 2017/541; 7) „treści o charakterze terrorystycznym” oznaczają materiały co najmniej jednego z poniższych rodzajów; a mianowicie materiały, które: a) podżegają do popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541, w przypadku gdy takie materiały, bezpośrednio lub pośrednio, na przykład poprzez pochwalanie aktów terrorystycznych, popierają popełnianie przestępstw terrorystycznych i tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw; b) nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541; c) nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej, w rozumieniu art. 4 lit. b) dyrektywy (UE) 2017/541; d) udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia jednego z przestępstw terrorystycznych, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541; e) stwarzają zagrożenie popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541; 8) „warunki umowne” oznaczają wszystkie warunki i klauzule umowne, niezależnie od ich nazwy lub formy, które regulują			10) treściach o charakterze terrorystycznym – należy przez to rozumieć materiały, o których mowa w art. 2 pkt 7 rozporządzenia 2021/784.	

	stosunek umowny między dostawcą usług hostingowych a jego użytkownikami; 9) „główna jednostka organizacyjna” oznacza siedzibę główną lub siedzibę statutową dostawcy usług hostingowych, w której wykonywane są główne funkcje finansowe i sprawowana jest kontrola operacyjna.				
Artykuł 3 Nakazy usunięcia	1. Właściwy organ każdego państwa członkowskiego jest uprawniony do wydania nakazu usunięcia zobowiązującego dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich. 2. W przypadku gdy właściwy organ nie wydał uprzednio dostawcy usług hostingowych nakazu usunięcia, udziela on temu dostawcy usług hostingowych informacji o mających zastosowanie procedurach i terminach co najmniej 12 godzin przed wydaniem nakazu usunięcia. Akapitu pierwszego nie stosuje się w należycie uzasadnionych przypadkach wyjątkowych. 3. Dostawcy usług hostingowych usuwają treści o charakterze terrorystycznym lub uniemożliwiają dostęp do treści terrorystycznych we wszystkich państwach członkowskich jak najszybciej, a w każdym razie nie później niż w ciągu jednej godziny od otrzymania nakazu usunięcia. 4. Właściwe organy wydają nakazy usunięcia przy użyciu wzoru określonego w załączniku I. Nakazy usunięcia zawierają następujące elementy: a) dane identyfikacyjne właściwego organu wydającego nakaz usunięcia i potwierdzenie autentyczności nakazu usunięcia przez ten właściwy organ; b) wystarczająco szczegółowe uzasadnienie wyjaśniające, dlaczego dane treści uznano za treści o charakterze terrorystycznym oraz wskazanie odpowiedniego rodzaju materiałów, o których mowa w art. 2 pkt 7; c) dokładny ujednolicony format adresowania zasobów (adres URL) oraz, w razie potrzeby, dodatkowe informacje służące identyfikacji treści o charakterze terrorystycznym; d) wskazanie niniejszego rozporządzenia jako podstawy prawnej nakazu usunięcia;	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a i art. 26d ust. 1 i 3 ustawy o działaniach antyterrorystycznych	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784. Art. 26d. 1. Nakaz usunięcia lub stwierdzenie naruszenia, o których mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej. Do postępowań w tych sprawach w zakresie nieuregulowanym w rozporządzeniu 2021/784 i niniejszej ustawie, stosuje się przepisy art. 6, art. 7, art. 7b, art. 8, art. 12, art. 14, art. 16, art. 24, art. 26 § 1 i 2, art. 28–30, art. 32, art. 33, art. 35 § 1, art. 50, art. 54–56, art. 63–65, art. 72, art. 75 § 1, art. 77, art. 97 § 1 pkt 4 i § 2, art. 104, art. 105 § 1, art. 112, art. 113 § 1, art. 156-158, art. 217 oraz art. 268a ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572). 3. Decyzje, o których mowa w ust. 1 i 2, są ostateczne i podlegają natychmiastowemu wykonaniu.	

	e) data, znacznik czasu i podpis elektroniczny właściwego organu wydającego nakaz usunięcia; f) łatwo zrozumiałe informacje na temat środków zaskarżenia przysługujących dostawcy usług hostingowych i dostawcy treści, w tym informacje na temat środków zaskarżenia do właściwego organu, możliwości wniesienia sprawy do sądu, wraz z terminami do wniesienia środków zaskarżenia; g) gdy jest to konieczne i proporcjonalne – decyzja o nieujawnianiu informacji o usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich zgodnie z art. 11 ust. 3. 5. Właściwy organ kieruje nakaz usunięcia do głównej jednostki organizacyjnej dostawcy usług hostingowych lub do jego przedstawiciela prawnego wyznaczonego zgodnie z art. 17. Właściwy organ przekazuje nakaz usunięcia punktowi kontaktowemu, o którym mowa w art. 15 ust. 1, za pomocą środków elektronicznych dających możliwość sporządzenia pisemnego potwierdzenia na warunkach, które umożliwiają ustalenie autentyczności nadawcy, w tym podanie dokładnej daty oraz godziny wysłania i otrzymania nakazu. 6. Dostawcy usług hostingowych bez zbędnej zwłoki informują właściwy organ, przy użyciu wzoru określonego w załączniku II, o usunięciu treści o charakterze terrorystycznym lub o uniemożliwieniu dostępu do treści terrorystycznych we wszystkich państwach członkowskich, wskazując w szczególności czas tego usunięcia lub uniemożliwienia dostępu. 7. Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu usunięcia ze względu na siłę wyższą lub faktyczną niemożliwość, których nie można przypisać dostawcy usług hostingowych, w tym z dających się obiektywnie uzasadnić przyczyn technicznych lub operacyjnych, informuje bez zbędnej zwłoki właściwy organ, który wydał nakaz usunięcia, o tych powodach, przy użyciu wzoru określonego w załączniku III. Termin określony w ust. 3 zaczyna biec od momentu, gdy ustaną powody, o których mowa w akapicie pierwszym niniejszego ustępu. 8. Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu usunięcia, ponieważ zawiera on oczywiste błędy lub nie zawiera informacji wystarczających do jego wykonania, informuje				

	o tym bez zbędnej zwłoki właściwy organ, który wydał nakaz usunięcia, zwracając się o niezbędne wyjaśnienia, przy użyciu wzoru określonego w załączniku III. Termin określony w ust. 3 zaczyna biec od momentu, gdy dostawca usług hostingowych otrzymał niezbędne wyjaśnienia. 9. Nakaz usunięcia staje się ostateczny po upływie terminu do wniesienia środka zaskarżenia, w przypadku gdy nie został on wniesiony zgodnie z prawem krajowym albo na skutek utrzymania nakazu usunięcia w wyniku wniesienia środka zaskarżenia. Kiedy nakaz usunięcia stanie się ostateczny, właściwy organ, który wydał nakaz usunięcia, informuje o tym właściwy organ, o którym mowa w art. 12 ust. 1 lit. c), państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę.				
Artykuł 4 Procedura dotycząca transgranicznych nakazów usunięcia	1. Z zastrzeżeniem art. 3, w przypadku gdy dostawca usług hostingowych nie ma głównej jednostki organizacyjnej ani przedstawiciela prawnego w państwie członkowskim właściwego organu, który wydał nakaz usunięcia, organ ten przekazuje jednocześnie kopię nakazu usunięcia właściwemu organowi państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę. 2. W przypadku gdy dostawca usług hostingowych otrzymuje nakaz usunięcia, o którym mowa w niniejszym artykule, podejmuje środki przewidziane w art. 3 oraz podejmuje niezbędne środki, by móc przywrócić treści lub dostęp do nich, zgodnie z ust. 7 niniejszego artykułu. 3. Właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, może z własnej inicjatywy – w ciągu 72 godzin od otrzymania kopii nakazu usunięcia zgodnie z ust. 1 – dokonać weryfikacji tego nakazu, aby ustalić, czy nakaz ten nie narusza w sposób poważny lub oczywisty niniejszego rozporządzenia lub praw podstawowych i wolności gwarantowanych w Karcie. W przypadku stwierdzenia takiego naruszenia, podejmuje w tej sprawie decyzję wraz z uzasadnieniem, w tym samym terminie.	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a i art. 26d ust. 1 i 3 ustawy o działaniach antyterrorystycznych	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784. Art. 26d. 1. Nakaz usunięcia lub stwierdzenie naruszenia, o których mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej. Do postępowań w tych sprawach w zakresie nieuregulowanym w rozporządzeniu 2021/784 i niniejszej ustawie, stosuje się przepisy art. 6, art. 7, art. 7b, art. 8, art. 12, art. 14, art. 16, art. 24, art. 26 § 1 i 2, art. 28–30, art. 32, art. 33, art. 35 § 1, art. 50, art. 54–56, art. 63–65, art. 72, art. 75 § 1, art. 77, art. 97 § 1 pkt 4 i § 2, art. 104, art. 105 § 1, art. 112, art. 113 § 1, art. 156-158, art. 217 oraz art. 268a ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572). 3. Decyzje, o których mowa w ust. 1 i 2, są ostateczne i podlegają natychmiastowemu wykonaniu.	

	4. Dostawcy usług hostingowych i dostawcy treści mają prawo wystąpienia – w ciągu 48 godzin od otrzymania nakazu usunięcia albo informacji, o których mowa w art. 11 ust. 2 – do właściwego organu państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, z wnioskiem wraz z uzasadnieniem o przeprowadzenie weryfikacji, o której mowa w ust. 3 akapit pierwszy niniejszego artykułu. W ciągu 72 godzin od otrzymania wniosku właściwy organ podejmuje w wyniku przeprowadzonej weryfikacji nakazu usunięcia decyzję wraz z uzasadnieniem, przedstawiając swoje ustalenia odnośnie do tego, czy doszło do naruszenia. 5. Przed podjęciem decyzji na podstawie ust. 3 akapit drugi lub decyzji stwierdzającej naruszenie na podstawie ust. 4 akapit drugi, właściwy organ informuje właściwy organ, który wydał nakaz usunięcia, o zamiarze podjęcia decyzji i o jej powodach. 6. W przypadku gdy właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, podejmuje decyzję wraz z uzasadnieniem na podstawie ust. 3 lub 4 niniejszego artykułu, niezwłocznie powiadamia o tej decyzji właściwy organ, który wydał nakaz usunięcia, dostawcę usług hostingowych, dostawcę treści, który wystąpił o przeprowadzenie weryfikacji na podstawie ust. 4 niniejszego artykułu, oraz – zgodnie z art. 14 – Europol. Jeżeli w decyzji stwierdza się naruszenie na podstawie ust. 3 lub 4 niniejszego artykułu, nakaz usunięcia przestaje wywoływać skutki prawne. 7. Po otrzymaniu decyzji stwierdzającej naruszenie, o której powiadomiono zgodnie z ust. 6, dostawca usług hostingowych natychmiast przywraca dane treści lub dostęp do nich, bez uszczerbku dla możliwości egzekwowania swoich warunków umownych zgodnie z prawem Unii i prawem krajowym.				
Artykuł 5 Środki szczególne	1. Dostawca usług hostingowych narażony na treści o charakterze terrorystycznym zgodnie z ust. 4 zamieszcza, w stosownych przypadkach, w swoich warunkach umownych oraz stosuje postanowienia mające przeciwdziałać wykorzystywaniu jego usług	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a, art. 26c	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784. Art. 26c. 1. Szef ABW sprawuje nadzór nad wdrażaniem środków, o których mowa	

	do publicznego rozpowszechniania treści o charakterze terrorystycznym. Działa on przy tym z zachowaniem należytej staranności, w sposób proporcjonalny i niedyskryminacyjny, odpowiednio uwzględniając we wszystkich okolicznościach prawa podstawowe użytkowników i mając na uwadze, w szczególności, zasadnicze znaczenie wolności wypowiedzi i informacji w otwartym i demokratycznym społeczeństwie, tak aby uniknąć usuwania materiałów, które nie stanowią treści o charakterze terrorystycznym. 2. Dostawca usług hostingowych narażony na treści o charakterze terrorystycznym zgodnie z ust. 4 podejmuje środki szczególne w celu ochrony swoich usług przed publicznym rozpowszechnianiem treści o charakterze terrorystycznym. Decyzja co do wyboru środków szczególnych pozostaje w gestii dostawcy usług hostingowych. Środki takie mogą obejmować co najmniej jeden z następujących środków: a) odpowiednie techniczne i operacyjne środki lub zdolności, takie jak odpowiedni personel lub środki techniczne do celów identyfikowania i niezwłocznego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich; b) łatwo dostępne i przyjazne dla użytkownika mechanizmy umożliwiające użytkownikom zgłaszanie lub sygnalizowanie dostawcy usług hostingowych domniemanych treści o charakterze terrorystycznym; c) inne mechanizmy zwiększające świadomość na temat dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług, takie jak mechanizmy służące moderowaniu użytkowników; d) inne środki, które dostawca usług hostingowych uzna za stosowne, by przeciwdziałać dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług. 3. Środki szczególne muszą spełniać wszystkie następujące wymogi: a) skutecznie zmniejszać poziom narażenia usług dostawcy usług hostingowych na treści o charakterze terrorystycznym; b) być ukierunkowane i proporcjonalne, uwzględniając w szczególności, jak duży jest poziom narażenia usług dostawcy usług hostingowych na treści o charakterze terrorystycznym,		i art. 26d ust. 2 i 3 ustawy o działaniach antyterrorystycznych	w art. 5 ust. 1-3 rozporządzenia 2021/784, przez: 1) dokonywanie kontroli środków szczególnych, które podjął dostawca usług hostingowych, w tym pod kątem ich zgodności z art. 5 ust. 2 i 3 rozporządzenia 2021/784; 2) wydawanie dostawcy usług hostingowych pisemnych zaleceń, mających na celu usunięcie stwierdzonych nieprawidłowości i dostosowanie jego działalności do przepisów rozporządzenia 2021/784. 2. Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego przeprowadzając czynności, o których mowa w ust. 1, ma prawo: 1) wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych; 2) żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia bądź wglądu w dokumentację techniczną i operacyjną wynikającą ze stosowania środków szczególnych. 3. Naruszenia przepisów prawa i nieprawidłowości stwierdzone w ramach nadzoru, usuwa dostawca usług hostingowych narażony na treści o charakterze terrorystycznym w terminie określonym w zaleceniu. Art. 26d. 2. Wskazywanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, o których mowa w art. 5 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej.	

