Warszawa, 24 października 2018 r.

INSTRUKCJA DLA PRZEDSTAWICIELA POLSKI
na posiedzenie Grupy Roboczej Rady UE ds. terroryzmu w dniu 25 października 2018 r. w Brukseli w sprawie projektu rozporządzenia dot. zapobiegania rozpowszechnianiu w internecie treści terrorystycznych

Uzgodniona z: MSWiA, MS, ABW, MON, MPiT, MF, MSZ,NASK, DT MC, DC MC

Informacje na temat przedstawiciela Polski na posiedzenie:	
Imię i nazwisko/stanowisko:	Maciej Groń / Dyrektor
Instytucja/komórka organizacyjna:	Ministerstwo Cyfryzacji, Departament Polityki Międzynarodowej
Numer telefonu:	+48 22 2455528
Adres poczty elektronicznej:	Maciej.gron@mc.gov.pl; sekretariat.dwmia@mc.gov.pl

Data poprzedniego posiedzenia: 5 października 2018 r.

Porządek spotkania

Dalsza dyskusja nad projektem rozporządzenia dot. zapobiegania rozpowszechnianiu w internecie treści terrorystycznych.

Stanowisko do zaprezentowania podczas posiedzenia

Przedstawiciel Polski zgłosi zastrzeżenia analityczne do całości rozporządzenia. W miarę przebiegu dyskusji zada pytania w celu wyjaśnienia wątpliwości co do projektowanych w dokumencie rozwiązań.

1. **Art. 2 Definicja dostawcy usług hostingowych**

W przedstawionej definicji dostawcy usług hostingowych mieści się potencjalnie wiele podmiotów.

- Czy Komisja może wskazać przykładowy katalog usług, które będą się mieściły w tej definicji?
- Czy definicja obejmuje także dostawców oferujących swoje usługi w relacjach biznesowych (B2B, business-to-business), np. dostawców usług chmurowych kierujących swoją ofertę do innych firm, nie konsumentów (B2C, business-to consumers)?

2. **Koszty wdrożenia systemu przez MŚP i ich możliwości działania – art. 4, 5, 6**

Nowa regulacja obejmuje swym zakresem platformy technologiczne niezależnie od skali ich działalności, czy poziomu rozwoju technologicznego.

- **Art. 4** przewiduje obowiązek usunięcia lub blokady treści przez dostawcę usług hostingowych w ciągu 1 godziny od momentu otrzymania nakazu. To oznacza, że usługodawca będzie musiał zapewnić punkt kontaktowy gotowy na reakcję i dostępny w trybie 24/7. To natomiast oznacza konieczność wyznaczenia przez przedsiębiorcę osób pracujących w systemie pracy zmianowej

– i poniesienie wydatków na ten cel. Mając na uwadze zagrożenie sankcjami i wymóg prawa taki punkt będzie musiał być utrzymywany w gotowości – niezależnie od tego ile realnie zgłoszeń do niego wpłynie oraz na ile usługi świadczone przez danego dostawcę są narażone na wykorzystanie do rozpowszechniania treści terrorystycznych. Czy Komisja Europejska oszacowała ile będzie kosztowało wdrożenie przez MŚP takiego punktu kontaktowego gotowego na przyjęcie zgłoszenia 24h na dobę 7 dni w tygodniu?

- **Art. 4 i 5** Czy nie ma obawy, że mali usługodawcy – zatrudniający mała ilość pracowników - nie będą wstanie należycie ocenić nakazów (art. 4) i zgłoszeń (art. 5) w krótkim czasie? Czy to nie oznacza, że możliwość odwołania się o nakazu usunięcia treści będzie dla nich tylko teoretyczna? Mając na uwadze ograniczone zasoby, którymi dysponują te firmy jaka ma być ich motywacja do odwoływania się od decyzji, skoro to oznaczać będzie dla nich dodatkowe koszty? Czy to nie oznacza ryzyka, że firmy będą prewencyjnie usuwały wszystkie podejrzane treści, także i te dopuszczalne, tylko po to, aby uchronić się przed odpowiedzialnością?

- **Art. 6** Wdrożenie środków proaktywnych służących blokadzie treści terrorystycznych, czy też przechowywanie usuniętych lub zablokowanych treści **(art. 7)** i raportowanie **(art. 8)** to kolejne dodatkowe koszty. Koszty te mogą obniżyć konkurencyjność mniejszych usługodawców. Duzi gracze sobie z nimi poradzą, ale czy w ten sposób nie utrudnia się działalności podmiotom z Europy?

