Stanowisko Polskiej Izby Informatyki i Telekomunikacji (PIIT)
w sprawie projektu regulacji Digital Services Act - dokument COM(2020) 825

Na wstępie pragniemy podziękować za możliwość udziału w konsultacjach tego od dawna oczekiwanego i jakże ważnego dla jednolitego rynku cyfrowego dokumentu oraz zadeklarować nasz systematyczny i czynny udział w jego opiniowaniu na dalszych etapach prac.

W naszej ocenie wybór instrumentu prawnego w postaci rozporządzenia, a nie dyrektywy, jest słuszny, biorąc pod uwagę cel, jakim jest zapewnienie zharmonizowanych i spójnych przepisów dla całego rozwijającego się unijnego rynku cyfrowego. Dotychczasowe doświadczenia związane ze sposobem implementacji i stosowaniem dyrektywy e-commerce w poszczególnych państwach członkowskich i nasilające się negatywne zjawiska i działania w przestrzeni on-line wskazywały na potrzebę dalszego ujednolicenia i dostosowania przepisów do zmieniających się realiów biznesowych i technologicznych, tak aby zapewnić równe szanse konkurowania i większą pewność prawną podmiotom cyfrowym działającym na rynku unijnym, przy jednoczesnym zachowaniu zasady „państwa pochodzenia" i tym samym zachęcić europejskie firmy do rozwijania swych usług i ekspansji cyfrowej także na rynki innych krajów UE.

Niezwykle istotne jest, że projektowane przepisy obejmują także podmioty spoza Unii Europejskiej, które świadczą usługi w państwach członkowskich. W tym zakresie bardzo słuszna jest kontynuacja podejścia przyjętego w RODO. Doceniamy również leżącą u podstaw projektu rozporządzenia zasadę ochrony wolności obywatelskich, w tym swobodę wypowiedzi, jak też ochronę użytkowników usług pośredników internetowych.

Popieramy zróżnicowanie przepisów odnoszących się do treści nielegalnych i treści szkodliwych, jak również pozostawienie odpowiedniego pola do samoregulacji, zgodnie z zasadą proporcjonalności. Doceniamy także pewne zalety zróżnicowania nałożonych obowiązków i wymagań w zależności od wielkości podmiotu świadczącego usługi pośrednictwa internetowego, co sprawia, że przepisy są proporcjonalne i nie stanowią bariery dla mniejszych podmiotów pragnących konkurować na rynku i proponować nowe, atrakcyjne dla użytkowników usługi. Zwracamy jednocześnie uwagę, że dla osiągnięcia celów regulacji niezbędne jest niekiedy, aby niektóre zasady dotyczyły wszystkich podmiotów świadczących daną usługę, z uwzględnieniem realnych możliwości ich przestrzegania.

Poniżej przedstawiamy szczegółowe uwagi, w tym dotyczące niektórych przepisów projektu wymagających jeszcze zmian i doprecyzowania

1. Podczas prac nad dokumentem, Komisja Europejska wskazywała na przyjęcie zasady, że co jest nielegalne offline, jest też nielegalne online. Niestety nie zostało to wprost wskazane w projekcie, chociażby w motywie 12, w którym przedstawiono szeroką interpretację (wraz z przykładami) tego co stanowi treści bezprawną (*illegal content*). Zawarcie w tekście takiego zdania z pewnością wzmocniłoby przesłanie całej regulacji i pozwoliłoby na uniknięcie ew. wątpliwości na etapie jej stosowania.

2. Jak w każdym akcie prawnym, kluczowe dla właściwego stosowania DSA jest precyzyjne sformułowanie definicji. Pragniemy w związku z tym zwrócić uwagę na pewną niejasność przepisów określających zakres podmiotowy regulacji i na problem jednolitości definicji w ustawodawstwie unijnym, w szczególności w zakresie definicji platformy on-line. Niestety, DSA nie definiuje jasno pojęcia platform internetowych, zwłaszcza dużych platform („*very large online platforms*"). W związku ze wskazanym kryterium wyodrębnienia dużych platform (45 milionów średniomiesięcznie aktywnych użytkowników – „*of average monthly active recipients*") nie jest jasne, jak liczyć wskazaną liczbę użytkowników, np. czy chodzi o użytkowników usług spełniających kryteria podane w definicji platformy online, czy wszystkich usług, które realizuje dany przedsiębiorca, ewentualnie grupa przedsiębiorców partnerskich i powiązanych. Podobnie nie wiadomo, kim jest „aktywny użytkownik"? Podsumowując, kwestie definicyjne są kluczowe dla rozeznania przez przedsiębiorców skutków wejścia w życie komentowane aktu. Bez tego może okazać się, że niektóre elementy platformy mogą podlegać innym rygorom regulacyjnym niż inne składowe lub dwa podmioty świadczące porównywalne usługi miałyby inny zakres obowiązków.