	a także zdolności techniczne i operacyjne, kondycję finansową, liczbę użytkowników usług dostawcy usług hostingowych oraz ilość dostarczanych przez nich treści; c) być stosowane w sposób, który uwzględnia pełne poszanowanie praw i uzasadnionego interesu użytkowników, w szczególności podstawowych praw użytkowników dotyczących wolności wypowiedzi i informacji, poszanowania życia prywatnego i ochrony danych osobowych; d) być stosowane w staranny i niedyskryminacyjny sposób. W przypadku gdy środki szczególne wiążą się ze stosowaniem środków technicznych, wprowadza się odpowiednie i skuteczne zabezpieczenia, w szczególności poprzez nadzór i weryfikację dokonywane przez człowieka, aby zapewnić dokładność i uniknąć usuwania materiałów, które nie stanowią treści o charakterze terrorystycznym. 4. Dostawca usług hostingowych jest narażony na treści o charakterze terrorystycznym, w przypadku gdy właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę: a) podjął decyzję, opartą na obiektywnych czynnikach, takich jak fakt otrzymania przez dostawcę co najmniej dwóch ostatecznych nakazów usunięcia w ciągu ostatnich 12 miesięcy, w której stwierdził, że dostawca usług hostingowy jest narażony na treści o charakterze terrorystycznym; oraz b) powiadomił dostawcę usług hostingowych o decyzji, o której mowa w lit. a). 5. Po otrzymaniu decyzji, o której mowa w ust. 4, lub, w stosownych przypadkach, w ust. 6, dostawca usług hostingowych powiadamia właściwy organ o środkach szczególnych, które podjął i które zamierza podjąć w celu zapewnienia zgodności z ust. 2 i 3. Dostawca usług hostingowych dokonuje tego powiadomienia w terminie trzech miesięcy od otrzymania decyzji, a następnie raz do roku. Obowiązek ten ustaje po podjęciu przez właściwy organ decyzji, na wniosek zgodnie z ust. 7, że dostawca usług hostingowych nie jest już narażony na treści o charakterze terrorystycznym.			Do postępowań w tych sprawach stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, o których mowa w ust. 1, oraz art. 107 tej ustawy. 3. Decyzje, o których mowa w ust. 1 i 2, są ostateczne i podlegają natychmiastowemu wykonaniu.	

	6. Jeżeli na podstawie dokonanego powiadomienia, o którym mowa w ust. 5, i w oparciu o, w stosownych przypadkach, inne obiektywne czynniki właściwy organ uzna, że podjęte środki szczególne nie są zgodne z wymogami ust. 2 i 3, organ ten kieruje do dostawcy usług hostingowych decyzję zobowiązującą go do podjęcia niezbędnych środków w celu zapewnienia zgodności z ust. 2 i 3. Dostawca usług hostingowych może wybrać, jaki rodzaj środków szczególnych podejmie. 7. Dostawca usług hostingowych może w dowolnym momencie zwrócić się do właściwego organu o dokonanie przeglądu oraz, w stosownych przypadkach, o zmianę lub uchylenie decyzji, o której mowa w ust. 4 lub 6. W terminie trzech miesięcy od otrzymania wniosku właściwy organ, w oparciu o obiektywne czynniki, podejmuje decyzję wraz z uzasadnieniem w sprawie tego wniosku i powiadamia o niej dostawcę usług hostingowych. 8. Wymóg podjęcia środków szczególnych pozostaje bez uszczerbku dla art. 15 ust. 1 dyrektywy 2000/31/WE i nie pociąga za sobą ogólnego obowiązku w zakresie nadzoru przez dostawców usług hostingowych przekazywanych lub przechowywanych przez nich informacji ani ogólnego obowiązku aktywnego poszukiwania faktów lub okoliczności wskazujących na bezprawną działalność. Wymóg podjęcia środków szczególnych nie obejmuje obowiązku stosowania przez dostawcę usług hostingowych zautomatyzowanych narzędzi.				
Artykuł 6 Zachowanie treści i związanych z nimi danych	1. Dostawcy usług hostingowych zachowują treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku nakazu usunięcia lub środków szczególnych na podstawie art. 3 lub 5, jak również związane z nimi dane, które zostały usunięte w wyniku usunięcia takich treści o charakterze terrorystycznym, które to treści i dane są konieczne do: a) kontroli w postępowaniach administracyjnych lub sądowych lub rozpatrywania skarg na podstawie art. 10 w przypadku decyzji o usunięciu treści o charakterze terrorystycznym i związanych z nimi danych lub o uniemożliwieniu do nich dostępu; lub	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a ustawy o działaniach antyterrorystycznych	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.	

	b) zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. 2. Treści o charakterze terrorystycznym i związane z nimi dane, o których mowa w ust. 1, zachowuje się przez okres sześciu miesięcy od usunięcia lub uniemożliwienia dostępu do nich. Treści o charakterze terrorystycznym są, na wniosek właściwego organu lub sądu, zachowywane przez kolejny określony okres wyłącznie wtedy, jeżeli jest to konieczne i tak długo, jak jest to konieczne do celów trwającej kontroli w postępowaniach administracyjnych lub sądowych, o których mowa w ust. 1 lit. a). 3. Dostawcy usług hostingowych zapewniają, aby treści o charakterze terrorystycznym i związane z nimi dane zachowane na podstawie ust. 1 podlegały odpowiednim zabezpieczeniom technicznym i organizacyjnym. Przedmiotowe zabezpieczenia techniczne i organizacyjne zapewniają, by dostęp do zachowanych treści o charakterze terrorystycznym i związanych z nimi danych oraz ich przetwarzanie odbywały się wyłącznie do celów, o których mowa w ust. 1, oraz zapewniają wysoki poziom ochrony odnośnych danych osobowych. W razie potrzeby dostawcy usług hostingowych dokonują przeglądu i aktualizacji tych zabezpieczeń.				
Artykuł 7 Obowiązki dostawców usług hostingowych w zakresie przejrzystości	1. Dostawcy usług hostingowych określają w swoich warunkach umownych w sposób jasny swoje zasady dotyczące przeciwdziałania rozpowszechnianiu treści o charakterze terrorystycznym, w tym, w stosownych przypadkach, rzeczowe wyjaśnienie funkcjonowania środków szczególnych, w tym, w stosownych przypadkach, stosowania zautomatyzowanych narzędzi. 2. Dostawca usług hostingowych, który w danym roku kalendarzowym podjął działania mające na celu przeciwdziałanie rozpowszechnianiu treści o charakterze terrorystycznym lub został zobowiązany do podjęcia działań na podstawie niniejszego rozporządzenia, udostępnia publicznie ogólnie dostępne sprawozdanie z przejrzystości na temat tych działań za ten rok. Publikuje on to sprawozdanie przed dniem 1 marca kolejnego roku.	N			Przepis stosuje się wprost

	3. Sprawozdania z przejrzystości zawierają co najmniej następujące informacje: a) informacje na temat środków wprowadzonych przez dostawcę usług hostingowych w związku z identyfikacją i usunięciem treści o charakterze terrorystycznym lub uniemożliwieniem dostępu do nich; b) informacje na temat środków wprowadzonych przez dostawcę usług hostingowych w celu przeciwdziałania ponownemu pojawianiu się w internecie materiałów, które wcześniej zostały usunięte lub do których dostęp został uniemożliwiony, ponieważ zostały one uznane za treści o charakterze terrorystycznym, w szczególności w przypadkach, w których zastosowano zautomatyzowane narzędzia; c) liczbę przypadków usunięcia treści o charakterze terrorystycznym lub przypadków uniemożliwienia dostępu do takich treści w wyniku nakazów usunięcia lub środków szczególnych oraz liczbę nakazów usunięcia, w przypadku których treści nie zostały usunięte lub dostęp do treści nie został uniemożliwiony na podstawie art. 3 ust. 7 akapit pierwszy i art. 3 ust. 8 akapit pierwszy, wraz z powodami, dla których tak się stało; d) liczbę skarg rozpatrzonych przez dostawcę usług hostingowych zgodnie z art. 10 i ich wynik; e) liczbę i wynik kontroli w postępowaniach administracyjnych lub sądowych wszczętych przez dostawcę usług hostingowych; f) liczbę przypadków, w których dostawca usług hostingowych został zobowiązany do przywrócenia treści lub przywrócenia dostępu do nich w wyniku kontroli w postępowaniach administracyjnych lub sądowych; g) liczbę przypadków, w których dostawca usług hostingowych przywrócił treści lub dostęp do nich na skutek skargi dostawcy treści.				
Artykuł 8 Sprawozdania właściwych organów z przejrzystości	1. Właściwe organy publikują roczne sprawozdania z przejrzystości dotyczące ich działalności prowadzonej na podstawie niniejszego rozporządzenia. Sprawozdania te zawierają co najmniej następujące informacje dotyczące danego roku kalendarzowego: a) liczba nakazów usunięcia wydanych na podstawie art. 3, ze wskazaniem liczby nakazów usunięcia podlegających art. 4 ust. 1 oraz liczby nakazów usunięcia zweryfikowanych na podstawie	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a ustawy o działaniach	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.	

	art. 4, oraz informacje dotyczące wykonania tych nakazów usunięcia przez dostawców usług hostingowych, w tym liczba przypadków, w których treści o charakterze terrorystycznym zostały usunięte lub dostęp do takich treści został uniemożliwiony oraz liczba przypadków, w których treści o charakterze terrorystycznym nie zostały usunięte ani dostęp do nich nie został uniemożliwiony; b) liczba decyzji podjętych zgodnie z art. 5 ust. 4, 6 lub 7 i informacje dotyczące wykonania tych decyzji przez dostawców usług hostingowych, w tym opis środków szczególnych; c) liczba przypadków, w których nakazy usunięcia i decyzje podjęte zgodnie z art. 5 ust. 4 i 6 stanowiły przedmiot kontroli w postępowaniach administracyjnych lub sądowych, i informacje na temat wyniku odpowiednich postępowań; d) liczba decyzji nakładających kary na podstawie art. 18 oraz opis rodzaju nałożonej kary. 2. Roczne sprawozdania z przejrzystości, o których mowa w ust. 1, nie zawierają informacji, które mogłyby narazić na szwank bieżącą działalność służącą zapobieganiu przestępstwom terrorystycznym, ich wykrywaniu, prowadzeniu postępowań przygotowawczych w ich sprawie i ich ściganiu lub na interesy bezpieczeństwa narodowego.		antyterrorystycznych		
Artykuł 9 Środki prawne	1. Dostawcy usług hostingowych, którzy otrzymali nakaz usunięcia wydany na podstawie art. 3 ust. 1 lub decyzję na podstawie art. 4 ust. 4 lub art. 5 ust. 4, 6 lub 7, mają prawo do skutecznego środka prawnego. Prawo to obejmuje prawo do zaskarżenia takiego nakazu usunięcia przed sądami państwa członkowskiego właściwego organu, który wydał dany nakaz usunięcia, oraz prawo do zaskarżenia decyzji na podstawie art. 4 ust. 4 lub art. 5 ust. 4, 6 lub 7 przed sądami państwa członkowskiego właściwego organu, który podjął daną decyzję. 2. Dostawcy treści, w przypadku gdy ich treści zostały usunięte lub dostęp do ich treści został uniemożliwiony w wyniku nakazu usunięcia, mają prawo do skutecznego środka prawnego. Prawo to obejmuje prawo do zaskarżenia nakazu usunięcia wydanego na podstawie art. 3 ust. 1 przed sądami państwa członkowskiego właściwego organu, który wydał dany nakaz usunięcia, oraz prawo do zaskarżenia decyzji na podstawie art. 4 ust. 4 przed sądami	T	Art. 1 pkt 2 projektu ustawy dot. art. 26d ust. 4 – 7 ustawy o działaniach antyterrorystycznych	Art. 26d. 4. Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał nakaz usunięcia lub dostawcy treści, którego treści obejmuje nakaz usunięcia, przysługuje prawo do wniesienia na ten nakaz skargi do sądu administracyjnego w terminie 30 dni od dnia: 1) jego dostarczenia w trybie, o którym mowa w art. 3 ust. 5 rozporządzenia 2021/784 - w przypadku dostawcy usług hostingowych; 2) otrzymania informacji, o której mowa w art. 11 ust. 1 rozporządzenia 2021/784 - w przypadku dostawcy treści. 5. Dostawcy usług hostingowych lub dostawcy treści, w stosunku do którego Szef ABW wydał	

	państwa członkowskiego właściwego organu, który podjął daną decyzję. 3. Państwa członkowskie wprowadzają skuteczne procedury korzystania z praw, o których mowa w niniejszym artykule.			decyzję, o której mowa w art. 4 ust. 4 rozporządzenia 2021/784, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego w terminie 30 dni od dnia otrzymania powiadomienia o tej decyzji. 6. Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał decyzję, o której mowa w art. 5 ust. 4, 6 lub 7 rozporządzenia 2021/784, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego. 7. Skargi, o których mowa w ust. 4 - 6, mogą być rozpoznawane w trybie uproszczonym, o którym mowa w art. 120 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2024 r. poz. 935), o ile strona nie zawnioskuje o przeprowadzenie rozprawy, a sąd uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione i przeprowadzenie rozprawy jest zbędne. Przepis art. 122 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi stosuje się.	
Artykuł 10 Mechanizm rozpatrywania skarg	1. Dostawca usług hostingowych ustanawia skuteczny i dostępny mechanizm umożliwiający dostawcom treści, w przypadku gdy ich treści zostały usunięte lub dostęp do ich treści został uniemożliwiony w wyniku środków szczególnych na podstawie art. 5, złożenie skargi dotyczącej danego usunięcia lub uniemożliwienia dostępu z żądaniem przywrócenia treści lub dostępu do nich. 2. Dostawca usług hostingowych rozpatruje bez zbędnej zwłoki wszelkie skargi, jakie otrzymał za pośrednictwem mechanizmu, o którym mowa w ust. 1, i bez zbędnej zwłoki przywraca treści lub dostęp do nich, w przypadku gdy ich usunięcie lub uniemożliwienie dostępu do nich było nieuzasadnione. Informuje on skarżącego	N			Przepis stosuje się wprost. W odniesieniu do ust. 2 zdanie trzecie zastosowanie mają przepisy Kodeksu postępowania administracyjnego i Prawa o postępowaniu przed sądem