- **Art. 6 ust. 2** przewiduje obowiązek sprawozdawczy dotyczący zastosowanych środków proaktywnych w sytuacji, gdy organ nadzorczy podjął ostateczną decyzję o usunięciu - nawet jednostkowym - treści. Raport ma być przedstawiany nie tylko 3 miesiące po otrzymaniu zapytania, ale także co roku od tej daty. Czy nie jest to zbyt restrykcyjne i nadmiarowe podejście w szczególności, gdy decyzje o usunięciu treści terrorystycznych, przez danego usługodawcę zdarzają się incydentalnie?

- **Art. 4, 5, 6 i 18** Czy powinno się stosować takie samo podejście do globalnych koncernów, jak i małych firm działających lokalnie – tylko na terenie jednego państwa? Jak wynika z impact assessment ponad 90% europejskich przedsiębiorstw dostarczających usługi hostingu to MŚP, a prawie połowa to mikroprzedsiębiorstwa (mniej niż 10 pracowników, obroty / bilans niższe niż 2 mln EUR).

3. **Relacje z Dyrektywą e-commerce (2000/31/WE) – art. 6**

- **Art. 6** rozporządzenia zakłada możliwość nałożenia na dostawców usług hostingu ogólnego obowiązku monitorowania treści pod kątem treści terrorystycznych. Oznacza to stosowanie mechanizmów filtrowania treści i de facto odstępstwo od art. 15 ust. 1 dyrektywy 2000/31/WE[1]. Artykuł 15 zakazuje państwom członkowskim nakładania na usługodawców

[1] *Artykuł 15 Brak ogólnego obowiązku w zakresie nadzoru*
1. Państwa Członkowskie nie nakładają na usługodawców świadczących usługi określone w art. 12, 13 i 14 ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.
2. Państwa Członkowskie mogą ustanowić w stosunku do usługodawców świadczących usługi społeczeństwa informacyjnego obowiązek niezwłocznego powiadamiania właściwych władz publicznych o rzekomych

ogólnego obowiązku monitorowania informacji. Czy Komisja przewiduje w związku z tym rewizję Dyrektywy e-commerce?

- **Art. 4** zakłada usunięcie lub zablokowanie treści o charakterze terrorystycznym lub uniemożliwiają dostępu do nich w ciągu jednej godziny od momentu otrzymania nakazu usunięcia. Jednocześnie art. 14 b dyrektywy o handlu elektronicznym wskazuje, że hostingodawca nie jest odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem że podejmuje niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony[2]. Czy nie ma tutaj konfliktu pomiędzy dyrektywą e-commerce, która zakłada niezwłoczne działanie z rozporządzeniem, które zawęża czas reakcji do 1 godziny?

- Czy Komisja Europejska bierze pod uwagę ryzyko odejścia od zasad Dyrektywy e-commerce? Czy wprowadzając wyłom w dyrektywie Komisja bierze pod uwagę, że rozmontowujemy system na którym dotychczas opierał się internet w UE. Czy w związku z tym są pomysły na nowe uregulowanie podstaw jego funkcjonowania?

4. **Tempo prac i czas na wdrożenie – art. 24**

- Komisja zakłada szybkie prace nad rozporządzeniem (koniec kadencji KE i wybory do Parlamentu w 2019 roku). Czy nie powinniśmy natomiast postawić bardziej na jakość wypracowywanych rozwiązań?

5. **Które organy krajowe powinny realizować zobowiązania wynikające z rozporządzenia**

- **Jakiego rodzaju organy powinny w realizować na poziomie krajowym zadania, o których mowa w art. 17 projektu?** (wydawanie nakazów usunięcia na podstawie art. 4; zgłaszanie treści o charakterze terrorystycznym dostawcom usług hostingowych na podstawie art. 5; nadzoru nad wdrażaniem proaktywnych środków na podstawie art. 6; egzekwowania obowiązków na podstawie rozporządzenia poprzez nakładanie sankcji na podstawie art. 18, na podstawie art. 13 państwa członkowskie powinny zapewnić koordynację i odpowiednie kanały komunikacji lub mechanizmy umożliwiające szybką wymianę istotnych informacji). **Czy w zamyśle Prezydencji powinny to być organy śledcze, kontrwywiadowcze, czy też centralne organy administracji rządowej (ministerialne)?**

Informacje dodatkowe

bezprawnych działaniach podjętych przez ich usługobiorców lub przez nich przekazanych informacjach lub obowiązek przekazywania właściwym władzom, na ich żądanie, informacji pozwalających na ustalenie tożsamości ich usługobiorców, z którymi mają umowy o przechowywanie.