3. Nie jest jasny zakres projektu rozporządzenia odnoszący się do usług związanych z komunikowaniem się. Z jednej strony motyw 14 zawiera wykluczenie z zakresu regulacji usług określonych w Dyrektywie 2018/1972 takich jak email i prywatne komunikatory (*e-mails or private communicators*). Z drugiej jednak strony w motywie 27 wskazano: „*Likewise, services used for communications purposes, and the technical means of their delivery, have also evolved considerably, giving rise to online services such as Voice over IP, messaging services and web-based e-mail services, where the communication is delivered via an internet access service. Those services, too, can benefit from the exemptions from liability, to the extent that they qualify as 'mere conduit', 'caching' or hosting service*." Z tekstu tego można wywnioskować, że usługi typu „*VOiP, messaging services, web-based e-mails*" mogą korzystać z wyjątków od odpowiedzialności pod określonym warunkiem, co sugerowałoby, że jednak są w jakimś zakresie objęte projektem regulacji. Konieczne jest wyraźne sprecyzowanie, czy i które usługi łączności interpersonalnej, objęte są wymogami rozporządzenia.

4. Postulujemy jednoznaczne wyłączenie spod DSA usług chmurowych Business-to-Business, w których usługa chmurowa dostawcy, z której korzysta użytkownik biznesowy (przedsiębiorstwo/organizacja) nie jest usługą dla odbiorców tego użytkownika biznesowego. Przykładami takich sytuacji mogą być:
   - serwis medialny uruchomiony przez firmę X na platformie dostawcy Y (maszyny wirtualne, bazy danych, zarządzanie chmurą);
   - platforma handlowa uruchomiona przez firmę A na platformie dostawcy B;
   - maszyny wirtualne używane przez firmę A na platformie dostawcy B;
   - system CRM firmy X uruchomiony przez firmę Z na platformie dostawcy Y;

   itp.

   W przypadkach takich jak opisane powyżej dostawca usługi chmurowej nie ma wpływu ani na zakres, ani na cele przetwarzania, ani na sposób prowadzenia działalności gospodarczej, jak

również nie ma wpływu na treści jakie są publikowane lub rozprzestrzeniane przez swojego biznesowego kontrahenta.
Zapis ten musi być precyzyjny, ponieważ w DSA pojawia się pojęcie „*recipient of the service*", które może dotyczyć zarówno osoby fizycznej, jak i prawnej (np. przedsiębiorstwa, organizacji). Zaś w definicjach „*intermediary services*", jak i w późniejszym ich opisie, można znaleźć opis serwisów, które mogą zgadzać się z ogólnym opisem i definicją serwisów chmurowych (por. European Commission Cloud Strategy (europa.eu) – strona 5, powszechnie znana definicja NIST lub definicje znajdujące się w takich dokumentach jak UCHWAŁA NR 97 RADY MINISTRÓW z dnia 11 września 2019 r. w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa" lub Komunikat KNF z 23 stycznia 2020 roku.)
Z powyższego wynika, że nie można ograniczyć zastosowania DSA tylko do sytuacji, kiedy klientem usługi jest osoba fizyczna (konsument). Jednak poszerzenie zasięgu działania DSA na wszelkie czynności przetwarzania w serwisach B2B (serwisach chmurowych) i nakładanie dodatkowych obowiązków wynikających z DSA wydaje się nietrafione. Zaznaczamy jeszcze raz, że wyłączenie dotyczyłoby serwisów chmurowych B2B jak opisanych powyżej, natomiast nie dotyczyłoby serwisów B2C i „*information society services*" jak jest to zapisane w DSA.
Pozostawiamy otwarte czy powinno to znaleźć się jako dodatkowy motyw w Rozporządzeniu (tak jak to jest zaznaczone w motywie (14) wyłączającym niektóre usługi), czy też w artykułach Rozporządzenia, np. w definicjach „*intermediary services*". Ponawiamy jednak apel o precyzyjność zapisu.