	o wyniku rozpatrzenia skargi w terminie dwóch tygodni od jej otrzymania. W przypadku odrzucenia skargi dostawca usług hostingowych informuje skarżącego o powodach swojej decyzji. Przywrócenie treści lub dostępu do nich nie wyklucza kontroli w postępowaniach administracyjnych lub sądowych zaskarżonej decyzji dostawcy usług hostingowych lub właściwego organu.				administracyjnym w odniesieniu do decyzji właściwego organu oraz przepisy regulujące sprawy cywilne (Kodeks cywilny oraz Kodeks postępowania cywilnego) w odniesieniu do decyzji dostawcy usług hostingowych.
Artykuł 11 Informacje dla dostawców treści	1. W przypadku gdy dostawca usług hostingowych usuwa treści o charakterze terrorystycznym lub uniemożliwia dostęp do nich, udostępnia on dostawcy treści informacje na temat takiego usunięcia lub uniemożliwienia dostępu. 2. Na wniosek dostawcy treści dostawca usług hostingowych informuje go o powodach usunięcia lub uniemożliwienia dostępu oraz o jego prawach do zaskarżenia nakazu usunięcia albo udostępnia dostawcy treści kopię nakazu usunięcia. 3. Obowiązek na podstawie ust. 1 i 2 nie ma zastosowania, jeżeli właściwy organ wydający nakaz usunięcia zdecyduje, że jest konieczne i proporcjonalne, aby nie ujawniać informacji ze względów bezpieczeństwa publicznego, takich jak zapobieganie przestępstwom terrorystycznym, prowadzenie postępowań przygotowawczych w ich sprawie, wykrywanie i ściganie takich przestępstw, tak długo, jak to konieczne, ale nie dłużej niż sześć tygodni od tej decyzji. W takim przypadku dostawca usług hostingowych nie ujawnia żadnych informacji dotyczących usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich. Ten właściwy organ może przedłużyć ten okres o kolejnych sześć tygodni, jeżeli takie nieujawnianie pozostaje uzasadnione.	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a ustawy o działaniach antyterrorystycznych	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.	

Artykuł 12 Wyznaczenie właściwych organów	1. Każde państwo członkowskie wyznacza organ lub organy właściwe w zakresie: a) wydawania nakazów usunięcia na podstawie art. 3; b) weryfikowania nakazów usunięcia na podstawie art. 4; c) nadzoru nad wdrażaniem środków szczególnych na podstawie art. 5; d) nakładania kar na podstawie art. 18. 2. Każde państwo członkowskie zapewnia, aby w ramach właściwego organu, o którym mowa w ust. 1 lit. a), został wyznaczony lub ustanowiony punkt kontaktowy zajmujący się wnioskami o wyjaśnienie i informacje zwrotne, które dotyczą nakazów usunięcia wydanych przez ten właściwy organ. Państwa członkowskie zapewniają, aby informacje na temat punktu kontaktowego były publicznie dostępne. 3. Do dnia 7 czerwca 2022 r. państwa członkowskie powiadamiają Komisję o właściwym organie lub właściwych organach, o których mowa w ust. 1, i o zmianach w tym zakresie. Komisja publikuje to powiadomienie oraz wszelkie jego zmiany w Dzienniku Urzędowym Unii Europejskiej. 4. Do dnia 7 czerwca 2022 r. Komisja tworzy internetowy rejestr zawierający wykaz właściwych organów, o których mowa w ust. 1, i punktów kontaktowych wyznaczonych lub ustanowionych na podstawie ust. 2 dla każdego właściwego organu. Komisja regularnie publikuje aktualizacje rejestru.	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a, art. 26b i art. 26c ustawy o działaniach antyterrorystycznych	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784. Art. 26b. 1. Szef ABW wyznacza w Agencji Bezpieczeństwa Wewnętrznego punkt kontaktowy, o którym mowa w art. 12 ust. 2 rozporządzenia 2021/784, działający w systemie całodobowym przez 7 dni w tygodniu. 2. Informacje o siedzibie i danych kontaktowych punktu, o którym mowa w ust. 1, oraz sposobie składania wniosków o wyjaśnienie i informacje zwrotne w sprawie nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści o charakterze terrorystycznym, zwanych dalej „nakazami usunięcia”, udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej Agencji Bezpieczeństwa Wewnętrznego. Art. 26c. 1. Szef ABW sprawuje nadzór nad wdrażaniem środków, o których mowa w art. 5 ust. 1- 3 rozporządzenia 2021/784, przez: 1) dokonywanie kontroli środków szczególnych, które podjął dostawca usług hostingowych, w tym pod kątem ich zgodności z art. 5 ust. 2 i 3 rozporządzenia 2021/784; 2) wydawanie dostawcy usług hostingowych pisemnych zaleceń, mających na celu usunięcie stwierdzonych nieprawidłowości i dostosowanie jego działalności do przepisów rozporządzenia 2021/784.	

				2. Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego przeprowadzając czynności, o których mowa w ust. 1, ma prawo: 1) wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych; 2) żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia bądź wglądu w dokumentację techniczną i operacyjną wynikającą ze stosowania środków szczególnych. 3. Dostawca usług hostingowych narażony na treści o charakterze terrorystycznym usuwa naruszenia przepisów prawa i nieprawidłowości stwierdzone w ramach nadzoru sprawowanego przez Szefa ABW w terminie określonym w zaleceniu.	
Artykuł 13 Właściwe organy	1. Państwa członkowskie zapewniają, aby ich właściwe organy dysponowały niezbędnymi uprawnieniami i wystarczającymi zasobami, aby osiągnąć cele i wypełnić swoje obowiązki określone w niniejszym rozporządzeniu. 2. Państwa członkowskie zapewniają, by ich właściwe organy wykonywały swoje zadania określone w niniejszym rozporządzeniu w sposób obiektywny i niedyskryminacyjny, z pełnym poszanowaniem praw podstawowych. Właściwe organy nie zwracają się o instrukcje do żadnego innego organu ani nie przyjmują od niego instrukcji w związku z wykonywaniem swoich zadań określonych w art. 12 ust. 1. Akapit pierwszy nie wyklucza sprawowania nadzoru zgodnie z krajowym prawem konstytucyjnym.	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a ustawy o działaniach antyterrorystycznych	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.	Zgodnie z ustawą o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu Szef ABW jest centralnym organem administracji rządowej, podlegającym bezpośrednio Prezesowi Rady Ministrów oraz podlegającym kontroli Sejmu RP (art. 3 ust. 1–3). Z

					kolei w świetle art. 5 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu do ustawowych zadań ABW należy m.in. ochrona bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.
Artykuł 14 Współpraca między dostawcami usług hostingowych, właściwymi organami oraz Europolem	1. Właściwe organy wymieniają się informacjami, koordynują swoje działania oraz współpracują ze sobą i, w stosownych przypadkach, z Europolem w odniesieniu do nakazów usunięcia, w szczególności w celu uniknięcia powielania wysiłków, a także w celu poprawy koordynacji i uniknięcia konfliktów w zakresie prowadzenia postępowań przygotowawczych w różnych państwach członkowskich. 2. Właściwe organy państw członkowskiego wymieniają informacje z właściwymi organami, o których mowa w art. 12 ust. 1 lit. c) i d), koordynują z nim działania i współpracują z nim w odniesieniu do środków szczególnych podjętych na podstawie art. 5 i kar nakładanych na podstawie art. 18. Państwa członkowskie zapewniają, by właściwe organy, o których mowa w art. 12 ust. 1 lit. c) i d), posiadały wszystkie istotne informacje. 3. Do celów ust. 1 państwa członkowskie zapewniają odpowiednie i bezpieczne kanały lub mechanizmy komunikacji umożliwiające terminową wymianę istotnych informacji. 4. W celu skutecznego wykonywania niniejszego rozporządzenia oraz unikania powielania wysiłków państwa członkowskie i dostawcy usług hostingowych mogą korzystać ze specjalnych narzędzi, w tym narzędzi ustanowionych przez Europol, w celu ułatwienia w szczególności:	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a ustawy o działaniach antyterrorystycznych	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.	Zgodnie z art. 8 ust. 1 ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, Szef ABW w celu realizacji zadań Agencji może podejmować współdziałanie z właściwymi organami i służbami innych państw. Ponadto zastosowanie będą miały przepisy ustawy z dnia 16 września 2011 r. *o*

	a) przetwarzania nakazów usunięcia na podstawie art. 3 i związanych z nimi informacji; oraz b) współpracy w celu określenia i wdrożenia środków szczególnych na podstawie art. 5. 5. W przypadku gdy dostawcy usług hostingowych dowiedzą się o treściach o charakterze terrorystycznym, które wiążą się z bezpośrednim zagrożeniem życia, natychmiast informują organy właściwe w zakresie prowadzenia postępowań przygotowawczych i ścigania przestępstw w zainteresowanym państwie członkowskim lub zainteresowanych państwach członkowskich. Jeżeli nie ma możliwości zidentyfikowania zainteresowanego państwa członkowskiego lub zainteresowanych państw członkowskich, dostawcy usług hostingowych powiadamiają na podstawie art. 12 ust. 2 punkt kontaktowy w państwie członkowskim, w którym mają główną jednostkę organizacyjną lub w którym ich przedstawiciel prawny ma miejsce pobytu lub siedzibę, oraz przekazują informacje dotyczące tych treści o charakterze terrorystycznym Europolowi na potrzeby odpowiednich dalszych działań. 6. Zachęca się właściwe organy do przesyłania Europolowi kopii nakazów usunięcia, umożliwiając mu w ten sposób przygotowanie sprawozdania rocznego zawierającego analizę rodzajów treści o charakterze terrorystycznym będących przedmiotem nakazów usunięcia lub uniemożliwienia dostępu do nich na podstawie niniejszego rozporządzenia.				*wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi*. Ustawa ta określa zasady i warunki wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej, organami ścigania państw trzecich, agencjami Unii Europejskiej, w tym Agencją Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) oraz z organizacjami międzynarodowymi, w celu rozpoznawania, wykrywania lub zwalczania przestępstw lub przestępstw skarbowych, w tym zagrożeń dla

					bezpieczeństwa i porządku publicznego oraz zapobiegania takim przestępstwom i zagrożeniom, a także ścigania sprawców przestępstw lub przestępstw skarbowych. Zgodnie z art. 1 ust. 2 pkt 1 ww. ustawy służbą uprawnioną do wymiany informacji z takimi podmiotami jest Agencja Bezpieczeństwa Wewnętrznego. Z kolei w odniesieniu do ust. 4 wskazać należy przepis ten nie wymaga wdrożenia do polskiego ustawodawstwa dodatkowych przepisów prawa krajowego, gdyż po pierwsze ma on bezpośrednie zastosowanie, a po drugie ma on

					formę fakultatywną, dopuszczając możliwość a nie zobowiązując państwa członkowskie lub dostawców usług hostingowych do korzystania ze specjalnych narzędzi, w tym narzędzi ustanowionych przez Europol. Stanowi o tym również brzmienie motywu 39 rozporządzenia, w którym unijny prawodawca stwierdza, że: „Aby ułatwić szybką wymianę informacji między właściwymi organami, jak również z dostawcami usług hostingowych, oraz aby uniknąć powielania wysiłków, należy zachęcać państwa członkowskie do korzystania ze

					specjalnych narzędzi opracowanych przez Europol, takich jak obecna aplikacja zarządzania zgłoszeniami podejrzanych treści w internecie lub narzędzia, które ją zastępują.”. Ponadto wskazać należy, że zgodnie z art. 15 rozporządzenia dostawcy usług hostingowych są zobowiązani do wskazania lub ustanowienia punktu kontaktowego do celów odbioru nakazów usunięcia za pomocą środków elektronicznych oraz ich niezwłocznego przetwarzania na podstawie art. 3 i 4 rozporządzenia. Informacje o punkcie kontaktowym mają być

					publicznie dostępne. Mając na uwadze, że przepis ten również stosuje się wprost, dostawcy usług hostingowych są zobowiązani do zaopatrzenia się w stosowne środki elektroniczne, które mają zapewnić skuteczność stosowania rozporządzenia w tym zakresie.
Artykuł 15 Punkty kontaktowe dostawców usług hostingowych	1. Każdy dostawca usług hostingowych wskazuje lub ustanawia punkt kontaktowy do celów odbioru nakazów usunięcia za pomocą środków elektronicznych oraz ich niezwłocznego przetwarzania na podstawie art. 3 i 4. Dostawca usług hostingowych zapewnia, aby informacje o punkcie kontaktowym były publicznie dostępne. 2. W informacjach, o których mowa w ust. 1 niniejszego artykułu, określa się języki urzędowe instytucji Unii, zgodnie z rozporządzeniem 1/58 (15), w których można zwracać się do punktu kontaktowego i w których mają się odbywać dalsze wymiany informacji w związku z nakazami usunięcia na podstawie art. 3. Te języki obejmują co najmniej jeden z języków urzędowych państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę.	N			Przepis stosuje się wprost
Artykuł 16 Jurysdykcja	1. Państwo członkowskie, w którym znajduje się główna jednostka organizacyjna dostawcy usług hostingowych, ma jurysdykcję do celów art. 5, 18 i 21. Uznaje się, że dostawca usług hostingowych, który nie ma głównej jednostki organizacyjnej w Unii, podlega	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a ustawy o	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.	