[2] Artykuł 14 Hosting

1. Państwa Członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę usługodawca nie był odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem że:
(…) b) usługodawca podejmuje niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony

Prace nad rozporządzeniem są prowadzone w szybkim tempie – ambicją Komisji Europejskiej jest, aby Rada UE zakończyła prace nad projektem do kwietnia 2019 r. Na poprzednich posiedzeniach Grupy Roboczej Rady UE ds. terroryzmu (25.09 i 5.10) odbyła się już dyskusja nad wszystkimi artykułami dokumentu. Odbyła się także runda zbierania uwag pisemnych. Na podstawie zebranych wkładów (11 państw) prezydencja opracowała na spotkanie 25.10 tekst kompromisowy rozporządzenia.

Celem rozporządzenia jest **zapobieganie rozpowszechnianiu treści terrorystycznych w internecie poprzez ich jak najszybsze usuwanie i zapobieganie ponownemu umieszczeniu w sieci**. Zgodnie z definicją treściami terrorystycznymi mogą być zarówno treści pochwalające lub gloryfikujące taką aktywność, popierające aktywność terrorystyczną, jak i stanowiące instrukcje lub wskazówki dotyczące faktycznego podejmowania działań terrorystycznych. Ta definicja spotkała się z dyskusją – m.in. postulowano, by była ona zbliżona do tej z dyrektyw w sprawie zwalczania terroryzmu. W wersji kompromisowej definicja została nieco zmodyfikowana – w kierunku większej precyzji.

Zaproponowany w rozporządzeniu **model opiera się na ścisłej współpracy pomiędzy właściwymi organami państwowymi, a podmiotami świadczącymi usługi hostingu**, zdefiniowanymi jako dostawcy usług społeczeństwa informacyjnego polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek oraz na udostępnianiu przechowywanych informacji osobom trzecim.

Rozmiar ani zasięg działania dostawcy usługi nie będzie miał znaczenia dla zastosowania rozporządzenia – podobnie jak jego ewentualna lokalizacja poza obszarem Unii Europejskiej (liczy się, że dostawca oferuje usługi w UE). **Rozporządzenie nie przewiduje wyłączeń dla MŚP** - jest to celowe działanie (tak można wnioskować z OSR rozporządzenia) ponieważ dla Komisji Europejskiej problemem nie jest współpraca z dużymi podmiotami, a właśnie z tymi mniejszymi portalami.

Podobnie jak RODO, czy dyrektywa NIS **zakłada się szacowanie ryzyka** - część obowiązków, wynikających z projektu, będzie wykonywana w sposób proporcjonalny i odpowiedni do zidentyfikowanych ryzyk. To ma przełożyć się na zmniejszenie ciężaru regulacyjnego w przypadku mniejszych podmiotów.

Kluczowym obowiązkiem (art. 4) przewidzianym w projekcie jest nakaz usunięcia lub uniemożliwianie dostępu do treści terrorystycznych w ciągu 1 godziny od momentu otrzymania stosownego nakazu uprawnionego organu. Rozporządzenie przewiduje możliwość odwołania się od takiej decyzji. Zapisane są w nim także wyjątkowe przypadki, w których jednogodzinny termin nie znajdzie zastosowania, np. w przypadku siły wyższej, lub nakaz usunięcia zawiera oczywiste błędy i wymaga korekty. Co do zasady natomiast, niezastosowanie się do nakazu usunięcia treści może wiązać się z sankcją finansową w wysokości nawet do 4 proc. rocznego obrotu dostawcy usług hostingowych.

W art. 5 przewidziano natomiast możliwość skierowania, przez właściwy organ państwa lub UE, zgłoszenia do dostawcy usług hostingowych. W oparciu o otrzymane powiadomienie, to dostawca usługi będzie mógł podjąć decyzje, czy dany komunikat stanowi treść terrorystyczną i powinien zostać usunięty. Tego typu treści powinny być przechowywane przez dostawcę usług hostingowych, z zachowaniem odpowiednich zabezpieczeń przez okres kolejnych 6 miesięcy na potrzeby ewentualnego postępowania wyjaśniającego, prowadzonego przez właściwe organy. Te same organy będą miały również możliwość nakazania dłuższego przechowywania wspomnianych wyżej informacji.

Zgodnie z art. 6 na dostawcę usługi hostingu mają zostać nałożone także obowiązki związane z proaktywnymi środkami zapobiegającym rozpowszechnianiu treści terrorystycznych. Do takich rozwiązań zalicza się m.in. mechanizmy automatycznie, analizujące treści w celu uniemożliwienia ponownego opublikowania informacji już raz usuniętych, a także wykrywania, identyfikacji i sprawnego

usuwania pojawiających się nowych treści terrorystycznych. Mechanizmy te powinny jednak działać pod nadzorem człowieka (art. 9).