5. Proponujemy, aby w zakresie motywu 36 i art. 10 (dot. punktów kontaktowych) oprócz wskazanych w przepisach języków istniał wymóg przyjmowania zgłoszeń w języku angielskim. W powiązaniu z art. 8.2.c. uznać należy, że brak języka angielskiego jako wymaganego może doprowadzić do sytuacji braku możliwości komunikacji z pośrednikiem internetowym, który oprócz języka narodowego wskaże do komunikacji mało znany język obowiązujący w UE. W efekcie zgłaszający użytkownicy indywidualni, *trusted flaggers* lub inne podmioty musiałyby zatrudniać tłumaczy tylko do zgłaszania naruszeń praw. Taka sama uwaga w zakresie języka odnosi się do art. 9 ust. 2. c.

6. W zakresie motywów 36-37 oraz art. 10 i 11 przepisy nie przewidują sytuacji, gdy pośrednik spoza UE nie spełni wynikających z nich obowiązków. Powstaje pytanie, czy jest jakaś sankcja za brak przedstawicielstwa w UE, poza art. 40? Czy można taki serwis np. wyłączyć na terenie UE na zasadzie art. 41.2. b, 41.3.b? Wiele nielegalnych treści (różnego rodzaju) dostępnych w UE pojawia się on-line za pośrednictwem przedsiębiorców zarejestrowanych w egzotycznych lokalizacjach, którzy nie przestrzegają przepisów prawa obowiązujących na terenie UE. Rozporządzenie powinno uwzględniać takie sytuacje oraz przewidywać odpowiednie sankcje pozwalające na skuteczne uniemożliwienie dostępu do nielegalnych treści hostowanych przez tego typu podmioty.

7. Popieramy wyraźne wskazanie w motywach, że pośrednik, który świadomie współpracuje z użytkownikiem usługi celem podjęcia działań nielegalnych nie świadczy usługi w sposób neutralny i tym samym nie może korzystać z wyłączenia odpowiedzialności przewidzianego w regulacji (motyw 20).

8. Wprowadzenie „zasady dobrego Samarytanina” (motyw 25 i art.6) jest słuszne, jako że pośrednik nie powinien być karany za samo podejmowanie w dobrej wierze proaktywnych działań w celu usuwania nielegalnych treści, ponad obowiązki wynikających z ustaw i rozporządzeń. Pośrednicy powinni być do takich działań wręcz zachęcani. Tym niemniej warto jeszcze wyraźniej wskazać, że zasada ta nie zwalnia pośrednika z odpowiedzialności związanej z obowiązkiem należytego reagowania w ramach procedury *notice and action* oraz wskutek otrzymania nakazu od uprawnionego organu. Istotne jest zatem, aby rozporządzenie DSA wyraźnie wskazywało, że nie tworzy ono zasady zwolnienia z odpowiedzialności dla tych usług pośrednictwa, które prowadzą z własnej inicjatywy dobrowolne działania mające na celu wykrywanie, identyfikację i usuwanie lub uniemożliwianie dostępu do nielegalnych treści. W szczególności, regulacje rozporządzenia DSA nie powinny prowadzić do przyjęcia zasady, że te dobrowolne środki nie prowadzą do uzyskania wiedzy w rozumieniu art. 5 rozporządzenia DSA.

   Wskazać też należy na aktualnie obowiązujące uregulowanie odpowiedzialności pośredników zawarte w art. 12-15 dyrektywy o handlu elektronicznym[1], które jak wskazuje Komisja powinno być zachowane w niezmienionej formie po jego przeniesieniu ze wskazanej wyżej dyrektywy do rozporządzenia DSA:

   - Głównym celem wprowadzenia „zasady dobrego Samarytanina”, zgodnie z motywem 25 rozporządzenia DSA, jest niezniechęcanie dostawców usług internetowych do dobrowolnych działań mających na celu zwalczanie treści niezgodnych z prawem. Obecnie obowiązujące regulacje art. 12-15 dyrektywy o handlu elektronicznym dotyczące odpowiedzialności pośredników nie stanowią czynnika zniechęcającego pośredników do takich działań. Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wyjaśnił, że przywileje związane z odpowiedzialnością z tytułu świadczenia usług hostingu są niedostępne dla dostawcy tych usług w przypadku, gdy dostawca usług nie podejmuje działań, pomimo że jest świadomy faktów lub okoliczności, na podstawie których rzetelny podmiot gospodarczy powinien zidentyfikować treść niezgodną z prawem i uniemożliwić dostęp do niej. TSUE wyjaśnił również wyraźnie, że utrata przywileju dotyczącego odpowiedzialności jest związana z *promowaniem* treści niezgodnych z prawem, a nie z uniemożliwianiem dostępu do nich, co jest obowiązkiem odstawy usług w każdym przypadku po uzyskaniu wiedzy lub znajomości faktów[2].

[1] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym*)*

[2] Sprawa L’Oréal/eBay (C-324/09):*“[S]am fakt, że operator rynku elektronicznego online przechowuje na swoim serwerze oferty sprzedaży, określa warunki jego funkcjonowania, jest za to wynagradzany i udziela swym klientom informacji o charakterze ogólnym, nie może prowadzić jeszcze do pozbawienia skuteczności przewidzianych dyrektywą 2000/31 odstępstw w zakresie odpowiedzialności (zob. analogicznie ww. wyrok w sprawach połączonych Google France i Google, pkt 116). Jeżeli jednak wspomniany operator udziela wsparcia, które polega w szczególności na optymalizacji prezentacji danych ofert sprzedaży lub na ich promocji, należy stwierdzić, że nie zachowuje on neutralnej pozycji między danym klientem(sprzedającym) a potencjalnymi nabywcami, lecz odgrywa czynną rolę, która może pozwolić mu na powzięcie wiedzy*

- Potrzeba podejmowania proaktywnych działań w zakresie zwalczania nielegalnych treści zawarta jest w już dokumentach unijnych. Komisja Europejska zarówno w swoim komunikacie z 2017 r. w sprawie zwalczania niezgodnych z prawem treści w Internecie[3], jak i w wynikającym z niego zaleceniu, wyraźnie stwierdziła, że środki mogą, a nawet powinny obejmować również proaktywne środki służące do wykrywania i usuwania niezgodnych z prawem treści w środowisku online. Komisja uznała również, że podjęcie takich dobrowolnych proaktywnych środków nie prowadzi automatycznie do utraty przez platformę internetową korzyści wynikających ze zwolnienia z odpowiedzialności przewidzianego w art. 14 dyrektywy o handlu elektronicznym. Ponadto Komisja wyjaśniła, że zwolnienie z odpowiedzialności jest dostępne jedynie dla dostawców usług hostingowych, którzy spełniają warunki określone w art. 14 dyrektywy o handlu elektronicznym.

9. Propozycja rozporządzenia DSA obejmuje wykreślenie art. 12-14 dyrektywy o handlu elektronicznym i ich powtórzenie ich w art. 3-5 rozporządzenia DSA. Komisja wyraźnie stwierdziła, że zabieg ten nie ma na celu zmiany zasad odpowiedzialności dostawców usług wymienionych w powyższych przepisach. Jednak należy zwrócić uwagę na to, aby powyższe rozwiązanie nie doprowadziło faktycznie do otwarcia dotychczasowych regulacji na zmiany skutkujące zawężeniem albo poszerzeniem zakresu zwolnień dostawców usług z odpowiedzialności za nielegalne treści i zakwestionowania istniejących albo tworzenia nowych tzw. „bezpiecznych przystani".