	jurysdykcji państwa członkowskiego, w którym ma miejsce pobytu lub siedzibę jego przedstawiciel prawny. 2. W przypadku gdy dostawca usług hostingowych, który nie ma głównej jednostki organizacyjnej w Unii, nie wyznaczy przedstawiciela prawnego, jurysdykcję mają wszystkie państwa członkowskie. 3. Jeżeli właściwy organ państwa członkowskiego wykonuje jurysdykcję na podstawie ust. 2, informuje o tym właściwe organy wszystkich pozostałych państw członkowskich.		działaniach antyterrorystycznych		
Artykuł 17 Przedstawiciel prawny	1. Dostawca usług hostingowych, który nie ma głównej jednostki organizacyjnej w Unii, wyznacza na piśmie osobę fizyczną lub prawną jako swojego przedstawiciela prawnego w Unii do celów odbioru, stosowania się do i wykonywania nakazów usunięcia i decyzji wydanych przez właściwe organy. 2. Dostawca usług hostingowych przekazuje swojemu przedstawicielowi prawnemu uprawnienia i zasoby niezbędne do stosowania się do tych nakazów usunięcia i decyzji oraz do współpracy z właściwymi organami. Przedstawiciel prawny ma miejsce pobytu lub siedzibę w jednym z państw członkowskich, w których dostawca usług hostingowych oferuje swoje usługi. 3. Przedstawiciel prawny może zostać pociągnięty do odpowiedzialności z tytułu naruszeń niniejszego rozporządzenia, bez uszczerbku dla odpowiedzialności dostawcy usług hostingowych i działań prawnych przeciwko dostawcy usług hostingowych. 4. Dostawca usług hostingowych powiadamia o wyznaczeniu przedstawiciela prawnego właściwy organ, o którym mowa w art. 12 ust. 1 lit. d), państwa członkowskiego, w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę. Dostawca usług hostingowych udostępnia publicznie informacje na temat przedstawiciela prawnego.	N			W tym zakresie zastosowanie będą miały przepisy ogólne regulujące stosunki cywilnoprawne między osobami fizycznymi i osobami prawnymi, wynikające w tym przypadku z umów cywilnoprawnych zawieranych pomiędzy przedstawicielem prawnym z jego mocodawcą (dostawcą usług hostingowych).
Artykuł 18 Kary	1. Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia przez dostawców usług hostingowych i podejmują wszelkie środki niezbędne do zapewnienia ich wykonania. Kary takie ograniczają się do przypadków naruszeń art. 3 ust. 3 i 6, art. 4	T	Art. 1 pkt 2 projektu ustawy dot. art. 26f -26h ustawy o działaniach	Art. 26f. 1. Dostawca usług hostingowych, który nie dopełnia obowiązku, o którym mowa w art. 3 ust. 3 lub 6, art. 4 ust. 2 lub 7, art. 5 ust. 1-3, 5 lub 6, art. 6, art. 7, art. 10, art. 11, art. 14 ust. 5, art. 15 ust. 1 lub art. 17	

	ust. 2 i 7, art. 5 ust. 1, 2, 3, 5 i 6, art. 6, 7, 10 i 11, art. 14 ust. 5, art. 15 ust. 1 oraz art. 17. Kary, o których mowa w akapicie pierwszym, muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie do dnia 7 czerwca 2022 r. powiadamiają Komisję o tych przepisach i środkach, a następnie niezwłocznie powiadamiają ją o zmianach mających wpływ na te przepisy i środki. 2. Państwa członkowskie zapewniają, by właściwe organy uwzględniały przy podejmowaniu decyzji w sprawie nałożenia kary i ustalaniu rodzaju i wysokości kary wszystkie istotne okoliczności, w tym: a) charakter, wagę i czas trwania naruszenia; b) umyślny lub wynikający z zaniedbania charakter naruszenia; c) wcześniejsze naruszenia popełnione przez dostawcę usług hostingowych; d) kondycję finansową dostawcy usług hostingowych; e) poziom współpracy dostawcy usług hostingowych z właściwymi organami; f) charakter i rozmiary dostawców usług hostingowych, w szczególności czy jest on mikro-, małym lub średnim przedsiębiorstwem; g) stopień winy dostawcy usług hostingowych, z uwzględnieniem podjętych przez niego środków technicznych i organizacyjnych w celu spełnienia wymogów niniejszego rozporządzenia. 3. Państwa członkowskie zapewniają, aby systematyczne lub uporczywe niedopełnianie obowiązków wynikających z art. 3 ust. 3 podlegało karom pieniężnym w wysokości do 4 % całkowitych obrotów dostawcy usług hostingowych w poprzednim roku obrotowym.		antyterrorystycznych	rozporządzenia 2021/784 podlega karze pieniężnej. 2. Karę pieniężną, o której mowa w ust. 1, nakłada Szef ABW, w drodze decyzji administracyjnej, biorąc pod uwagę warunki i okoliczności określone w art. 18 rozporządzenia 2021/784 w wysokości do 4% całkowitych obrotów uzyskanych przez dostawcę usług hostingowych w poprzednim roku obrotowym. 3. Decyzje, o których mowa w ust. 2, są ostateczne. 4. Środki z kar pieniężnych, o których mowa w ust. 1, stanowią dochód budżetu państwa. Art. 26g. 1. W związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej, dostawca usług hostingowych jest obowiązany do dostarczenia Szefowi ABW, na każde jego żądanie, w terminie 30 dni od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. 2. W przypadku niedostarczenia danych przez dostawcę usług hostingowych lub gdy dostarczone przez tego dostawcę dane uniemożliwiają ustalenie podstawy wymiaru kary pieniężnej, Szef ABW ustala podstawę wymiaru tej kary w sposób szacunkowy uwzględniając ogólnie dostępne dane finansowe dotyczące tego dostawcy, w tym kryteria, o których mowa w art. 7 ust. 1 pkt 1–3 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236).	

				Art. 26h. Karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja Szefa ABW, o której mowa w art. 26f ust. 2, stała się prawomocna.	
Artykuł 19 Wymogi techniczne i zmiany załączników	1. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 20 w celu uzupełnienia niniejszego rozporządzenia o niezbędne wymogi techniczne dotyczące środków elektronicznych, które mają być stosowane przez właściwe organy do przekazywania nakazów usunięcia. 2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 20 w celu dokonywania zmian załączników, by skutecznie odpowiedzieć na ewentualną potrzebę poprawienia treści wzorów nakazów usunięcia oraz służących przekazywaniu informacji na temat niemożliwości wykonania nakazów usunięcia.	N			
Artykuł 20 Wykonywanie przekazanych uprawnień	1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule. 2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 19, powierza się Komisji na czas nieokreślony od dnia 7 czerwca 2022 r. 3. Przekazanie uprawnień, o którym mowa w art. 19, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych. 4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa. 5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie. 6. Akt delegowany przyjęty na podstawie art. 19 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu	N			

	Parlamentowi Europejskiemu i Radzie lub gdy przed upływem tego terminu zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.				
Artykuł 21 Monitorowanie	1. Państwa członkowskie gromadzą i przesyłają Komisji do dnia 31 marca każdego roku informacje, które uzyskały od swoich właściwych organów i dostawców usług hostingowych podlegających ich jurysdykcji i które dotyczą podjętych przez te organy i dostawców zgodnie z niniejszym rozporządzeniem w poprzednim roku kalendarzowym. Informacje te obejmują: a) liczbę wydanych nakazów usunięcia oraz liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkość, z jaką dokonano usunięcia lub uniemożliwiono dostęp; b) środki szczególne podjęte na podstawie art. 5, w tym liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkość, z jaką dokonano usunięcia lub uniemożliwiono dostępu; c) liczbę wniosków o dostęp, z którymi wystąpiły właściwe organy, w odniesieniu do treści zachowywanych przez dostawcę usług hostingowych na podstawie art. 6; d) liczbę wszczętych procedur rozpatrywania skarg oraz działań podjętych przez dostawców usług hostingowych na podstawie art. 10; e) liczbę wszczętych kontroli w postępowaniach administracyjnych lub sądowych oraz decyzji podjętych przez właściwy organ zgodnie z prawem krajowym. 2. Do dnia 7 czerwca 2023 r. Komisja ustala szczegółowy program monitorowania wyników, rezultatów i skutków niniejszego rozporządzenia. W programie monitorowania określa się wskaźniki i środki służące do gromadzenia danych i innych niezbędnych dowodów, a także przedziały czasowe, w jakich mają one być gromadzone. Wyszczególnia się w nim działania, które mają zostać podjęte przez Komisję i państwa członkowskie przy gromadzeniu i analizowaniu danych i innych dowodów w celu monitorowania postępów i dokonania oceny niniejszego rozporządzenia na podstawie art. 23.	T	Art. 1 pkt 2 projektu ustawy dot. art. 26a oraz art. 26e ustawy o działaniach antyterrorystycznych	Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784. Art. 26e. Dostawca usług hostingowych, w stosunku do którego został wydany nakaz usunięcia, w terminie do dnia 1 marca każdego roku przekazuje Szefowi ABW dane, o których mowa w art. 21 ust. 1 lit. b i d rozporządzenia 2021/784 za rok poprzedni.	

Artykuł 22 Sprawozdanie z wykonania	Do dnia 7 czerwca 2023 r. Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie ze stosowania niniejszego rozporządzenia. To sprawozdanie obejmuje informacje dotyczące monitorowania na podstawie art. 21 oraz informacje wynikające z obowiązków w zakresie przejrzystości na podstawie art. 8. Państwa członkowskie przekazują Komisji informacje niezbędne do sporządzenia sprawozdania.	N			
Artykuł 23 Ocena	Do dnia 7 czerwca 2024 r. Komisja dokonuje oceny niniejszego rozporządzenia oraz przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące jego stosowania, obejmujące informacje na temat: a) skuteczności funkcjonowania mechanizmów gwarancyjnych i zabezpieczających, w szczególności tych przewidzianych w art. 4 ust. 4, art. 6 ust. 3 i art. 7–11; b) wpływu stosowania niniejszego rozporządzenia na prawa podstawowe, w szczególności na wolność wypowiedzi i informacji, poszanowanie życia prywatnego i ochronę danych osobowych; oraz c) przyczyniania się niniejszego rozporządzenia do ochrony bezpieczeństwa publicznego. W stosownych przypadkach sprawozdaniu towarzyszą wnioski ustawodawcze. Państwa członkowskie przekazują Komisji informacje niezbędne do sporządzenia sprawozdania. Komisja ocenia też konieczność i wykonalność ustanowienia europejskiej platformy ds. treści o charakterze terrorystycznym w internecie, która służyłaby ułatwianiu komunikacji i współpracy w ramach niniejszego rozporządzenia.	N			
Artykuł 24 Wejście w życie i stosowanie	Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej. Niniejsze rozporządzenie stosuje się od dnia 7 czerwca 2022 r.	N			
dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW					
Artykuł 21 Środki służące zwalczaniu treści internetowych publicznie	1. Państwa członkowskie podejmują niezbędne środki, aby zapewnić natychmiastowe usuwanie treści internetowych publicznie nawołujących do popełnienia przestępstwa terrorystycznego, o czym mowa w art. 5, które znajdują się na serwerach na ich terytorium. Podejmują także działania mające		Przepisy zmieniające art. 2 projektu ustawy dot.	Art. 2. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812 i 1222) art. 32c otrzymuje brzmienie:	Art. 21 dyrektywy 2017/541 z dnia 15 marca 2017 r. nakłada na państwa

nawołujących do popełnienia przestępstwa	doprowadzić do usunięcia takich treści znajdujących się na serwerach poza ich terytorium. 2. Państwa członkowskie mogą, jeśli usunięcie treści, o których mowa w ust. 1, u źródła nie jest wykonalne, podjąć środki w celu zablokowania użytkownikom korzystającym z internetu na ich terytorium dostępu do takich treści. 3. Środki polegające na usuwaniu i blokowaniu muszą być wprowadzane na podstawie przejrzystych procedur i gwarantują odpowiednią ochronę, w szczególności w celu zapewnienia, aby środki te nie wykraczały poza to, co jest konieczne i proporcjonalne, oraz aby użytkownicy byli informowani o przyczynie wprowadzenia tych środków. Środki ochronne odnoszące się do środków polegających na usuwaniu lub blokowaniu obejmują również możliwość wystąpienia na drogę sądową.		art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu	„Art. 32c. 1. W celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa oraz ścigania ich sprawców sąd, na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, w drodze postanowienia, może zarządzić: 1) usunięcie lub zablokowanie dostępności w systemie teleinformatycznym przez usługodawcę świadczącego usługi drogą elektroniczną, 2) zablokowanie dostępności w systemie teleinformatycznym przez przedsiębiorcę telekomunikacyjnego - określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa, zwane dalej odpowiednio „usunięciem” lub „blokadą dostępności”. 2. Wniosek, o którym mowa w ust. 1, może obejmować blokadę dostępności określonych danych informatycznych, jeżeli ich usunięcie jest lub może okazać się niewykonalne. 3. Wniosek, o którym mowa w ust. 1, przedstawia się wraz z materiałami uzasadniającymi potrzebę usunięcia lub blokady dostępności. 4. Przepisu ust. 1 nie stosuje się do dostawców usług hostingowych i treści o	członkowskie obowiązek zapewnienia natychmiastowego usuwania treści internetowych publicznie nawołujących do popełnienia przestępstwa terrorystycznego, nie wskazując przy tym podmiotu zobowiązanego do usuwania takich treści. Z kolei rozporządzenie 2021/784 nakłada zobowiązania do usuwania treści o charakterze terrorystycznym wyłącznie na dostawców usług hostingowych, nie nakładając takich obowiązków na inne podmioty świadczące usługi drogą elektroniczną, w tym np. usługi tzw. coachingu. Oba przedmiotowe

				charakterze terrorystycznym, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. U. UE L 172 z 17.05.2021, str. 79). 5. Postanowienie, o którym mowa w ust. 1, wydaje Sąd Okręgowy w Warszawie. 6. W przypadkach niecierpiących zwłoki, w celu zapobieżenia zdarzeniu o charakterze terrorystycznym lub uprawdopodobniającemu popełnienie przestępstwa szpiegostwa, Szef ABW, po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, może zarządzić blokadę dostępności, zwracając się jednocześnie do sądu, o którym mowa w ust. 5, z wnioskiem o wydanie postanowienia w tej sprawie. 7. Usługodawca świadczący usługi drogą elektroniczną lub przedsiębiorca telekomunikacyjny jest obowiązany do natychmiastowego dokonania czynności określonych w postanowieniu sądu lub przekazanym mu zarządzeniu Szefa ABW. 8. Wniosek Szefa ABW, o którym mowa w ust. 1, zawiera w szczególności: 1) numer sprawy i jej kryptonim, jeżeli został jej nadany; 2) opis zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej; 3) okoliczności uzasadniające potrzebę usunięcia lub blokady dostępności;	akty (dyrektywa i rozporządzenie) są względem siebie komplementarne i powinny być stosowane równolegle. W związku z tym wymagana jest modyfikacja art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, która zapewni, że przepis ten będzie miał zastosowanie w przypadkach publikowania lub prób publikowania w internecie treści o charakterze terrorystycznym przez podmioty niebędące dostawcami usług hostingowych w rozumieniu rozporządzenia 2021/784. W tym zakresie art. 32c ustawy o Agencji Bezpieczeństwa