Do dodatkowych obowiązków usługodawców świadczących usługi hostingu należeć będą również:

- Art. 8 ust. 1 zawarcie w warunkach korzystania z usługi **informacji o wdrożonej polityce zapobiegania rozpowszechnianiu treści terrorystycznych**, w tym informacji o stosowanych narzędziach służących ich automatycznemu wykrywaniu.
- Art. 8 ust. 2 i 3 **sporządzanie rocznych raportów** dotyczących działań przedsięwziętych przez usługodawcę w zakresie przeciwdziałania terroryzmowi.
- Art. 14 **powołanie punktu kontaktowego, dostępnego w trybie 24/7**, zapewniającego ciągłą możliwość sprawnego kontaktu z właściwym organem państwowym.
- Art. 11 kontakt z dostawcami treści (których treści zostały usunięte) w zakresie podejmowanych działań, w tym w zakresie przypadków usunięcia lub uniemożliwienia dostępu do informacji publikowanych przez dostawcę treści.
- Art. **10 counter notice - procedura skarg, składanych przez dostawców treści**, w przypadku usunięcia informacji terrorystycznych na skutek otrzymanego powiadomienia (w oparciu o art. 5) lub na skutek samodzielnie zastosowanych środków proaktywnych wykrywających treści o potencjalnie terrorystycznym charakterze (w oparciu o art. 6).

Do obowiązków państw członkowskich (art. 17) będzie należało wyznaczenie właściwego organu lub organów na potrzeby:

- **wydawania nakazów usunięcia** na podstawie art. 4;
- **zgłaszania treści** o charakterze terrorystycznym dostawcom usług hostingowych na podstawie art. 5;
- **nadzoru nad wdrażaniem proaktywnych środków** na podstawie art. 6;
- egzekwowania obowiązków na podstawie rozporządzenia poprzez **nakładanie sankcji** na podstawie art. 18 – **mogą one sięgać do 4% wysokości całkowitych obrotów** dostawców usług hostingowych w ostatnim roku obrotowym.
- Ponadto na podstawie art. 13 **państwa członkowskie powinny zapewnić koordynację i odpowiednie kanały komunikacji** lub mechanizmy umożliwiające szybką wymianę istotnych informacji.

Oceniają rozporządzenie można zauważyć, że jest ono bardzo ambitne. Należy się zgodzić, że kluczowe jest zapewnienie szybkiej i zdecydowanej reakcji w czasie następującym bezpośrednio po zamieszczeniu treści terrorystycznych online – z uwagi na ich tempo rozprzestrzeniania w cyfrowej rzeczywistości. Z drugiej strony należy dostrzegać ryzyko cenzury treści publikowanych w internecie, czy wręcz autocenzury (mechanizmy proaktywne), wprowadzanej przez usługodawców z obawy przed sankcjami finansowymi.

Realizacja rozporządzenia nie będzie bezkosztowa – oznacza ono wydatki zarówno po stronie dostawców usług hostingowych (mechanizmy filtrowania treści, punkty działające 24/7, sporządzanie rocznych raportów), **jak i budżetu państwa** (zapewnienie obsługi systemu – art.4, 5, 6 i 18). Można powiedzieć, że jeżeli tak projektowany system ma działać to ponoszenie tych wydatków jest konieczne – pewne wyliczenia kosztów zostały sporządzone przez Komisję Europejską w Ocenie skutków

regulacji. Jakie będą to jednak realnie koszty zależy oczywiście od praktycznego stosowania przepisów (ilość nakazów usunięcia, na ile szeroko będą stosowane środki proaktywnego wykrywania treści terrorystycznych, realne zagrożenie sankcjami i ich wysokość itp.).

Dokładnej analizy wymagać będzie kwestia relacji rozporządzenia z dyrektywą o handlu elektronicznym (2000/31/WE), w Polsce implementowanej w ramach ustawy o świadczeniu usług drogą elektroniczną. **Art. 6 niniejszego rozporządzenia oznacza de facto odstępstwo od art. 15 ust. 1 dyrektywy 2000/31/WE** – który zakłada, że państwa członkowskie nie nakładają na usługodawców ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.

Do istotnego ryzyka związanego z realizacją projektu niniejszego rozporządzenia zaliczyć należy zakładane szybkie tempo prac (Komisja zakłada zakończenie negocjacji w Radzie do kwietnia 2019 r.). Problematyczne może być wdrożenie projektowanych w nim rozwiązań. W zmodyfikowanej propozycji prezydencji w art. 24 wydłużono zakładany termin stosowania rozporządzenia z 6 miesięcy jak chciała KE, na 1 rok po wejściu w życie rozporządzenia. Tym niemniej wciąż nie jest to długi termin, dlatego już teraz – na etapie negocjacji - należy się zastanowić, która instytucja / lub instytucje w kraju będą realizowały zadania przewidywane w rozporządzeniu.