   W powyższym kontekście należy zwrócić uwagę na to, że propozycja rozporządzenia wskazuje na konieczność „wyjaśnienia" („*clarification*") zasad odpowiedzialności przez wprowadzenie „zasady dobrego Samarytanina". Ponadto, sporządzone z inicjatywy Parlamentu Europejskiego[4] sprawozdanie dotyczące propozycji rozporządzenia DSA wspomina, że mechanizm *notice and action* określony w rozporządzeniu DSA powinien "*zagwarantować, że zawiadomienia nie spowodują automatycznego pociągnięcia do odpowiedzialności prawnej, ani nie nałożą żadnego wymogu usunięcia, w odniesieniu do konkretnych treści lub oceny legalności*"[5]. Literalne brzmienie tego stwierdzenia rodzi wątpliwości w kontekście warunków odpowiedzialności określonych w dyrektywie o handlu elektronicznym. Dodatkowo, w ramach przeniesienia regulacji art. 12-14 dyrektywy o handlu elektronicznym do rozporządzenia DSA, dokonano też zmiany terminologii w motywach tych dokumentów dotyczących zasad odpowiedzialności dostawców usług, tj. ze sformułowania „pasywnego charakteru" („*passive*

o danych dotyczących poszczególnych ofert lub na sprawowanie nad nimi kontroli. A zatem w odniesieniu do wspomnianych danych nie może on powoływać się na odstępstwo w zakresie odpowiedzialności, o którym mowa w art. 14 dyrektywy."

[3] pkt 3.3. Komunikatu: https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms

[4] Report with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL): https://www.europarl.europa.eu/doceo/document/A-9-2020-0181_EN.html

[5] *„That notice-and-action mechanism should: (…) guarantee that notices will not automatically trigger legal liability nor should they impose any removal requirement, for specific pieces of the content or for the legality assessment"*

nature") usług, jak w motywie (42) dyrektywy o handlu elektronicznym, koniecznego do zwolnienia z odpowiedzialności, na sformułowanie „neutralnego" świadczenia usług, jak w motywach 18, 20 i 25 rozporządzenia DSA. Praktyczne znaczenie takiej zmiany nie jest jasne.

10. Projektodawca słusznie pozostawił zasadę braku ogólnego obowiązku monitorowania przez pośredników internetowych treści zamieszczanych przez użytkowników. Warto jednocześnie zauważyć, iż nie wykluczył obowiązku monitorowania w specyficznych przypadkach, aczkolwiek niestety odnosi się do tej kwestii jedynie na poziomie motywu 28, a nie przepisu regulacji. Warto byłoby rozważyć wskazanie tego wprost w tekście art. 7.

11. Istotne jest przewidziane w art. 13 i 23 obowiązku transparentności i raportowania nie naruszały tajemnicy przedsiębiorstwa, poufności umów handlowych i prywatności użytkowników. Transparentność nie musi być równoznaczna z podawaniem szerokich danych i wszystkich żądanych informacji do wiadomości publicznej, w zakresie, w którym informacje dotykają tajemnicy handlowej i poufności powinny być one przekazywane wyłącznie poprzez raporty kierowane do organów nadzorujących i Komisji Europejskiej i jedynie w ramach formalnych procesów raportowych, gwarantujących bezpieczeństwo tak przekazywanych informacji. Komisja Europejska powinna zadbać o to, aby obowiązujące zasady raportowania były sprawiedliwe, proporcjonalne i jednolite we wszystkich krajach UE.

    W odniesieniu do procedury kierowania do pośredników nakazów podjęcia działań dot. treści nielegalnych (art.8), *jak też procedury notice and action* (art.14) nasze zastrzeżenie budzi to, że wymóg wskazania przez zgłaszającego dokładnej/dokładnych *url* jako elektronicznej lokalizacji nielegalnych treści może być uznany nie za fakultatywny, lecz obowiązkowy. Dotychczasowe doświadczenia wskazują, że w przypadku niektórych typów nielegalnych treści oraz technologii podanie dokładnej *ur*l nie zawsze jest skutecznym środkiem do trwałego usunięcia nielegalnej treści, jako że treści usunięte spod konkretnej *url* mogą natychmiast pojawiać się ponownie pod nieco zmienionym *ur*l. Z tego względu powiadomienie umożliwiające pośrednikowi jednoznaczną identyfikację nielegalnych treści powinno być dostosowane do rodzaju treści oraz technologii udostępniania treści, a podanie dokładnej *url* powinno być traktowane jako jeden ze sposobów, a nie bezwzględnie wymagany sposób wskazania elektronicznej lokalizacji nielegalnych treści lub ich identyfikacji. Jednocześnie pozytywnie odbieramy fakt, że przepisy w tym zakresie przewidują podanie przez zgłaszającego/organ wydający nakaz dodatkowych informacji istotnych dla danego przypadku. Uzasadniony jest także przepis umożliwiający powiadamianie o kilku treściach bezprawnych poprzez jedno zgłoszenie. Wymóg dotyczący adresu URL jest problematyczny również w przypadku nielegalnych usług i platform strukturalnie naruszających prawo, ponieważ nie przewidziano przepisu "stay-down", więc te same treści naruszające prawo będą wielokrotnie umieszczane za pomocą różnych adresów URL.

12. Z zadowoleniem przyjmujemy przepisy dot. roli samoregulacji, w szczególności z uwagi na fakt, że na rynku polskim funkcjonują już z powodzeniem kodeksy samoregulacyjne odnoszące się do rzeczywistości internetowej, w tym reklamy on-line i treści udostępnianych w internecie.

13. Odnosząc się do kwestii krajowego organu nadzorującego, pragniemy na tym etapie prac nad dokumentem jedynie wskazać, że z punktu widzenia przedsiębiorców korzystne byłoby, aby był to jeden organ, celem uniknięcia rozproszenia odpowiedzialności i zadań pomiędzy kilka organów, co zwiększa niepewność prawną i może skutkować różnymi podejściami interpretacyjnymi do danego przepisu. Nie chcemy jeszcze przesądzać, czy w Polsce Koordynator ds. Usług Cyfrowych (*Digital Services Coordinator*) powinien działać w ramach nowo powołanego organu, czy też być przypisany do jednego z istniejących już organów regulacyjnych i nadzorujących. Zdecydowanie dobrze oceniamy wymóg niezależności koordynatorów krajowych od rządów oraz konieczność jak największej koordynacji z unijnymi partnerami, co ułatwi jednolite stosowanie prawa. Jest to szczególnie ważne z uwagi na szeroki zakres kompetencji nowych podmiotów (poza nakładaniem kar, wydawanie decyzji administracyjnych, kontrole, nakaz udostępniania dokumentów). Wszystkie te nowe zasady oraz kompetencje będą musiały być szczegółowo przeanalizowane pod kątem potencjalnych naruszeń swobody prowadzenia działalności gospodarczej i konieczności poszanowania tajemnicy przedsiębiorstwa.

14. Art. 17 opisujący zasady działania wewnętrznego systemu rozpatrywania przez platformę skarg/wniosków składanych przez użytkowników (*internal complaint handling system*) odnosi się wyłącznie do sytuacji, gdy wskutek zgłoszenia nielegalnej treści platforma podejmuje decyzję o:
    i. usunięciu tej treści lub uniemożliwieniu do niej dostępu;
    ii. zawieszeniu lub uniemożliwienia użytkownikowi korzystania z usługi;
    iii. zawieszeniu lub zamknięciu konta użytkownika

    i użytkownik kwestionuje którąś z powyższych decyzji. Nie jest natomiast w ogóle przewidziana i opisana procedura składania skargi na decyzję platformy o niepodejmowaniu żadnego z powyższych działań i pozostawieniu treści, której dotyczyło zgłoszenie. Podobne ograniczenie dotyczy przesłanek do rozstrzygnięcia sporu w drodze procedury pozasądowej mediacji, którą szczegółowe opisano w art.18. Zakładamy, że jest to niedopatrzenie ze strony unijnego legislatora i że celem przepisów nie było ograniczenie prawa do skutecznego sprzeciwu i rozwiązania sporu dotyczącego treści, która decyzją platformy, nie została usunięta wskutek zgłoszenia w ramach procedury *notice and action.* Dlatego postulujemy stosowne uzupełnienie przepisów w tym zakresie.

15. Pragniemy zwrócić uwagę na kolejne wątpliwości dot. art. 18 oraz motywu 45, które ustanawiają dedykowaną procedurę polubowną, acz obowiązkową obok istniejącej już regulacji w tym zakresie ADR/ODR. Nie jest jasne jaka byłaby relacja opisanej w nim procedury do istniejących już przepisów prawa konsumenckiego dot. ODR/ADR. Mamy wątpliwości czy takie mnożenie organów i procedur jest efektywne, szczególnie w odniesieniu do konsumentów, oraz jak w praktyce będą funkcjonować potencjalnie równoległe sprzeczne orzeczenia różnych organów i sądów podjęte w tym samym sporze.

    Ponadto, przewidziany mechanizm, w którym użytkownik nigdy nie ponosi kosztów mediacji, nawet gdy przegrywa postępowanie mediacyjne, rodzi ryzyko nadużyć i jest nieproporcjonalny.

Niezbędne jest utrzymanie ogólnej zasady procesowej, zgodnie z którą strona przegrywająca spór ponosi jego koszty.

Mechanizmy ADR należy zabezpieczyć przez złym wykorzystaniem. Jeśli przepisy, które pozwoliłyby każdej osobie - w tym podmiotom działającym w złej wierze - na korzystanie z alternatywnych metod rozwiązywania sporów w celu rozstrzygnięcia każdego sporu, to otwiera to drogę do nadużyć. Efektem będą miliony decyzji podejmowanych przez platformy ad hoc, co może osłabić próby opracowania solidnych i przejrzystych systemów zarządzania treściami. Na przykład podmioty objęte ochroną mogą zareagować, składając bardziej ogólne oświadczenia w ramach polityki moderowania treści, aby uniknąć zarzutów o niespójność działań; alternatywnie, polityki i praktyki podmiotów objętych ochroną mogą stać się zbyt sztywne, niezdolne do dostosowania się do stale zmieniającego się otoczenia w treściach online z obawy, że staną w obliczu zarzutów o niespójność. Z tego powodu uważamy, że bardziej właściwe jest, aby organ regulacyjny nadzorował, na poziomie systemowym, procesy odwoławcze.

16. Pozytywnie odnosimy się do roli przypisanej „trusted flaggers" w procesie zawiadamiania o towarach i treściach nielegalnych, która w naszej ocenie przyczyni się do szybszego ich usuwania z przestrzeni internetowej. Dla właściwego funkcjonowanie tego rodzaju „sygnalistów" niezmiernie ważne jest jednak, aby działali oni w sposób całkowicie neutralny i wolny od jakichkolwiek uprzedzeń. Tendencyjne ocenianie wpisów może bowiem skutkować naruszeniem zasady swobody wypowiedzi.

17. Popieramy przepisy art. 20, które upoważniają platformy do podejmowania działań wobec użytkowników i podmiotów umieszczających nielegalne treści oraz dokonujących częstych nieuzasadnionych zgłoszeń. Zwiększają one pewność prawną działalności platform, jako że konkretne działanie platformy w takich przypadkach nie będzie oparte wyłącznie o regulamin platformy (*Terms and Conditions*), który użytkownicy mogą zaskarżyć, lecz o wyraźne przepisy prawa.

    Rozumiemy przyczyny wprowadzenia poprzez art.22 i odpowiadający mu motyw 49 obowiązku identyfikacji wiarygodności użytkowników biznesowych (*traderów*) przez platformy e-commerce, co w założeniu ma przyczynić się do zwiększenia zaufania użytkowników do zakupów on-line i do ograniczenia pojawiania się nielegalnych produktów, usług i treści na tych platformach. Wątpliwości budzi jednak nałożenie obowiązku dołożenia starań („*make reasonable efforts*") przy weryfikacji rzetelności podawanych danych. Można zasadnie wątpić, czy tego rodzaju działania weryfikujące, które będą stanowić istotne obciążenie, są celowe. Pragniemy ponadto wskazać na pewną lukę w przepisach. art. 22 ust. 4 nakłada na platformę e-commerce obowiązek usunięcia danych *tradera* wskazanych w ust. 1 i 2 po zakończeniu relacji kontraktowej z tymże *traderem*. Nie ma obowiązku retencji danych, tymczasem retencja takich danych przez 2 lata na potrzeby organów śledczych umożliwiłaby znacznie skuteczniejsze wykrywanie przestępstw związanych z udostępnianiem nielegalnych produktów/treści/usług. Z punktu widzenia dalszego rozwoju e-commerce i związanej z tym ochrony użytkownika ważny i potrzebny jest przepis wprowadzony w art. 22 ust. 7 – czyli

obowiązek dostosowania interfejsów platform w sposób umożliwiający realizację „*traderom*" obowiązków ustawowych, co powinno ułatwić należyte zapewnienie informacji przedkontraktowych, polityk prywatności czy zgód.

Ponadto, zakres powyższej zasady, tzw. „*Know Your Business Customer*" („KYBC"), w formule proponowanej w rozporządzeniu DSA jest zbyt wąski. Ogranicza się on do platform, które umożliwiają "konsumentom zawieranie z przedsiębiorcami umów na odległość", tj. rynków, wykluczając tym samym inne usługi. W związku z tym, nie zapewnia on znaczącej pomocy w zwalczaniu nielegalnych stron internetowych, które zawierają umowy o korzystanie z takich usług. Obowiązki KYBC powinny mieć również zastosowanie do usług, na których opierają się serwisy pirackie i inni dostawcy nielegalnych usług. Zobowiązanie szerszego zakresu przedsiębiorców do ujawniania swojej tożsamości w Internecie automatycznie ograniczyłoby dostęp do nielegalnych lub szkodliwych treści w sieci. Argumenty przemawiające za zasadnością rozszerzenia zakresu stosowania art. 22 rozporządzenia DSA są następujące:

- Treści art. 5 dyrektywy o handlu elektronicznym zawiera już obowiązek identyfikacji przedsiębiorstw na ich stronach internetowych. W artykule tym brakuje jednak odpowiednich sankcji. Stąd przedsiębiorstwa, które zamierzają czerpać zyski z treści niezgodnych z prawem, nie wypełniają tego obowiązku i nie ponoszą żadnych konsekwencji. Rozporządzenie DSA stanowi okazję do naprawienia tej sytuacji.
- Rozszerzenie zastosowania art. 22 rozporządzenia byłoby zgodne z wyraźnymi celami tej inicjatywy prawodawczej, a mianowicie stworzeniem bezpiecznego, przewidywalnego i zaufanego środowiska online. Przedsiębiorstwa nie mogą korzystać z Internetu bez nazwy domeny, bez hostingu lub bez usług reklamowych czy płatniczych. Te usługi pośrednictwa, mające bezpośredni związek z przedsiębiorstwem, są zatem w stanie najlepiej zapewnić dostęp do swoich usług jedynie tym przedsiębiorstwom, które są gotowe przestrzegać obowiązujących przepisów dotyczących identyfikacji. W przypadku, gdyby pośrednik nie dokonał weryfikacji tożsamości swojego klienta biznesowego, musiałby zaprzestać świadczenia usług na rzecz danego klienta, co stanowiłoby istotny czynnik zniechęcający do prowadzenia nielegalnej lub szkodliwej działalności.
- Obowiązki KYBC wydają się być bardzo dobrym narzędziem, ponieważ nakładają one minimalne obciążenia na legalnie działające przedsiębiorstwa, z których wszystkie są łatwe do zidentyfikowania.
- Obowiązki w zakresie zasady KYBC już istnieją, np. w treści dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE). Istnieją już publicznie dostępne rejestry identyfikujące przedsiębiorców, w tym: krajowe rejestry spółek (w Polsce: Krajowy Rejestr Sądowy KRS), europejski rejestr działalności gospodarczej (EBR), czy rejestr beneficjentów ostatecznych (w Polsce: Centralny Rejestr Beneficjentów Rzeczywistych CRBR). Dostępność tych baz danych sprawia, że obowiązki KYBC są łatwe do wdrożenia przy minimalnych obciążeniach administracyjnych w ramach procesu rejestracji i późniejszych weryfikacji.
- Ograniczenie zakresu zastosowania zasady KYBC do rynków internetowych byłoby straconą szansą na zajęcie się kwestią nielegalnych treści w Internecie w szerokim zakresie. Również Parlament Europejski wzywał do wprowadzenia w propozycji

rozporządzenia obowiązków dotyczących KYBC o szerokim zakresie, czyli nie tylko w odniesieniu do rynków).

18. W art. 41 ust. 3. b, biorąc pod uwagę cel, jakim jest skuteczność przepisu, można byłoby rozważyć zmiany treści z koniunkcji, na alternatywę i tym samym brzmienie: *"where the Digital Services Coordinator considers that the provider has not sufficiently complied with the requirements of the first indent, that the infringement persists and causes serious harm~~,~~ ~~and~~ or that the infringement entails a serious criminal offence involving a threat to the life or safety of persons, request the competent judicial authority of that Member State to order the temporary restriction of access of recipients of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider of intermediary services on which the infringement takes place*".