				4) szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać usunięciu lub blokadzie dostępności; 5) dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowane będzie usunięcie lub blokada dostępności, ze wskazaniem sposobu stosowania tego usunięcia lub blokady dostępności; 6) cel usunięcia lub blokady dostępności; 7) czas prowadzonej blokady dostępności. 9. Blokadę dostępności zarządza się na okres nie dłuższy niż 30 dni. Sąd, o którym mowa w ust. 5, może, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, wydać postanowienie o jednorazowym przedłużeniu blokady dostępności na okres nie dłuższy niż 3 miesiące, jeżeli nie ustały przyczyny jej zarządzenia. 10. Do wniosku, o którym mowa w ust. 6 i 9, stosuje się odpowiednio przepisy ust. 3 i 8. Sąd przed wydaniem postanowienia, o którym mowa w ust. 1, 6 i 9, zapoznaje się z materiałami uzasadniającymi wniosek. 11. Wnioski, o których mowa w ust. 1, 6 i 9, sąd rozpoznaje jednoosobowo, przy czym czynności sądu związane z rozpoznawaniem tych wniosków są realizowane w warunkach przewidzianych dla przekazywania, przechowywania i udostępniania informacji niejawnych oraz z odpowiednim zastosowaniem przepisów wydanych na podstawie art. 181 § 2 Kodeksu postępowania karnego. W posiedzeniu sądu może wziąć udział wyłącznie prokurator i Szef ABW.	Wewnętrznego oraz Agencji Wywiadu stanowi wdrożenie art. 21 dyrektywy 2017/541 z dnia 15 marca 2017 r.

				12. Na postanowienia sądu, o których mowa w ust. 1, 6 i 9, przysługuje zażalenie Szefowi ABW, Pierwszemu Zastępcy Prokuratora Generalnego Prokuratorowi Krajowemu, usługodawcy świadczącemu usługi drogą elektroniczną lub albo przedsiębiorcy telekomunikacyjnemu. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego. 13. Blokady dostępności zaprzestaje się w przypadku: 1) nieudzielenia przez sąd, w terminie 5 dni od złożenia wniosku w trybie ust. 6, zgody na zarządzenie przez Szefa ABW blokady dostępności; 2) nieudzielenia przez sąd zgody na przedłużenie blokady dostępności w trybie ust. 9; 3) upływu okresu, na który blokada dostępności została wprowadzona. 14. Sąd, Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy oraz Szef ABW prowadzą w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych, rejestry postanowień, pisemnych zgód, zarządzeń i wniosków dotyczących usunięcia lub blokady dostępności. 15. O zastosowaniu usunięcia lub blokady dostępności Szef ABW powiadamia ministra właściwego do spraw informatyzacji, jeżeli usługodawca świadczący usługi drogą elektroniczną lub przedsiębiorca telekomunikacyjny ma siedzibę na terytorium Rzeczypospolitej Polskiej. 16. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób dokumentowania usunięcia lub blokady dostępności oraz	

				przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków, a także wzory stosowanych druków i rejestrów, uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów.”.	
			Przepisy przejściowe art. 3 projektu ustawy	Art. 3. Do blokad dostępności, o których mowa w art. 32c ust. 1 ustawy zmienianej w art. 2, zarządzonych i niezakończonych przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.	
			Przepisy przejściowe art. 4 projektu ustawy	Art. 4. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 32c ust. 14 ustawy zmienianej w art. 2 zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 32c ust. 16 ustawy zmienianej w art. 2, w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż przez okres 12 miesięcy od dnia wejścia w życie niniejszej ustawy.	
			Przepisy końcowe art. 5 projektu ustawy	Art. 5. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.	

ODWRÓCONA TABELA ZGODNOŚCI

Tytuł projektu:		ustawa o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (UC37)	
Lp.	**Jedn. redakcyjna**	**Treść przepisu projektu ustawy**	**Uzasadnienie wprowadzenia**
1.	Art. 2	Art. 2. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812 i 1222) art. 32c otrzymuje brzmienie: „Art. 32c. 1. W celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa oraz ścigania ich sprawców sąd, na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, w drodze postanowienia, może zarządzić: 1) usunięcie lub zablokowanie dostępności w systemie teleinformatycznym przez usługodawcę świadczącego usługi drogą elektroniczną, 2) zablokowanie dostępności w systemie teleinformatycznym przez przedsiębiorcę telekomunikacyjnego - określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa, zwane dalej odpowiednio „usunięciem” lub „blokadą dostępności”. 2. Wniosek, o którym mowa w ust. 1, może obejmować blokadę dostępności określonych danych informatycznych, jeżeli ich usunięcie jest lub może okazać się niewykonalne. 3. Wniosek, o którym mowa w ust. 1, przedstawia się wraz z materiałami uzasadniającymi potrzebę usunięcia lub blokady dostępności. 4. Przepisu ust. 1 nie stosuje się do dostawców usług hostingowych i treści o charakterze terrorystycznym, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. U. UE L 172 z 17.05.2021, str. 79). 5. Postanowienie, o którym mowa w ust. 1, wydaje Sąd Okręgowy w Warszawie. 6. W przypadkach niecierpiących zwłoki, w celu zapobieżenia zdarzeniu o charakterze terrorystycznym lub uprawdopodobniającemu popełnienie przestępstwa szpiegostwa, Szef ABW,	Przepis w zakresie w jakim dotyczy możliwości zarządzenia usunięcia lub zablokowania przez przedsiębiorcę telekomunikacyjnego dostępności w systemie teleinformatycznym określonych danych informatycznych lub określonych usług teleinformatycznych mających związek ze zdarzeniem uprawdopodabniającego popełnienie przestępstwa szpiegostwa nie stanowi wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. *w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW*.

		po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, może zarządzić blokadę dostępności, zwracając się jednocześnie do sądu, o którym mowa w ust. 5, z wnioskiem o wydanie postanowienia w tej sprawie. 7. Usługodawca świadczący usługi drogą elektroniczną lub przedsiębiorca telekomunikacyjny jest obowiązany do natychmiastowego dokonania czynności określonych w postanowieniu sądu lub przekazanym mu zarządzeniu Szefa ABW. 8. Wniosek Szefa ABW, o którym mowa w ust. 1, zawiera w szczególności: 1) numer sprawy i jej kryptonim, jeżeli został jej nadany; 2) opis zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej; 3) okoliczności uzasadniające potrzebę usunięcia lub blokady dostępności; 4) szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać usunięciu lub blokadzie dostępności; 5) dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowane będzie usunięcie lub blokada dostępności, ze wskazaniem sposobu stosowania tego usunięcia lub blokady dostępności; 6) cel usunięcia lub blokady dostępności; 7) czas prowadzonej blokady dostępności. 9. Blokadę dostępności zarządza się na okres nie dłuższy niż 30 dni. Sąd, o którym mowa w ust. 5, może, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, wydać postanowienie o jednorazowym przedłużeniu blokady dostępności na okres nie dłuższy niż 3 miesiące, jeżeli nie ustały przyczyny jej zarządzenia. 10. Do wniosku, o którym mowa w ust. 6 i 9, stosuje się odpowiednio przepisy ust. 3 i 8. Sąd przed wydaniem postanowienia, o którym mowa w ust. 1, 6 i 9, zapoznaje się z materiałami uzasadniającymi wniosek. 11. Wnioski, o których mowa w ust. 1, 6 i 9, sąd rozpoznaje jednoosobowo, przy czym czynności sądu związane z rozpoznawaniem tych wniosków są realizowane w warunkach przewidzianych dla przekazywania, przechowywania i udostępniania informacji niejawnych oraz z odpowiednim zastosowaniem przepisów wydanych na podstawie art. 181 § 2 Kodeksu postępowania karnego. W posiedzeniu sądu może wziąć udział wyłącznie prokurator i Szef ABW. 12. Na postanowienia sądu, o których mowa w ust. 1, 6 i 9, przysługuje zażalenie Szefowi ABW, Pierwszemu Zastępcy Prokuratora Generalnego Prokuratorowi Krajowemu, usługodawcy	Projektowany przepis ma na celu zapewnić skuteczne rozpoznawanie, przeciwdziałanie i zwalczanie przestępstwa szpiegostwa przez rozszerzenie w tym zakresie uprawnień Agencji Bezpieczeństwa Wewnętrznego. Przyjęcie takiego rozwiązania prawnego jest konieczne z uwagi na potrzebę minimalizacji oddziaływania niekorzystnych skutków wynikających z trwającego konfliktu zbrojnego na terytorium Ukrainy, w szczególności znacznie zwiększonej aktywności działań wywiadowczych skierowanych przeciwko Polsce ze strony służb Federacji Rosyjskiej oraz Białorusi.

		świadczącemu usługi drogą elektroniczną lub albo przedsiębiorcy telekomunikacyjnemu. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego. 13. Blokady dostępności zaprzestaje się w przypadku: 1) nieudzielenia przez sąd, w terminie 5 dni od złożenia wniosku w trybie ust. 6, zgody na zarządzenie przez Szefa ABW blokady dostępności; 2) nieudzielenia przez sąd zgody na przedłużenie blokady dostępności w trybie ust. 9; 3) upływu okresu, na który blokada dostępności została wprowadzona. 14. Sąd, Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy oraz Szef ABW prowadzą w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych, rejestry postanowień, pisemnych zgód, zarządzeń i wniosków dotyczących usunięcia lub blokady dostępności. 15. O zastosowaniu usunięcia lub blokady dostępności Szef ABW powiadamia ministra właściwego do spraw informatyzacji, jeżeli usługodawca świadczący usługi drogą elektroniczną lub przedsiębiorca telekomunikacyjny ma siedzibę na terytorium Rzeczypospolitej Polskiej. 16. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób dokumentowania usunięcia lub blokady dostępności oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków, a także wzory stosowanych druków i rejestrów, uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów.”.	

Projekt

R O Z P O R Z Ą D Z E N I E

P R E Z E S A R A D Y M I N I S T R Ó W

z dnia

w sprawie sposobu dokumentowania usunięcia lub blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków

Na podstawie art. 32c ust. 16 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812 i 1222) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) sposób dokumentowania prowadzonego przez Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW”, usunięcia lub blokady dostępności, o których mowa w art. 32c ust. 1 i 6 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
2) sposób przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków;
3) wzory stosowanych druków i rejestrów.

§ 2. 1. Dokumentację usunięcia lub blokady dostępności stanowią:

1) wniosek Szefa ABW do Sądu Okręgowego w Warszawie, zwanego dalej „Sądem”, o zarządzenie usunięcia;
2) wniosek Szefa ABW do Sądu o zarządzenie lub przedłużenie blokady dostępności;
3) postanowienie Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego w sprawie wystąpienia przez Szefa ABW z wnioskiem o zarządzenie przez Sąd usunięcia;
4) postanowienie Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego w sprawie wystąpienia przez Szefa ABW z wnioskiem o zarządzenie lub przedłużenie przez Sąd blokady dostępności;
5) postanowienie Sądu w sprawie zarządzenia usunięcia;

6) postanowienie Sądu w sprawie zarządzenia lub przedłużenia blokady dostępności;
7) wniosek Szefa ABW do Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego o wyrażenie zgody na zarządzenie blokady dostępności w przypadkach niecierpiących zwłoki;
8) postanowienie Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego w sprawie zarządzenia przez Szefa ABW blokady dostępności w przypadkach niecierpiących zwłoki;
9) zarządzenie przez Szefa ABW blokady dostępności w przypadkach niecierpiących zwłoki;
10) wniosek Szefa ABW do Sądu w sprawie zatwierdzenia zarządzenia przez Szefa ABW blokady dostępności w przypadkach niecierpiących zwłoki;
11) postanowienie Sądu w sprawie zatwierdzenia zarządzenia przez Szefa ABW blokady dostępności w przypadkach niecierpiących zwłoki;
12) zażalenie Szefa ABW lub Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego na postanowienie Sądu w sprawie usunięcia lub blokady dostępności;
13) zawiadomienie ministra właściwego do spraw informatyzacji o zarządzeniu usunięcia;
14) zawiadomienie ministra właściwego do spraw informatyzacji o zarządzeniu blokady dostępności.

2. Dokumenty, o których mowa w ust. 1:

1) pkt 1–6, sporządza się według wzorów określonych w załączniku nr 1 do rozporządzenia;
2) pkt 7–11, sporządza się według wzorów określonych w załączniku nr 2 do rozporządzenia;
3) pkt 13 i 14, sporządza się według wzoru określonego w załączniku nr 3 do rozporządzenia.

§ 3. 1. Dokumentacja usunięcia lub blokady dostępności jest przekazywana za pośrednictwem funkcjonariusza ABW, zwanego dalej „przedstawicielem Szefa ABW”, posiadającego pisemne upoważnienie udzielone przez Szefa ABW lub upoważnionego przez niego funkcjonariusza ABW.

2. Przedstawiciel Szefa ABW, z zachowaniem przepisów o ochronie informacji niejawnych, doręcza wniosek Szefa ABW Pierwszemu Zastępcy Prokuratora Generalnego Prokuratorowi Krajowemu, a po wydaniu postanowienia przez Sąd, osobiście odbiera te dokumenty.

§ 4. 1. Wzór rejestru zarządzeń i wniosków, o których mowa w § 2 ust. 1 pkt 1, 2, 7, 9 i 10, prowadzonego przez Szefa ABW, jest określony w załączniku nr 4 do rozporządzenia.

2. Wzór rejestru postanowień, o których mowa w § 2 ust. 1 pkt 3, 4 i 8, prowadzonego przez Pierwszego Zastępcę Prokuratora Generalnego Prokuratora Krajowego, jest określony w załączniku nr 5 do rozporządzenia.

3. Wzór rejestru postanowień, o których mowa w § 2 ust. 1 pkt 5, 6 i 11, prowadzonego przez Sąd, jest określony w załączniku nr 6 do rozporządzenia.

§ 5. 1. Dokumenty, o których mowa w § 2 ust. 1:

1) pkt 1–11, sporządza się w trzech egzemplarzach;

2) pkt 13 i 14, sporządza się w dwóch egzemplarzach.

2. Sąd przechowuje pierwszy egzemplarz dokumentów, o których mowa w § 2 ust. 1 pkt 1–11.

3. Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy przechowuje drugi egzemplarz dokumentów, o których mowa w § 2 ust. 1 pkt 1–11.

4. Minister właściwy do spraw informatyzacji przechowuje pierwszy egzemplarz dokumentu, o którym mowa w § 2 ust. 1 pkt 13 i 14.

5. Pozostałą dokumentację usunięcia lub blokady dostępności przechowuje się w ABW.

6. Dokumenty, o których mowa w ust. 1–5, przechowuje się w sposób określony w przepisach dotyczących ochrony informacji niejawnych.

§ 6. Dokumentację usunięcia lub blokady dostępności przechowuje jednostka organizacyjna ABW, która wnioskowała o usunięcie albo prowadziła tę blokadę, w sposób określony w przepisach dotyczących ochrony informacji niejawnych.

§ 7. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.[1)]

PREZES RADY MINISTRÓW

[1)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Prezesa Rady Ministrów z dnia 18 lipca 2016 r. w sprawie sposobu dokumentowania blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków (Dz. U. poz. 1056), które utraciło moc z dniem wejścia w życie niniejszego rozporządzenia zgodnie z art. 4 ustawy z dnia …….. 2024 r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. poz. ……).

Załączniki
do rozporządzenia
Prezesa Rady Ministrów
z dnia
(poz.)

Załącznik nr 1

WZÓR WNIOSKU SZEFA ABW DO SĄDU O ZARZĄDZENIE USUNIĘCIA

……..
(klauzula tajności po wypełnieniu)

…… ……
(sygnatura literowo-cyfrowa) *(miejscowość, data)*

……
(pieczątka nagłówkowa)

Egz. nr ____

SĄD OKRĘGOWY
W WARSZAWIE

WNIOSEK NR .....
(nr w rejestrze)

Na podstawie art. 32c ust. …… ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) wnoszę o

ZARZĄDZENIE

usunięcia przez …….
(nazwa usługodawcy świadczącego usługi drogą elektroniczną)

w systemie teleinformatycznym określonych:
- danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
- usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

w sprawie ……,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

[*)] Niepotrzebne skreślić

prowadzonej przez ……...,
(nazwa jednostki organizacyjnej ABW)

polegającej na ……,
(szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać usunięciu)

wobec ……

……..,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego będzie zastosowane zarządzenie usunięcia)

w sposób ……..,
(sposób usunięcia)

……..
(klauzula tajności po wypełnieniu)

……..
(klauzula tajności po wypełnieniu)

w celu ……
(cel usunięcia)

……..
(klauzula tajności po wypełnieniu)

UZASADNIENIE: ……
(opis zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa, w miarę możliwości jego kwalifikacja prawna, okoliczności uzasadniające potrzebę zarządzenia usunięcia)
……...
……...
……...

KIEROWNIK JEDNOSTKI ORGANIZACYJNEJ ABW Z SIEDZIBĄ W WARSZAWIE

..... *(data, podpis, pieczątka imienna)*

SZEF AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

..... *(data, podpis, pieczątka imienna)*

DYREKTOR DELEGATURY ABW

..... *(data, podpis, pieczątka imienna)*

……
klauzula tajności po wypełnieniu)

WZÓR WNIOSKU SZEFA ABW DO SĄDU O ZARZĄDZENIE LUB PRZEDŁUŻENIE BLOKADY DOSTĘPNOŚCI

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa)

……
(miejscowość, data)

……
(pieczątka nagłówkowa)

Egz. nr ____

SĄD OKRĘGOWY
W WARSZAWIE

WNIOSEK NR .....
(nr w rejestrze)

Na podstawie art. 32c ust. …… ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) wnoszę o

ZARZĄDZENIE / PRZEDŁUŻENIE[*)]

zablokowania przez ……..
(nazwa usługodawcy świadczącego usługi drogą elektroniczną / przedsiębiorcy telekomunikacyjnego)

dostępności w systemie teleinformatycznym określonych:

– danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
– usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

w sprawie …….,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

prowadzonej przez ……...,
(nazwa jednostki organizacyjnej ABW)

polegającej na ……,
(szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać zablokowaniu)

na okres ……,
(czas prowadzonej blokady dostępności)

wobec ……

……..,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności)

w sposób ……..,
(sposób stosowania blokady dostępności)

[*)] Niepotrzebne skreślić

……..
(klauzula tajności po wypełnieniu)

……..
(klauzula tajności po wypełnieniu)

…….
(sygnatura literowo-cyfrowa)

Egz. nr ____

w celu ……
(cel prowadzonej blokady dostępności)

UZASADNIENIE: ……
(opis zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa, w miarę możliwości jego kwalifikacja prawna, okoliczności uzasadniające potrzebę zastosowania blokady dostępności)
……..
……..
……..

KIEROWNIK JEDNOSTKI ORGANIZACYJNEJ ABW Z SIEDZIBĄ W WARSZAWIE

.....
(data, podpis, pieczątka imienna)

SZEF AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

.....
(data, podpis, pieczątka imienna)

DYREKTOR DELEGATURY ABW

.....
(data, podpis, pieczątka imienna)

……..
(klauzula tajności po wypełnieniu)

WZÓR POSTANOWIENIA PIERWSZEGO ZASTĘPCY PROKURATORA GENERALNEGO PROKURATORA KRAJOWEGO W SPRAWIE WYSTĄPIENIA PRZEZ SZEFA ABW Z WNIOSKIEM O ZARZĄDZENIE USUNIĘCIA

……..
(klauzula tajności po wypełnieniu)

……. ……
(sygnatura literowo-cyfrowa) *(miejscowość, data)*

sygn. akt …….

…….……..
(nr wniosku)

Egz. nr ____

POSTANOWIENIE

Na podstawie art. 32c ust. …… ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) postanawiam

WYRAZIĆ ZGODĘ / NIE WYRAZIĆ ZGODY[*)]

na wystąpienie przez Szefa Agencji Bezpieczeństwa Wewnętrznego do Sądu Okręgowego w Warszawie z wnioskiem o zarządzenie usunięcia przez ……
…….....
(nazwa usługodawcy świadczącego usługi drogą elektroniczną)

w systemie teleinformatycznym określonych:

– danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
– usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

w sprawie .....,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

wobec .....

.....,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego będzie zastosowanie zarządzenie usunięcia)

na podstawie, w sposób i w okolicznościach określonych we wniosku Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia ……. r. o nr ……

UZASADNIENIE: ……..
(w przypadku odmowy wyrażenia zgody)
……..

PIERWSZY ZASTĘPCA
PROKURATORA GENERALNEGO
PROKURATOR KRAJOWY

……... ……..…
(miejscowość, data, godzina) *(podpis, pieczątka imienna)*

[*)] Niepotrzebne skreślić

……..
(klauzula tajności po wypełnieniu)

WZÓR POSTANOWIENIA PIERWSZEGO ZASTĘPCY PROKURATORA GENERALNEGO PROKURATORA KRAJOWEGO W SPRAWIE WYSTĄPIENIA PRZEZ SZEFA ABW Z WNIOSKIEM O ZARZĄDZENIE LUB PRZEDŁUŻENIE PRZEZ SĄD BLOKADY DOSTĘPNOŚCI

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa)

……
(miejscowość, data)

sygn. akt …….

……..
(nr wniosku)

Egz. nr ____

POSTANOWIENIE

Na podstawie art. 32c ust. …… ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) postanawiam

WYRAZIĆ ZGODĘ / NIE WYRAZIĆ ZGODY[*)]

na wystąpienie przez Szefa Agencji Bezpieczeństwa Wewnętrznego do Sądu Okręgowego w Warszawie z wnioskiem o zarządzenie/przedłużenie[*)] zablokowania przez ……..
(nazwa usługodawcy świadczącego usługi drogą elektroniczną / przedsiębiorcy telekomunikacyjnego)

dostępności w systemie teleinformatycznym określonych:

- danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
- usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

w sprawie .....,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

na okres .....,
(czas prowadzonej blokady dostępności)

wobec .....
.....,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności)

na podstawie, w sposób i w okolicznościach określonych we wniosku Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia ……. r. o nr ……

UZASADNIENIE: ……..
(w przypadku odmowy wyrażenia zgody)

……..

PIERWSZY ZASTĘPCA
PROKURATORA GENERALNEGO
PROKURATOR KRAJOWY

……..
(miejscowość, data, godzina)

……..…
(podpis, pieczątka imienna)

[*)] Niepotrzebne skreślić

.....
(klauzula tajności po wypełnieniu)

……..
(klauzula tajności po wypełnieniu)

…… ……
(sygnatura literowo-cyfrowa) *(miejscowość, data)*

sygn. akt …….

……..
(nr wniosku)

Egz. nr ____

POSTANOWIENIE

dnia …….

Sąd Okręgowy w Warszawie w składzie:

Sędzia ……..

z udziałem: ……..

po rozpoznaniu wniosku Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia …… r. o nr ……. w przedmiocie zarządzenia usunięcia na podstawie art. 32c ust. …… ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) postanawia

ZARZĄDZIĆ / ODMÓWIĆ ZARZĄDZENIA[*)]

usunięcie/-a przez …….
(nazwa usługodawcy świadczącego usługi drogą elektroniczną)

w systemie teleinformatycznym określonych:

– danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
– usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

wobec ……

……,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego będzie zastosowane zarządzenie usunięcia)

w sprawie ……...,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

w celu ……..…
(cel usunięcia)

.....
(klauzula tajności po wypełnieniu

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa) Egz. nr ____

UZASADNIENIE: . ……..
(w przypadku odmowy zarządzenia usunięcia)[*)]
……
……

SĘDZIA SĄDU OKRĘGOWEGO

……
(podpis i pieczątka imienna)

[*)] Niepotrzebne skreślić

Wykonano w 3 egz.
Egz. nr 1 – Sąd Okręgowy w Warszawie
Egz. nr 2 – Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy
Egz. nr 3 – ABW
Wykonał: .....

……..
(klauzula tajności po wypełnieniu)

WZÓR POSTANOWIENIA SĄDU W SPRAWIE ZARZĄDZENIA LUB PRZEDŁUŻENIA BLOKADY DOSTĘPNOŚCI

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa)

……
(miejscowość, data)

sygn. akt …….

……..
(nr wniosku)

Egz. nr ____

POSTANOWIENIE

dnia …….

Sąd Okręgowy w Warszawie w składzie:

Sędzia ……..

z udziałem: ……..

po rozpoznaniu wniosku Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia …… r. o nr ……. w przedmiocie zarządzenia / przedłużenia*) blokady dostępności na podstawie art. 32c ust. …… ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) postanawia

ZARZĄDZIĆ / PRZEDŁUŻYĆ / ODMÓWIĆ ZARZĄDZENIA / PRZEDŁUŻENIA*)

zablokowanie/-a przez ……
(nazwa usługodawcy świadczącego usługi drogą elektroniczną / przedsiębiorcy telekomunikacyjnego)

dostępności w systemie teleinformatycznym określonych:

– danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa*)
– usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa*)

na okres ……,
(czas prowadzonej blokady dostępności)

wobec …….

……,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności)

w sprawie ……....,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

w celu ……..…
(cel prowadzonej blokady dostępności)

.....
(klauzula tajności po wypełnieniu

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa) Egz. nr ____

UZASADNIENIE: . ……..
(w przypadku odmowy zarządzenia / przedłużenia blokady dostępności)[*)]
……
……

SĘDZIA SĄDU OKRĘGOWEGO

……
(podpis i pieczątka imienna)

[*)] Niepotrzebne skreślić

Wykonano w 3 egz.
Egz. nr 1 – Sąd Okręgowy w Warszawie
Egz. nr 2 – Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy
Egz. nr 3 – ABW
Wykonał: .....

……..
(klauzula tajności po wypełnieniu)

Załącznik nr 2

WZÓR WNIOSKU SZEFA ABW DO PIERWSZEGO ZASTĘPCY PROKURATORA GENERALNEGO PROKURATORA KRAJOWEGO O WYRAŻENIE ZGODY NA ZARZĄDZENIE BLOKADY DOSTĘPNOŚCI W PRZYPADKACH NIECIERPIĄCYCH ZWŁOKI

……..
(klauzula tajności po wypełnieniu)

……
(miejscowość, data)

……
(sygnatura literowo-cyfrowa)

……
(pieczątka nagłówkowa)

Egz. nr ____

PIERWSZY ZASTĘPCA
PROKURATORA GENERALNEGO
PROKURATOR KRAJOWY

WNIOSEK NR .....
(nr w rejestrze)

Na podstawie art. 32c ust. 6 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) wnoszę o

WYRAŻENIE ZGODY NA ZARZĄDZENIE

zablokowania przez …….
(nazwa usługodawcy świadczącego usługi drogą elektroniczną / przedsiębiorcy telekomunikacyjnego)

dostępności w systemie teleinformatycznym określonych:

- danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
- usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

w przypadkach niecierpiących zwłoki w sprawie ……,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

prowadzonej przez ……..,
(nazwa jednostki organizacyjnej ABW)

polegającej na ……..…,
(szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać zablokowaniu)

na okres ……..……..,
(czas prowadzonej blokady dostępności)

wobec ……..…….

……..……,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności)

……..
(klauzula tajności po wypełnieniu)

(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa) Egz. nr ____

w sposób ……,
(sposób stosowania blokady dostępności)

w celu ……..
(cel prowadzonej blokady dostępności)

UZASADNIENIE: ……
(opis zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa, w miarę możliwości jego kwalifikacja prawna, okoliczności uzasadniające potrzebę zastosowania blokady dostępności)
……..
……...
……...

KIEROWNIK JEDNOSTKI ORGANIZACYJNEJ ABW Z SIEDZIBĄ W WARSZAWIE

……
(data, podpis, pieczątka imienna)

SZEF AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

……
(data, podpis, pieczątka imienna)

DYREKTOR DELEGATURY ABW

……
(data, podpis, pieczątka imienna)

*) Niepotrzebne skreślić

……...
(klauzula tajności po wypełnieniu)

WZÓR POSTANOWIENIA PIERWSZEGO ZASTĘPCY PROKURATORA GENERALNEGO PROKURATORA KRAJOWEGO W SPRAWIE ZARZĄDZENIA PRZEZ SZEFA ABW BLOKADY DOSTĘPNOŚCI W PRZYPADKACH NIECIERPIĄCYCH ZWŁOKI

……..
(klauzula tajności po wypełnieniu)

…… ……
(sygnatura literowo-cyfrowa) *(miejscowość, data)*

sygn. akt …….

…….……
(nr wniosku)

Egz. nr ____

POSTANOWIENIE

Na podstawie art. 32c ust. 6 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) postanawiam

WYRAZIĆ ZGODĘ / NIE WYRAZIĆ ZGODY[*)]

na zarządzenie przez Szefa Agencji Bezpieczeństwa Wewnętrznego zablokowania przez …….…….

(nazwa usługodawcy świadczącego usługi drogą elektroniczną / przedsiębiorcy telekomunikacyjnego)

dostępności w systemie teleinformatycznym określonych:

– danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
– usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

w przypadkach niecierpiących zwłoki w sprawie ……,

(numer sprawy i jej kryptonim, jeżeli został jej nadany)

na okres ……,

(czas prowadzonej blokady dostępności)

wobec …….…….

…….……,

(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności)

na podstawie, w sposób i w okolicznościach określonych we wniosku Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia ……..…….. o nr …….……...…….

UZASADNIENIE: …….

(w przypadku odmowy wyrażenia zgody)

…….…….

PIERWSZY ZASTĘPCA
PROKURATORA GENERALNEGO
PROKURATOR KRAJOWY

…….. ……..…
(miejscowość, data, godzina) *(podpis, pieczątka imienna)*

[*)] Niepotrzebne skreślić

.....
(klauzula tajności po wypełnieniu)

WZÓR ZARZĄDZENIA PRZEZ SZEFA ABW BLOKADY DOSTĘPNOŚCI W PRZYPADKACH NIECIERPIĄCYCH ZWŁOKI

……..
(klauzula tajności po wypełnieniu)

…… ……
(sygnatura literowo-cyfrowa) *(miejscowość, data)*

……
(pieczątka nagłówkowa)

Egz. nr ____

ZARZĄDZENIE NR .....
(nr zgodny z nr wniosku)

Na podstawie art. 32c ust. 6 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812)

ZARZĄDZAM

blokadę dostępności, począwszy od dnia ……...……, godz. ……, w sprawie …….…….., wobec ……
……..,
na podstawie, w sposób i w okolicznościach określonych we wniosku Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia …… o nr …….. oraz postanowieniu Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego z dnia ……..

SZEF
AGENCJI BEZPIECZEŃSTWA
WEWNĘTRZNEGO

.....
(data, podpis, pieczątka imienna)

…….
(klauzula tajności po wypełnieniu)

WZÓR WNIOSKU SZEFA ABW DO SĄDU W SPRAWIE ZATWIERDZENIA ZARZĄDZENIA PRZEZ SZEFA ABW BLOKADY DOSTĘPNOŚCI W PRZYPADKACH NIECIERPIĄCYCH ZWŁOKI

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa)

……
(miejscowość, data)

……
(pieczątka nagłówkowa)

Egz. nr ____

SĄD OKRĘGOWY
W WARSZAWIE

WNIOSEK NR .....
(nr w rejestrze)

Na podstawie art. 32c ust. …… ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) wnoszę o

ZATWIERDZENIE

zarządzenia nr …… Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia …..……. r.
w przedmiocie zablokowania przez …...……...…..
(nazwa usługodawcy świadczącego usługi drogą elektroniczną / przedsiębiorcy telekomunikacyjnego)

dostępności w systemie teleinformatycznym określonych:

- danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
- usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

w przypadkach niecierpiących zwłoki w sprawie .....,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

prowadzonej przez .....,
(nazwa jednostki organizacyjnej ABW)

polegającej na .....,
(szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać zablokowaniu)

na okres .....,
(czas prowadzonej blokady dostępności)

wobec .....

.....,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności)

w sposób .....,
(sposób stosowania blokady dostępności)

w celu .....
(cel prowadzonej blokady dostępności)

[*)] Niepotrzebne skreślić

……..
(klauzula tajności po wypełnieniu)

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa)

Egz. nr ____

UZASADNIENIE: ……..
(opis zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa, w miarę możliwości jego kwalifikacja prawna, okoliczności uzasadniające potrzebę zastosowania blokady dostępności)

…….
…….
…….

KIEROWNIK JEDNOSTKI ORGANIZACYJNEJ ABW Z SIEDZIBĄ W WARSZAWIE

.....
(data, podpis, pieczątka imienna)

SZEF AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

.....
(data, podpis, pieczątka imienna)

DYREKTOR DELEGATURY ABW

.....
(data, podpis, pieczątka imienna)

……..
(klauzula tajności po wypełnieniu)

WZÓR POSTANOWIENIA SĄDU W SPRAWIE ZATWIERDZENIA ZARZĄDZENIA PRZEZ SZEFA ABW BLOKADY DOSTĘPNOŚCI W PRZYPADKACH NIECIERPIĄCYCH ZWŁOKI

……..
(klauzula tajności po wypełnieniu)

…… ……
(sygnatura literowo-cyfrowa) *(miejscowość, data)*

sygn. akt …….

…….……..
(nr wniosku)

Egz. nr ____

POSTANOWIENIE

dnia ……...

Sąd Okręgowy w Warszawie w składzie:

Sędzia ……..…….

z udziałem: ……...

po rozpoznaniu wniosku Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia …… r. o nr ……. w przedmiocie zatwierdzenia zarządzenia przez Szefa Agencji Bezpieczeństwa Wewnętrznego blokady dostępności zastosowanej w przypadkach niecierpiących zwłoki na podstawie art. 32c ust. 6 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) postanawia

ZATWIERDZIĆ / ODMÓWIĆ ZATWIERDZENIA[*)]

zarządzenie/-a przez Szefa Agencji Bezpieczeństwa Wewnętrznego zablokowania przez ……..…….
(nazwa usługodawcy świadczącego usługi drogą elektroniczną / przedsiębiorcy telekomunikacyjnego)

dostępności w systemie teleinformatycznym określonych:

– danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)]
– usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)]

w przypadkach niecierpiących zwłoki w sprawie ……..,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

na okres ……..……,
(czas prowadzonej blokady dostępności)

wobec
……...
……
.,
(dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności)

……..
(klauzula tajności po wypełnieniu)

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa) Egz. nr ____

w sprawie

……...,
(numer sprawy i jej kryptonim, jeżeli został jej nadany)

w celu

……..…....
(cel prowadzonej blokady dostępności)

UZASADNIENIE: .....
(*w przypadku odmowy zatwierdzenia blokady dostępności*)
.....
.....

SĘDZIA SĄDU OKRĘGOWEGO

……
(podpis i pieczątka imienna)

*) Niepotrzebne skreślić

Wykonano w 3 egz.
Egz. nr 1 - Sąd Okręgowy w Warszawie
Egz. nr 2 Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy
Egz. nr 3 - ABW
Wykonał: .....

……..
(klauzula tajności po wypełnieniu)

Załącznik nr 3

WZÓR ZAWIADOMIENIA MINISTRA WŁAŚCIWEGO DO SPRAW INFORMATYZACJI O ZARZĄDZENIU USUNIĘCIA

……..
(klauzula tajności po wypełnieniu)

…… ……
(sygnatura literowo-cyfrowa) *(miejscowość, data)*

……
(pieczątka nagłówkowa)

Egz. nr ____

MINISTER _____

Na podstawie art. 32c ust. 15 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) informuję, iż na podstawie:

1. postanowienia Sądu Okręgowego w Warszawie z dnia …… r., sygn. akt ……[*)];
2. zarządzenia nr ……... Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia ……. r.[*)]

……..……

(nazwa usługodawcy świadczącego usługi drogą elektroniczną)

dokonał usunięcia w systemie teleinformatycznym określonych:

– danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)],
– usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)].

Jednocześnie informuję, że usunięcie polegało na ……...
……...……
……...
……..……
…… ……..……..

SZEF
AGENCJI BEZPIECZEŃSTWA
WEWNĘTRZNEGO

……
(data, podpis, pieczątka imienna)

Wykonano w 2 egz.
Egz. nr 1 - ……
Egz. nr 2 - ABW
Wykonał: ……..

[*)] Niepotrzebne skreślić

numer strony/liczba stron

……
(klauzula tajności po wypełnieniu)

WZÓR ZAWIADOMIENIA MINISTRA WŁAŚCIWEGO DO SPRAW INFORMATYZACJI O ZARZĄDZENIU BLOKADY DOSTĘPNOŚCI

……..
(klauzula tajności po wypełnieniu)

…… ……
(sygnatura literowo-cyfrowa) *(miejscowość, data)*

……
(pieczątka nagłówkowa)

Egz. nr ____

MINISTER _____

Na podstawie art. 32c ust. 15 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) informuję, iż na podstawie:

1. postanowienia Sądu Okręgowego w Warszawie z dnia …… r., sygn. akt ……[*)];
2. zarządzenia nr ……... Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia ……. r.[*)]

……
(nazwa usługodawcy świadczącego usługi drogą elektroniczną / przedsiębiorcy telekomunikacyjnego)

dokonał blokady dostępności w systemie teleinformatycznym określonych:

– danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa[*)],
– usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa[*)].

Jednocześnie informuję, że blokada dostępności polegała na ……...
……...……
……..
i była stosowana wobec ……..
……..…….
……..

SZEF
AGENCJI BEZPIECZEŃSTWA
WEWNĘTRZNEGO

…….
(data, podpis, pieczątka imienna)

Wykonano w 2 egz.
Egz. nr 1 - ……
Egz. nr 2 - ABW
Wykonał: ……..

[*)] Niepotrzebne skreślić

……
(klauzula tajności po wypełnieniu)

Załącznik nr 4

WZÓR REJESTRU ZARZĄDZEŃ I WNIOSKÓW SZEFA ABW W SPRAWIE ZARZĄDZENIA USUNIĘCIA ALBO BLOKADY DOSTĘPNOŚCI W SYSTEMACH TELEINFORMATYCZNYCH OKREŚLONYCH DANYCH INFORMATYCZNYCH LUB USŁUG TELEINFORMATYCZNYCH

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa)

……
(miejscowość, data)

……
(pieczątka nagłówkowa)

Egz. nr ____

REJESTR
ZARZĄDZEŃ I WNIOSKÓW SZEFA ABW
W SPRAWIE USUNIĘCIA LUB BLOKADY DOSTĘPNOŚCI W SYSTEMACH TELEINFORMATYCZNYCH OKREŚLONYCH DANYCH INFORMATYCZNYCH LUB USŁUG TELEINFORMATYCZNYCH

Zawiera ..... **kart**
Założono ….....
(dzień / miesiąc / rok)
Zakończono .....
(dzień / miesiąc / rok)

Lp.	Numer wniosku (-ów) Szefa ABW	Numer zarządzenia Szefa ABW	Kryptonim sprawy	Rodzaj danych informatycznych lub usług teleinformatycznych podlegających usunięciu lub zablokowaniu	Imię i nazwisko Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego oraz informacja o jego postanowieniu	Rodzaj i data wydania postanowienia przez Sąd Okręgowy w Warszawie	Data usunięcia/ okres, na który zarządzono blokadę dostępności, oraz data jej rozpoczęcia, przedłużenia i zakończenia	Inne dane

numer strony/liczba stron

……..
(klauzula tajności po wypełnieniu)

Załącznik nr 5

WZÓR REJESTRU POSTANOWIEŃ PIERWSZEGO ZASTĘPCY PROKURATORA GENERALNEGO PROKURATORA KRAJOWEGO W SPRAWIE WNIOSKU O ZARZĄDZENIE USUNIĘCIA ALBO ZARZĄDZENIA LUB PRZEDŁUŻENIA BLOKADY DOSTĘPNOŚCI W SYSTEMACH TELEINFORMATYCZNYCH OKREŚLONYCH DANYCH INFORMATYCZNYCH LUB USŁUG TELEINFORMATYCZNYCH

……..
(klauzula tajności po wypełnieniu)

…… *(sygnatura literowo-cyfrowa)*

…… *(miejscowość, data)*

…… *(pieczątka nagłówkowa)*

Egz. nr ____

REJESTR
POSTANOWIEŃ PIERWSZEGO ZASTĘPCY PROKURATORA GENERALNEGO PROKURATORA KRAJOWEGO W SPRAWIE USUNIĘCIA LUB BLOKADY DOSTĘPNOŚCI W SYSTEMACH TELEINFORMATYCZNYCH OKREŚLONYCH DANYCH INFORMATYCZNYCH LUB USŁUG TELEINFORMATYCZNYCH

Zawiera ..... kart
Założono ….....
(dzień / miesiąc / rok)
Zakończono .....
(dzień / miesiąc / rok)

Lp.	**Określenie organu wnioskującego o wyrażenie zgody**	**Nr zarządzenia lub wniosku**	**Imię, nazwisko Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego oraz informacja o jego postanowieniu**	**Rodzaj i data wydania postanowienia**	**Data usunięcia/ okres, na który zarządzono blokadę dostępności**	**Inne dane mające związek z wpisem do rejestru**

numer strony/liczba stron

…….
(klauzula tajności po wypełnieniu)

Załącznik nr 6

WZÓR REJESTRU POSTANOWIEŃ SĄDU OKRĘGOWEGO W WARSZAWIE W SPRAWIE ZARZĄDZENIA USUNIĘCIA ALBO ZARZĄDZENIA LUB PRZEDŁUŻENIA BLOKADY DOSTĘPNOŚCI W SYSTEMACH TELEINFORMATYCZNYCH OKREŚLONYCH DANYCH INFORMATYCZNYCH LUB USŁUG TELEINFORMATYCZNYCH

……..
(klauzula tajności po wypełnieniu)

……
(sygnatura literowo-cyfrowa)

……
(miejscowość, data)

……
(pieczątka nagłówkowa)

Egz. nr ____

REJESTR
POSTANOWIEŃ SĄDU OKRĘGOWEGO W WARSZAWIE
W SPRAWIE USUNIĘCIA LUB BLOKADY DOSTĘPNOŚCI W SYSTEMACH TELEINFORMATYCZNYCH OKREŚLONYCH DANYCH INFORMATYCZNYCH LUB USŁUG TELEINFORMATYCZNYCH

Zawiera ..... kart
Założono ….....
(dzień / miesiąc / rok)
Zakończono .....
(dzień / miesiąc / rok)

Lp.	**Określenie organu wnioskującego o wydanie postanowienia**	**Nr wniosku**	**Rodzaj i data wydania postanowienia**	**Data usunięcia/ okres, na który wnioskuje się o wyrażenie zgody na blokadę dostępności / przedłużenie blokady dostępności / zatwierdzenie blokady dostępności w przypadkach niecierpiących zwłoki**	**Inne dane mające związek z wpisem do rejestru**

…….
(klauzula tajności po wypełnieniu)

UZASADNIENIE

Projekt rozporządzenia Prezesa Rady Ministrów w sprawie sposobu dokumentowania usunięcia lub blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków został opracowany na podstawie upoważnienia ustawowego z art. 32c ust. 16 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812 i 1222).

Przedmiotowa materia jest aktualnie uregulowana w rozporządzeniu Prezesa Rady Ministrów z dnia 18 lipca 2016 r. w sprawie sposobu dokumentowania blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków (Dz. U. poz. 1056).

Wydanie nowego rozporządzenia wynika z konieczności uwzględnienia w jego przepisach zmian wprowadzonych przez:

1) art. 2 ustawy z dnia …. r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. poz.…), z którego wynika możliwość usunięcia określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym przez usługodawcę świadczącego usługi drogą elektroniczną oraz rozszerzenie katalogu podmiotów mogących dokonać blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym o przedsiębiorcę telekomunikacyjnego;
2) art. 5 pkt 9 ustawy z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. poz. 1834), które rozszerzyły zakres art. 32c ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, umożliwiając zarządzenie zablokowania dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych w celu zapobiegania, przeciwdziałania i wykrywania przestępstwa szpiegostwa, co oznacza rozszerzenie zastosowania blokady dostępności na określone dane informatyczne lub usługi teleinformatyczne mające związek ze zdarzeniem uprawdopodabniającym popełnienie przestępstwa szpiegostwa, nie tylko tych mających związek ze zdarzeniem o charakterze terrorystycznym. Wobec powyższych zmian w art. 11 ust. 2 ustawy z dnia

17 sierpnia 2023 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw wskazano, że dotychczasowe przepisy wykonawcze wydane na podstawie art. 32c ust. 14 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie wymienionego przepisu, jednak nie dłużej niż przez 24 miesiące od dnia wejścia w życie ustawy z dnia 17 sierpnia 2023 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw;

3) art. 13 ustawy z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz. U. poz. 1860), w zakresie potrzeby zastąpienia użytych w rozporządzeniu wyrazów „Prokurator Generalny” wyrazami „Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy”.

Niezależnie od powyższych zmian, w projekcie zaproponowano usunięcie z katalogu dokumentacji blokady dostępności wniosku Szefa ABW do Sądu Okręgowego w Warszawie o wyrażenie zgody na przedłużenie blokady dostępności zarządzonej przez Szefa ABW w przypadkach niecierpiących zwłoki oraz postanowienia Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego i postanowienia Sądu w tym zakresie. Powyższe wynika z bezzasadności różnicowania trybów wnioskowania o przedłużenie blokady dostępności na tryb zwykły oraz tryb wykorzystywany w przypadkach niecierpiących zwłoki. Na skutek powyższej zmiany usunięto wzory powyższych dokumentów, określone dotychczas w załączniku nr 3 do projektu i dokonano przenumerowania pozostałych załączników.

W pozostałym zakresie projektowane rozporządzenie powiela rozwiązania zawarte w obecnie obowiązującym rozporządzeniu Prezesa Rady Ministrów z dnia 18 lipca 2016 r. w sprawie sposobu dokumentowania blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków (Dz. U. poz. 1056).

Projektowane rozporządzenia określa sposób dokumentowania prowadzonego przez Agencję Bezpieczeństwa Wewnętrznego usunięcia lub blokady dostępności, o której mowa w art. 32c ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków powstałych przy dokonywaniu usunięcia lub blokady dostępności, jak również wzory stosowanych druków i rejestrów.

Projektowany akt wykonawczy w § 2 szczegółowo określa zakres dokumentów

stanowiących dokumentację usunięcia lub blokady dostępności. Wśród niej wskazano wnioski Szefa ABW kierowane do Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego i Sądu Okręgowego w Warszawie w zakresie dotyczącym usunięcia oraz blokowania określonych danych informatycznych lub usług teleinformatycznych, a także postanowienia Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego i Sądu Okręgowego w Warszawie w tych sprawach. Dodatkowo do dokumentacji zaliczono również zarządzenia Szefa ABW oraz zażalenia Szefa ABW oraz Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego na postanowienie Sądu Okręgowego w Warszawie w sprawie przedmiotowych czynności, a także zawiadomienie ministra właściwego do spraw informatyzacji o zarządzeniu usunięcia oraz o zarządzeniu blokady dostępności.

Niniejszy projekt rozporządzenia w § 3 określa sposób przekazywania dokumentacji dotyczącej usunięcia oraz blokady dostępności z zachowaniem przepisów o ochronie informacji niejawnych.

W § 4 określono wzory prowadzonych przez Sąd Okręgowy w Warszawie, Pierwszego Zastępcę Prokuratora Generalnego Prokuratora Krajowego oraz Szefa ABW, zgodnie z art. 32c ust. 14 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, rejestrów postanowień, zarządzeń i wniosków.

Z kolei w § 5 uregulowano sposób sporządzania wspomnianej dokumentacji, a w § 6 określono kwestie dotyczące jej przechowywania.

Rozporządzenie wejdzie w życie 14 dni po dniu ogłoszenia, stosownie do art. 4 ust. 1 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2019 r. poz. 1461).

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), w związku z § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348, z późn. zm), projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej, gdyż materia objęta projektem pozostaje w gestii państw członkowskich Unii Europejskiej i nie podlega harmonizacji. Z tego względu projekt rozporządzenia nie został przedstawiony właściwym instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt rozporządzenia nie dotyczy funkcjonowania samorządu terytorialnego.

Nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i w związku z tym nie podlega obowiązkowi notyfikacji.

Z uwagi na ograniczony zakres podmiotowy projekt rozporządzenia nie ma wpływu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Projekt rozporządzenia nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm).

W stosunku do projektu rozporządzenia nie była dokonywana ocena OSR w trybie § 32 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów.

Nazwa projektu: Rozporządzenie Prezesa Rady Ministrów w sprawie sposobu dokumentowania usunięcia lub blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków **Ministerstwo wiodące i ministerstwa współpracujące** Kancelaria Prezesa Rady Ministrów Agencja Bezpieczeństwa Wewnętrznego **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** 12.08.2024 r. **Źródło** art. 32c ust. 16 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812, z późn. zm.) **Nr w Wykazie prac …**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Potrzeba wydania rozporządzenia Prezesa Rady Ministrów w sprawie sposobu dokumentowania usunięcia lub blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków wynika z konieczności uwzględnienia w jego przepisach zmian wprowadzonych przez:

1) art. 2 ustawy z dnia …. r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. poz.…), z którego wynika możliwość usunięcia określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym przez usługodawcę świadczącego usługi drogą elektroniczną oraz rozszerzenie katalogu podmiotów mogących dokonać blokady dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym o przedsiębiorcę telekomunikacyjnego;
2) art. 5 pkt 9 ustawy z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. poz. 1834), które rozszerzyły zakres art. 32c ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, umożliwiając zarządzenie zablokowania dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych w celu zapobiegania, przeciwdziałania i wykrywania przestępstwa szpiegostwa, co oznacza rozszerzenie zastosowania blokady dostępności na określone dane informatyczne lub usługi teleinformatyczne mające związek ze zdarzeniem uprawdopodabniającym popełnienie przestępstwa szpiegostwa, nie tylko tych mających związek ze zdarzeniem o charakterze terrorystycznym. Wobec powyższych zmian w art. 11 ust. 2 ustawy z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw wskazano, że dotychczasowe przepisy wykonawcze wydane na podstawie art. 32c ust. 14 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie wymienionego przepisu, jednak nie dłużej niż przez 24 miesiące od dnia wejścia w życie ustawy z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw;
3) art. 13 ustawy z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy - Prawo o ustroju sądów powszechnych, ustawy - Kodeks postępowania karnego oraz niektórych innych ustaw (Dz. U. poz. 1860), w zakresie potrzeby zastąpienia użytych w rozporządzeniu wyrazów „Prokurator Generalny” wyrazami „Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy”.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

W związku z dyspozycją art. 4 ustawy z dnia …. r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. poz.…) konieczne jest wydanie rozporządzenia Prezesa Rady Ministrów określającego sposób dokumentowania prowadzonego przez Agencję Bezpieczeństwa Wewnętrznego, usunięcia lub blokady dostępności, o których mowa w art. 32c ust. 1 i 6 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, jak również przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków, jak również wzory stosowanych w przedmiotowej sprawie druków i rejestrów.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na charakter wprowadzanych regulacji, nie przeprowadzano analizy porównawczej.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie

Szef Agencji Bezpieczeństwa Wewnętrznego	1	Dane własne	dokumentowanie usunięcia lub blokady dostępności określonych danych informatycznych lub usług teleinformatycznych
Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy	1		dokumentowanie usunięcia lub blokady dostępności określonych danych informatycznych lub usług teleinformatycznych
Sąd Okręgowy w Warszawie	1		dokumentowanie usunięcia lub blokady dostępności określonych danych informatycznych lub usług teleinformatycznych

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt rozporządzenia zostanie zamieszczony, stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. *o działalności lobbingowej w procesie stanowienia prawa* (Dz. U. z 2017 r. poz. 248) oraz zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – *Regulamin pracy Rady Ministrów* (M. P. z 2022 r. poz. 348, z późn. zm.), w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2024 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	–	–	–	–	–	–	–	–	–	–	–	–
budżet państwa	–	–	–	–	–	–	–	–	–	–	–	–
JST	–	–	–	–	–	–	–	–	–	–	–	–
pozostałe jednostki (oddzielnie)	–	–	–	–	–	–	–	–	–	–	–	–
Wydatki ogółem	–	–	–	–	–	–	–	–	–	–	–	–
budżet państwa	–	–	–	–	–	–	–	–	–	–	–	–
JST	–	–	–	–	–	–	–	–	–	–	–	–
pozostałe jednostki (oddzielnie)	–	–	–	–	–	–	–	–	–	–	–	–
Saldo ogółem	–	–	–	–	–	–	–	–	–	–	–	–
budżet państwa	–	–	–	–	–	–	–	–	–	–	–	–
JST	–	–	–	–	–	–	–	–	–	–	–	–
pozostałe jednostki (oddzielnie)	–	–	–	–	–	–	–	–	–	–	–	–

Źródła finansowania	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł,	duże przedsiębiorstwa	-	-	-	-	-	-	-
	sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-

ceny stałe z 2024 r.)	rodzina, obywatele oraz gospodarstwa domowe	–	–	–	–	–	–	–
W ujęciu niepieniężnym	duże przedsiębiorstwa	-						
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe	Projektowana regulacja nie ma wpływu na sytuację ekonomiczną i społeczną rodziny, obywateli oraz gospodarstw domowych						
	osoby niepełnosprawne, osoby starsze	Projektowana regulacja nie ma wpływu na sytuację ekonomiczną i społeczną osób niepełnosprawnych oraz osób starszych.						
Niemierzalne		-						

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie przewiduje się wpływu projektowanej regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorców.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☒ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz: Brak.

9. Wpływ na rynek pracy

Nie przewiduje się wpływu projektowanej regulacji na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	

11.Planowane wykonanie przepisów aktu prawnego

Planuje się, że rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Ze względu na charakter wprowadzanej regulacji, nie jest planowana ewaluacja efektów projektu, a tym samym nie przewiduje się stosowania mierników ewaluacji.

13.Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak.