CYFROWA POLSKA

Warszawa, dnia 16 września 2025 r.

Szanowny Pan

Krzysztof Gawkowski

Wiceprezes Rady Ministrów,

Minister Cyfryzacji

Szanowny Panie Premierze,

W imieniu Związku Cyfrowa Polska mam przyjemność przekazać opracowanie pt. „Propozycje uproszczenia unijnych regulacji cyfrowych", zawierające nasze rekomendacje dotyczące uproszczenia ram prawnych kształtujących funkcjonowanie gospodarki cyfrowej w Unii Europejskiej.

Obecne skomplikowane i kosztowne procedury w rozdrobnionych systemach krajowych utrudniają wykorzystanie potencjału jednolitego rynku. Podejście regulacyjne Unii hamuje innowacje, a przedsiębiorstwa cyfrowe zniechęca do działania w wielu krajach UE różnorodność wymogów, mnożenie instytucji regulacyjnych i tzw. gold-plating prawa unijnego. W efekcie z tak dużym obciążeniem są w stanie poradzić sobie głównie największe przedsiębiorstwa – często spoza UE – podczas gdy młode innowacyjne spółki rezygnują z działalności na rynku europejskim.

Opracowanie, które mam przyjemność przedstawić w załączeniu do niniejszego pisma zawiera diagnozę obecnej sytuacji oraz rekomendacje konkretnych uproszczeń regulacyjnych. Ich celem jest zmniejszenie ilości niepotrzebnych, biurokratycznych barier i obciążeń oraz uproszczenie całego ekosystemu unijnych regulacji cyfrowych, celem odblokowania potencjału do innowacji na jednolitym rynku cyfrowym w Unii Europejskiej.

Dokument ten wpisuje się w szerszą dyskusję o potrzebie ujednolicenia i uproszczenia licznych regulacji cyfrowych obowiązujących w UE. Obecnie przedsiębiorcy muszą mierzyć się z dziesiątkami aktów prawnych o nakładających się obowiązkach, a także z fragmentacją i zróżnicowaną praktyką państw członkowskich. Stworzenie bardziej spójnych, przejrzystych i efektywnych ram prawnych to klucz do tego, aby regulacje zamiast być barierą – stały się narzędziem wspierającym rozwój innowacyjnych usług i technologii w Europie.

W dokumencie analizujemy kluczowe obszary prawne, w tym:

- **sztuczną inteligencję (AI Act)** - potrzebę proporcjonalnych, opartych na ryzyku regulacji wspierających innowacje,
- **regulacje dotyczące treści (DSA, dyrektywy sektorowe)** - ograniczenie dublujących się obowiązków i uproszczenie sprawozdawczości,
- **prywatność i ochronę danych (RODO, ePrivacy)** - większą przejrzystość, pewność prawa i dostosowanie do realiów nowej generacji technologii,
- **bezpieczeństwo i cyberbezpieczeństwo (NIS2, CRA, inne akty)** - harmonizację wymogów i redukcję obciążeń biurokratycznych,
- **rynek cyfrowy (DMA)** - zapewnienie spójności i przewidywalności regulacyjnej.

Jako Związek przekazujemy niniejsze opracowanie, aby mogło służyć jako inspiracja i praktyczne wskazówki dla stanowiska Polski na forum Unii Europejskiej wobec zestawu propozycji legislacyjnych Unii Europejskiej mających na celu uproszczenie regulacji. Uważamy, że nasz kraj powinien aktywnie wspierać inicjatywy prowadzące do uproszczenia otoczenia regulacyjnego, co wzmocni zarówno konkurencyjność gospodarki europejskiej, jak i polskiej.

Naszym zdaniem uproszczenie i ujednolicenie przepisów w obszarze cyfrowym będzie miało fundamentalne znaczenie dla zwiększenia konkurencyjności, przyciągania inwestycji i budowy silnej pozycji Europy w globalnym wyścigu technologicznym.

Mam nadzieję, że nasze opracowanie okaże się użyteczne i pozwoli na realizację ambitnych i słusznych celów z zakresu uproszczenia unijnego otoczenia prawnego z korzyścią dla europejskiej i krajowej gospodarki oraz naszego potencjału innowacyjnego. Pozostaję do Pana pełnej dyspozycji.

Z wyrazami szacunku,

Michał Kanownik

Prezes Zarządu

Związek Cyfrowa Polska

Załączniki:

1. PROPOZYCJE UPROSZCZENIA UNIJNYCH REGULACJI CYFROWYCH ZWIĄZKU CYFROWA POLSKA

PROPOZYCJE UPROSZCZENIA UNIJNYCH REGULACJI CYFROWYCH

ZWIĄZKU CYFROWA POLSKA

Spis treści:

WSTĘP

Za wstęp do niniejszego opracowania może posłużyć następujący passus z raportu przygotowanego na zlecenie Komisji Europejskiej przez Mario Draghiego "A competitiveness strategy for Europe" (cześć A, str. 30):

> *Regulatory barriers to scaling up are particularly onerous in the tech sector, especially for young companies.* [...] *Regulatory barriers constrain growth in several ways. First, complex and costly procedures across fragmented national systems discourage inventors from filing Intellectual Property Rights (IPRs), hindering young companies from leveraging the Single Market. Second, the EU's regulatory stance towards tech companies hampers innovation: the EU now has around 100 tech-focused laws and over 270 regulators active in digital networks across all Member States. Many EU laws take a precautionary approach, dictating specific business practices ex ante to avert potential risks ex post. For example, the AI Act imposes additional regulatory requirements on general purpose AI models that exceed a pre-defined threshold of computational power – a threshold which some state-of-the-art models already exceed. Third, digital companies are deterred from doing business across the EU via subsidiaries, as they face heterogeneous requirements, a proliferation of regulatory agencies and "gold plating" of EU legislation by national authorities. Fourth, limitations on data storing and processing create high compliance costs and hinder the creation of large, integrated data sets for training AI models. This fragmentation puts EU companies at a disadvantage relative to the US, which relies on the private sector to build vast data sets, and China, which can leverage its central institutions for data aggregation. This problem is compounded by EU competition enforcement possibly inhibiting intra-industry cooperation. Finally, multiple different national rules in public procurement generate high ongoing costs for cloud providers. The net effect of this burden of regulation is that only larger companies – which are often non-EU based – have the financial capacity and incentive to bear the costs of complying. Young innovative tech companies may choose not to operate in the EU at all.*

Wnioski płynące z raportu są jasne: unijne bariery regulacyjne szczególnie mocno utrudniają rozwój przedsiębiorstw technologicznych, zwłaszcza młodych. Problem ten ma wiele wymiarów:

- Skomplikowane i kosztowne procedury w rozdrobnionych systemach krajowych utrudniają wykorzystanie potencjału jednolitego rynku.
- Podejście regulacyjne Unii hamuje innowacje. Obecnie obowiązuje około 100 aktów prawnych dotyczących technologii i działa ponad 270 organów nadzorujących sieci cyfrowe we wszystkich państwach członkowskich. Wiele przepisów ma charakter ostrożnościowy, z góry narzucając szczegółowe praktyki biznesowe, by uniknąć potencjalnych zagrożeń w przyszłości. Przykładem jest Akt w sprawie sztucznej inteligencji, który nakłada dodatkowe wymogi na modele AI ogólnego przeznaczenia przekraczające określony próg mocy obliczeniowej – który to część najnowszych modeli już dziś przekracza.

- Przedsiębiorstwa cyfrowe zniechęca do działania w wielu krajach UE różnorodność wymogów, mnożenie instytucji regulacyjnych i tzw. *gold-plating* prawa unijnego.

- Ograniczenia w przechowywaniu i przetwarzaniu danych podnoszą koszty i utrudniają budowę dużych, zintegrowanych zbiorów danych potrzebnych do szkolenia modeli AI. Skutkuje to gorszą pozycją unijnych przedsiębiorstw wobec USA, gdzie sektor prywatny swobodnie tworzy takie zbiory, i Chin, które wykorzystują centralne instytucje państwowe do agregowania danych. Sytuację dodatkowo pogarsza sposób egzekwowania prawa konkurencji, mogący utrudniać współpracę w obrębie branży.

- Różnice w przepisach dotyczących zamówień publicznych w poszczególnych krajach generują wysokie koszty stałe dla dostawców usług chmurowych.

W efekcie z tak dużym obciążeniem są w stanie poradzić sobie głównie największe przedsiębiorstwa – często spoza UE – podczas gdy młode innowacyjne spółki rezygnują z działalności na rynku europejskim.

Diagnoza ta wyznacza ramy dla rekomendacji konkretnych uproszczeń regulacyjnych przedstawionych w niniejszym opracowaniu. Ich celem jest zmniejszenie ilości niepotrzebnych, biurokratycznych barier i obciążeń oraz uproszczenie całego ekosystemu unijnych regulacji cyfrowych, celem odblokowania potencjału do innowacji na jednolitym rynku cyfrowym w Unii Europejskiej

PROPOZYCJE UPROSZCZENIA UNIJNYCH REGULACJI CYFROWYCH

Na poparcie zasługują ambitne cele Kompasu konkurencyjności Komisji Europejskiej, zakładające wzmocnienie wyników gospodarczych Europy i wykorzystanie rewolucji związanej ze sztuczną inteligencją oraz cyfryzacją. Uproszczenie regulacji, obejmujące ograniczenie obciążeń i usprawnienie procesów, będzie kluczowe dla stworzenia środowiska sprzyjającego innowacjom. Unia Europejska może podjąć pozytywne kroki, aby ożywić swoją gospodarkę, zwłaszcza w obszarze cyfrowym:

- Przyspieszyć wdrażanie najlepszych technologii w kluczowych branżach oraz wspierać inwestycje w przełomowe innowacje w najbardziej obiecujących segmentach łańcucha wartości AI;
- Skierować większe inwestycje w infrastrukturę obliczeniową, sieci i umiejętności cyfrowe – fundamenty dobrze prosperującej gospodarki cyfrowej;
- Rzetelnie oceniać prawdopodobne skutki gospodarcze projektowanych regulacji technologicznych, zapewniając, że będą one wspierać, a nie tłumić innowacje, z uwzględnieniem całościowego wpływu na szerokie grono interesariuszy.

Unia Europejska będzie mierzyć się z wyzwaniami w dążeniu do realizacji tej wizji:

1. **Złożoność regulacyjna:** krajobraz regulacyjny staje się coraz bardziej skomplikowany, a niektóre przepisy nakładają się, są przestarzałe lub sprzeczne ze sobą. Obecne ramy regulacyjne już spowalniają wprowadzanie na rynek produktów wykorzystujących AI w UE. W konsekwencji konsumenci i przedsiębiorstwa w UE mają dostęp do mniejszej liczby narzędzi AI niż odbiorcy w pozostałych częściach świata.

   Instytucje UE powinny powstrzymać się przed dalszym wprowadzaniem nowych regulacji, które nałożą kolejne warstwy przepisów w już przepełnionej przestrzeni regulacyjnej oraz ograniczą konkurencyjność. Ważne jest, aby przed wprowadzeniem kolejnych regulacji w pełni usystematyzować, doprecyzować i wdrożyć wszystkie niedawno przyjęte akty prawne, zamiast poszerzać ich zakres lub zmieniać je bez uzasadnienia.

2. **Wymogi sprawozdawcze**: to kluczowy obszar wymagający analizy. Dużą pomocą byłoby uproszczenie, poprzez harmonizację, obowiązków w zakresie dezinformacji, cyberbezpieczeństwa, zrównoważonego rozwoju i przetwarzania danych. Przykładowo, unijne ustawodawstwo dotyczące treści wymaga złożenia ośmiu różnych, powielających się sprawozdań. Sprawozdania te powinny zostać połączone lub przynajmniej charakteryzować się spójnym słownikiem pojęć, jednolitym harmonogramem oraz wspólnymi wskaźnikami oceny. Wyciąg z istniejących wymogów sprawozdawczych:

Sprawozdanie w zakresie przejrzystości	Miejsce publikacji	Częstotliwość
DSA (sprawozdanie VLOP-u/VLOSE)	Sprawozdanie w zakresie przejrzystości	Dwa razy do roku

DSA (sprawozdanie inne niż VLOP-u)	Sprawozdanie w zakresie przejrzystości	Co roku
Informacja o miesięcznej liczbie aktywnych odbiorców na podstawie DSA	Sprawozdanie w zakresie przejrzystości	Dwa razy do roku
Wzmocniony unijny Kodeks postępowania w zakresie zwalczania dezinformacji	Dostarczane bezpośrednio do regulatora; publikowane w centrum przejrzystości	Dwa razy do roku
Treści o charakterze terrorystycznym	Sprawozdanie w zakresie przejrzystości	Co roku

3. **Asymetryczne regulacje*:*** Europa musi nie tylko wspierać swoje małe i średnie przedsiębiorstwa (MŚP) i startupy, lecz także umożliwiać swoim przedsiębiorstwom skalowanie działalności i docieranie do globalnych odbiorców. Nierówne traktowanie ostatecznie zaszkodziłoby szerszemu ekosystemowi, czyniąc usługi większych firm droższymi dla europejskich przedsiębiorstw niezależnie od ich wielkości. Istnieje ryzyko, że zmiany regulacyjne nałożą nieproporcjonalne obciążenia na różne przedsiębiorstwa, nie biorąc pod uwagę powszechnych korzyści z korzystania z wiodących platform.

4. **Rosnące ryzyko protekcjonizmu:** aby Europa mogła przyspieszyć innowacje i rozwój technologiczny, konieczne będzie utrzymanie szerokiego dostępu do handlu międzynarodowego. Jeśli Europa podniesie lub stworzy nowe bariery handlowe lub regulacyjne wobec firm technologicznych albo przyjmując środki dyskryminacyjne w takich obszarach jak zamówienia publiczne, zaszkodzi to konkurencyjności UE poprzez ograniczenie dostępu europejskich przedsiębiorstw i użytkowników do najlepszych usług cyfrowych. Ten delikatny moment geopolityczny wymaga rozsądnego i długofalowego podejścia – takiego, które pozwoli ocenić, jak najlepiej zadbać o konkurencyjność i bezpieczeństwo Europy, a także upewnić się, że bieżące negocjacje i spory handlowe nie zaszkodzą długoterminowym interesom Unii.

OBSZARY REGULACYJNE WYMAGAJĄCE UPROSZCZENIA - NAJWAŻNIEJSZE WNIOSKI

1. Sztuczna inteligencja

- Jeśli Akt w sprawie sztucznej inteligencji ma wspierać zaufanie i innowacje, należy go dostosować tak, by był bardziej oparty na ocenie ryzyka, proporcjonalny, nowoczesny i łatwiejszy do wdrożenia.

- Kluczowe jest, aby wdrożenie Aktu nie rozszerzało prawa autorskiego poprzez niewykonalne obowiązki lub eksterytorialne skutki. Aby zachować integralność decyzji współustawodawców, kodeks praktyk dotyczący AI ogólnego przeznaczenia musi być wolny od „goldplatingu" polegającego na tworzeniu wymagań wykraczających poza pierwotny zakres Aktu.

- Jeśli ramy regulacyjne mają pozostać aktualne i skuteczne w miarę rozwoju AI, progi obliczeniowe dla modeli AI ogólnego przeznaczenia oraz „stwarzających ryzyko systemowe" powinny zostać podniesione, z wyraźną mapą drogową przejścia w przyszłości na oceny oparte na ich możliwościach. Zasada proporcjonalności musi również dotyczyć modyfikacji modeli: obowiązki związane z dostrajaniem powinny zależeć od wagi wprowadzanych zmian, a aktualizacja raportu o modelu powinna być konieczna tylko wtedy, gdy wcześniejszy raport staje się przez to nieaktualny.

- Przesłanką napędową dla powstania Aktu było zapewnienie harmonizacji regulacyjnej na całym jednolitym rynku cyfrowym. Zamiast tego ustawa tworzy skomplikowaną biurokrację egzekwowania prawa. Sama Irlandia wyznaczyła dziewięć różnych organów krajowych do ochrony praw podstawowych w zastosowaniach sztucznej inteligencji wysokiego ryzyka zgodnie z Aktem. Jeśli sytuacja ta powtórzy się we wszystkich 27 państwach członkowskich, powstanie ponad 240 takich organów. Oprócz bezprecedensowo złożonego systemu nadzoru i egzekwowania, który w praktyce obciąży zdolności administracyjne państw członkowskich (Akt przewiduje ponad 80 środków wykonawczych w różnych organach), nierozwiązane pozostają kwestie nakładania się Aktu na istniejący dorobek prawny, w szczególności RODO i dyrektywę UE ws. praw autorskich. Te kwestie również pogłębiają fragmentację unijnego rynku. Krajowe organy ochrony danych wykorzystują zarówno RODO, jak i Akt o sztucznej inteligencji do kształtowania otoczenia regulacyjnego w zakresie SI bez jasnej odpowiedzialności poprzez wytyczne i opinie, nie uwzględniając implikacji dla innowacyjności, wzrostu gospodarczego ani konkurencyjności, co jest całkowicie sprzeczne ze strategią UE w zakresie sztucznej inteligencji.

- Ponadto, struktura nadzoru i egzekwowania przepisów AIA może utrudniać wejście na rynek i fragmentować rynek cyfrowy ze względu na kwestie jurysdykcyjne i wielość organów regulacyjnych o nakładających się uprawnieniach. W przeciwieństwie do poprzednich strategii UE, ustawa o sztucznej inteligencji nie zawiera mechanizmów takich jak zasada „one-stop-shop” zasada kraju pochodzenia (“country of origin” - COO), co komplikuje zapewnienie zgodności z przepisami.

- Pierwotnym celem ustawy o sztucznej inteligencji nigdy nie było regulowanie samej technologii, ale skupienie się na konkretnych zastosowaniach wysokiego ryzyka. Przepisy dotyczące modeli AI ogólnego przeznaczenia (GPAI) wyraźnie odbiegają od tego celu. Zamiast tego regulują one technologię, która w dużej mierze jest już objęta istniejącymi przepisami dotyczącymi jej stosowania, poprzez RODO czy europejską dyrektywę ws. praw autorskich. Należy zauważyć, że modele GPAI są komórkami macierzystymi ekosystemu sztucznej inteligencji. Podobnie jak komórki macierzyste, modele GPAI mają charakter fundamentalny i są wszechstronne, umożliwiając wykonywanie szerokiego zakresu zadań w różnych dziedzinach bez konieczności

dostosowywania ich do konkretnych zastosowań. Dalsze narzucanie regulacji GPAI określonych w ustawie miałoby zatem wpływ na cały cykl innowacji w dziedzinie sztucznej inteligencji. Akt powinien powrócić do swojego pierwotnego celu, jakim jest regulowanie zastosowań sztucznej inteligencji wysokiego ryzyka, a sekcja, która w sposób zbędny reguluje technologię sztucznej inteligencji, rozdział V i towarzyszące mu motywy, powinny zostać usunięte. Co ważne, usunięcie odniesień do GPAI z Aktu nie oznacza „braku regulacji". Opracowywanie, wdrażanie i stosowanie modeli sztucznej inteligencji w UE jest już regulowane przez istniejący dorobek prawny.

2. Regulacje dotyczące treści

- Należy powstrzymać się od wprowadzania nowych przepisów dotyczących moderowania treści, zwodniczych interfejsów i systemów rekomendacji – np. w ramach Aktu o sprawiedliwości cyfrowej czy Tarczy demokracji – ponieważ już teraz wiele aktów prawnych (DSA, Dyrektywa dotycząca nieuczciwych praktyk handlowych , RODO, Akt o AI, Dyrektywa o audiowizualnych usługach medialnych, Rozporządzenie w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego) nakłada rozbudowane obowiązki w tych obszarach.

- Należy podjąć skoordynowane działania w celu rozwiązania nakładających się obowiązków w tych instrumentach, aby zwiększyć pewność prawa i ułatwić prowadzenie działalności w UE. W szczególności uprościć należy wymogi dotyczące raportowania przejrzystości i oceny ryzyka oraz usunąć przepisy dyrektywy audiowizualnej, które w zakresie moderacji treści i ochrony małoletnich zostały zastąpione przez DSA.

- Wprowadzić większą elastyczność w wyznaczaniu VLOP-ów oraz VLOSE na podstawie DSA:

    - umożliwiając negocjowane odstępstwa dla podmiotów o niskim profilu ryzyka.

    - liczba użytkowników nie powinna być jedynym kryterium wyznaczenia.

- Należy wzmocnić ochronę tajemnicy przedsiębiorstwa w zestawieniu z wymogami związanymi z ujawnianiem informacji z Dyrektywy ws. prawa autorskiego, Aktu w sprawie danych i Aktu w sprawie AI.

- Należy zapewnić dostawcom usług elastyczność w projektowaniu wewnętrznych systemów zgodności i nadzoru, biorąc pod uwagę złożone i nakładające się wymogi nadzorcze zawarte w wielu aktach prawnych.

3. Prywatność

- Dostosowanie europejskiego prawa ochrony prywatności do nowej epoki rozwoju Europy przy jednoczesnym uwzględnieniu europejskich wartości wymaga czegoś więcej niż usunięcia barier biurokratycznych dla niewielkiej części przedsiębiorstw. Uproszczenia są potrzebne także większym firmom, które mocno inwestują w Europie i napędzają całe ekosystemy start-upów i deweloperów. Równie ważne jest, by

Europa pokazała, że może być liderem AI dzięki nowemu podejściu do zasad prywatności, które powstały z myślą o starszych technologiach.

- Europa powinna skupić się na wspieraniu innowacji, nagradzaniu najlepszych praktyk w zakresie prywatności oraz zapobieganiu realnym szkodom dla obywateli. Można to osiągnąć dzięki prostszemu i faktycznie opartemu na ryzyku podejściu do RODO i przepisów o prywatności (ePrivacy), w szczególności:
    - Zasady powinny być stosowane proporcjonalnie, a nie sztywno – tak by zmniejszyć obowiązki przedsiębiorstw w zależności od poziomu ryzyka,
    - Należy uznać rolę uzasadnionego interesu jako podstawy prawnej, tak jak uczyniła to EROD w swojej opinii dotyczącej szkolenia modeli AI. UE musi pokazać, że zgoda osoby, której dane dotyczą nie jest jedynym rozwiązaniem, jeśli chodzi o skuteczną ochronę danych. Potrzebne jest zwiększenie pewności prawa (i zaufanie biznesu) w zakresie korzystania z uzasadnionego interesu jako podstawy prawnej, tworząc białą listę rodzajów przetwarzania, w których taka podstawa jest odpowiednia – pod warunkiem zastosowania odpowiednich zabezpieczeń. Powinno to obejmować przypadki stosowania uznanych, weryfikowalnych technologii podnoszących prywatność (PET).
    - Uproszczenie i zwiększenie odporności unijnego reżimu przekazywania danych. Docenić należy wagę decyzji stwierdzających odpowiedni stopień ochrony, niemniej jednak potrzebne jest uproszczenie poprzez wprowadzenie domniemania dla przekazywania danych wewnątrz grupy przedsiębiorstw, dokonywanego w zwykłym toku działalności, gdy grupa *samo*certyfikuje przestrzeganie odpowiednich zabezpieczeń. Ocena przepisów państwa trzeciego przy braku decyzji o adekwatności powinna uwzględniać rzeczywiste prawdopodobieństwo dostępu władz tego kraju do danych osób z UE.
    - Konieczne jest ograniczenie obciążeń administracyjnych, które znacząco zwiększają koszty prowadzenia działalności w UE dla firm każdej wielkości: mniej powielanej dokumentacji potrzebnej do zapewnienia zgodności z RODO; ograniczenie ciężaru realizacji wniosków o dostęp do danych przez wyłączenie przypadków nieproporcjonalnych itd.
    - Zasady RODO dotyczące danych szczególnej kategorii wymagają doprecyzowania, aby wspierać odpowiedzialną innowację w dziedzinie AI. Obecne szerokie interpretacje i ograniczone wyjątki powodują niepewność prawną w zakresie wykorzystania danych szczególnej kategorii do wspierania badań naukowych, zwalczania uprzedzeń lub poprawy reprezentatywności kulturowej i regionalnej modeli AI. Zalecamy wprowadzenia jaśniejszych zasad przetwarzania danych, które zostały wyraźnie upublicznione przez jednostki (przy odpowiednich zabezpieczeniach) oraz jednoznaczne uznanie za kwalifikowany wyjątek rozwoju modeli AI ogólnego przeznaczenia na potrzeby badań naukowych. Zmiany te zapewnią niezbędną pewność prawa dla innowatorów i wzmocnią ambicje Europy w dziedzinie AI.

4. Bezpieczeństwo

- Cyberbezpieczeństwo jest kluczową kwestią w obecnym kontekście geopolitycznym i technologicznym. Istnieje możliwość uproszczenia przepisów UE tak, aby lepiej chroniły obywateli, a jednocześnie były mniej uciążliwe dla przedsiębiorstw.

- Procesy certyfikacji warunkujące dostęp do rynku UE zawierają zbędne, nakładanie się wymogi i narzucają niepotrzebną presję czasową. Zalecamy uproszczenie przejścia z Dyrektywy RED na Akt o odporności cyfrowej (CRA) oraz zapewnienie przedsiębiorstwom co najmniej 12 miesięcy na dostosowanie się do nowych specyfikacji po ich ogłoszeniu. Prawo powinno również uznawać certyfikacje branżowe za spełniające wymagania.

- Obowiązujące przepisy tworzą liczne, nakładające się wymogi dotyczące zgłaszania incydentów (RODO, Rozporządzenie ws. operacyjnej odporności cyfrowej, Dyrektywa NIS2, Akt o odporności cyfrowej i Akt w sprawie AI). Oczekiwane jest uproszczenie tych wymagań poprzez wprowadzenie jednego portalu i procedury zgłaszania incydentów do tej samej jednostki. Potrzebna jest harmonizacja progów i terminów zgłaszania we wszystkich instrumentach, wzorując się na podejściu przyjętym w Dyrektywie NIS2. Cenne będzie jednoznaczne wskazanie, że jedno zgłoszenie spełnia obowiązki wynikające ze wszystkich właściwych przepisów.

- Wiele unijnych aktów prawnych (np. Dyrektywa NIS2, Akt o odporności cyfrowej, Rozporządzenie ws. operacyjnej odporności cyfrowej, Akt o cybersolidarności, Akt o cyberbezpieczeństwie, RODO) tworzy złożony obraz wymogów w zakresie zarządzania cyberbezpieczeństwem, koordynacji i współpracy. Aby zwiększyć przejrzystość i skuteczność dla przedsiębiorstw w UE, zalecane jest:

    - wykorzystywanie istniejących, uznanych na świecie międzynarodowych ram bezpieczeństwa zamiast tworzenia nowych, odrębnych i specyficznych dla UE wymagań;

    - aktywne zniechęcanie państw członkowskich do przyjmowania własnych krajowych systemów certyfikacji cyberbezpieczeństwa, które odbiegają od zharmonizowanego podejścia Unii lub norm międzynarodowych.

- Problemy dotyczące bezpieczeństwa podążają za postępem technologicznym. Aby lepiej ocenić, jak nowe propozycje regulacji technologicznych mogą wpłynąć na bezpieczeństwo, zalecane jest nadanie ENISA kompetencji do przeprowadzania ocen wpływu na bezpieczeństwo dla wszystkich nowych przepisów z zakresu nowych technologii, aby uniknąć niezamierzonych skutków dla bezpieczeństwa obywateli.

5. Akt o rynkach cyfrowych (DMA)

- DMA wprowadza rozwiązania przynoszące natychmiastowe i długoterminowe korzyści: zapobiega dublowaniu postępowań; skraca czas prowadzenia spraw poprzez usunięcie sporów o właściwość; umożliwia organom krajowym skupienie się na działaniach uzupełniających.

- Konieczna jest większa przejrzystość w zakresie rozgraniczenia między DMA a tradycyjnym prawem konkurencji. Nie powinny one być stosowane przez strony jako

zamienne ścieżki prawne. Praktyki objęte obowiązkami *ex ante* z DMA mogą nadal być sankcjonowane *ex post* na podstawie art. 102 TFUE, co otwiera drzwi do strategicznego wyboru jurysdykcji i równoległych postępowań egzekucyjnych oraz zwiększa ryzyko stosowania rozbieżnych standardów prawnych do identycznych praktyk biznesowych.

- Postępowania przygotowawcze prowadzone przez organy krajowe oraz procesy z powództwa prywatnego w państwach członkowskich pojawiają się równolegle z egzekwowaniem DMA. Trend ten bezpośrednio podważa cel harmonizacji określony w DMA.

- Podstawowe zasady sprawiedliwego postępowania, przewidywalności, proporcjonalności i przejrzystości procedur powinny być lepiej określone i konsekwentnie stosowane w ramach DMA.

- Co więcej, obowiązki wynikające z artykułu 5 DMA nie są „samowykonalne", jak zakładali prawodawcy. Komisja Europejska (KE) ma zatem bardzo szeroki zakres uznaniowości, aby decydować, jak powinno wyglądać przestrzeganie przepisów, bez możliwości uzyskania przez strażników dostępu dalszych wyjaśnień. Wynika to z bezprecedensowych uprawnień KE do interpretowania DMA w sposób, którego prawodawcy nie przewidzieli. Jednocześnie cele polityczne DMA nie są wystarczająco jasno określone.

- KE nie wypracowała spójnego podejścia do wdrażania DMA, które zapewniałoby pewność prawną, stale przesuwając granice zgodności. Egzekwowanie DMA do tej pory nie dało jasnych sygnałów dotyczących priorytetowych obszarów i prowadziło do wielokrotnych iteracji rozwiązań zgodności, generując dodatkowe koszty i komplikując długoterminowe planowanie. Dyskusje z regulatorami odbywają się ponadto w bardzo ograniczonym czasie, niezależnie od technicznej złożoności poruszanej kwestii – szczególnie w kontekście procesów specyfikacyjnych.

PROPOZYCJE UPROSZCZEŃ AKTU W SPRAWIE SZTUCZNEJ INTELIGENCJI

Podsumowanie

Akt w sprawie sztucznej inteligencji

- Przyjęcie proporcjonalnego i opartego na ryzyku podejścia do dostrajania, poprzez wytyczne Urzędu ds. AI oraz akty wykonawcze.
    - Uznanie, że obowiązujące regulacje już obejmują istotną część ryzyk, które są zarządzane przez pierwotnego dostawcę modelu lub, na poziomie systemu AI, przez podmiot, który dokonuje dostrajania. Doprecyzowanie, że pierwotny dostawca modelu AI ogólnego przeznaczenia nie ponosi odpowiedzialności za zgodność z przepisami w przypadku modyfikacji lub dostrajania modelu przez podmiot trzeci.
    - Modyfikacje powinny być klasyfikowane według ich technicznego charakteru, a nie podmiotu, który je wykonuje. W przypadku ustalania, które formy dostrajania podlegają wymogom, powinny obowiązywać te same progi – niezależnie od tego, czy dostrajania dokonuje ten sam podmiot, czy strona trzecia
    - Wprowadzenie możliwości zakwestionowania statusu modelu AI ogólnego przeznaczenia w oparciu o rzeczywiste możliwości dostrojonego modelu lub przypadki jego użycia.
    - Uproszczenie obowiązków związanych z aktualizacją Wzoru w celu podsumowania: wyłączenie obowiązku aktualizacji dla modyfikacji, które nie wprowadzają istotnych zmian w ogólnym charakterze lub możliwościach modelu; dopuszczenie aktualizacji w formie opisowej.
    - Wdrożenie stopniowanych obowiązków, przy czym pełne obowiązki powinny mieć zastosowanie wyłącznie w przypadku istotnego dostrajania.
- Ograniczenie zakresu terytorialnego obowiązków związanych z prawem autorskim, w szczególności wyłączeń w zakresie text i data miningu.
    - Ograniczenie zakresu terytorialnego art. 53 do działań podlegających prawu Unii, w tym unijnemu prawu autorskiemu. Przykładowo, wypuszczenie modelu na rynek unijny, trenowanie przeprowadzone w Unii.
    - Wyjaśnienie, że intencją art. 53 jest dostosowanie a nie rozszerzenie obowiązującego unijnego prawa autorskiego.
    - Wyjaśnienie, że art. 53 służy jedynie harmonizacji zastrzeżeń dotyczących szkolenia modeli AI ogólnego przeznaczenia; uniknięcie interpretacji, które mogłyby objąć całe indeksowanie stron internetowych i kolidować z funkcjami wyszukiwarek (np. robots.txt).

- Weryfikacja progów obliczeniowych dla modeli AI ogólnego przeznaczenia oraz ryzyk systemowych.
    - Podniesienie progów obliczeniowych do 10^{23} dla modeli AI ogólnego przeznaczenia oraz do 10^{26} dla modeli AI ogólnego przeznaczenia z ryzykiem systemowym.
    - Ustalenie progów modyfikacji w odniesieniu do mocy obliczeniowej modelu bazowego (np. jednej trzeciej obliczeń pierwotnego modelu AI ogólnego przeznaczenia), zamiast stosowania jednego, stałego progu dla wszystkich modeli.
    - Opracowanie mapy drogowej określającej, w jaki sposób progi te będą z czasem uzupełniane lub zastępowane oceną opartą na możliwościach, w celu zapewnienia odporności na zmiany w przyszłości.
- Uproszczenie samooceny AI wysokiego ryzyka
    - Wydanie wytycznych Komisji dotyczących wyłączeń dla AI wysokiego ryzyka przed lutym 2026 roku, zawierających jasne, obiektywne i praktyczne kryteria oceny ryzyka i potencjalnego wpływu.
    - Uznanie za wystarczającą samoocenę dokonaną w dobrej wierze przez dostawcę, z domniemaniem zasadności wyłączenia, o ile nie pojawią się przeciwne dowody.
    - Wskazanie w wytycznych, że obowiązki dotyczące dokumentacji powinny być proporcjonalne do kontekstu, a także umożliwienie stosowania uproszczonych formatów w przypadku, gdy brak jest widocznego i istotnego ryzyka.
- Rewizja podejścia do regulacji sztucznej inteligencji ogólnego przeznaczenia
    - Powrót do oryginalnego, technologicznie neutralnego podejścia w ramach Aktu.
    - Wykreślenie rozdziału V i motywów towarzyszących.
- Przyjęcie sprawnego mechanizmu rozstrzygania spraw transgranicznych
    - Wprowadzenie w rozdziale VII Aktu mechanizmu na wzór zasad takich, jak “one-stop-shop” czy “country of origin”.

Kodeks praktyk dla modeli AI ogólnego przeznaczenia

- Zawarcie w kodeksie praktyk dla modeli AI ogólnego przeznaczenia wymogów wyraźnie przewidzianych przez Akt w sprawie sztucznej inteligencji.
- Ujednolicenie kanałów ujawniania informacji, np. poprzez umożliwienie spełnienia obowiązków w zakresie przejrzystości z Aktu w sprawie sztucznej inteligencji za pomocą standardowej w branży publikacji kart modelu.
- Uproszczenie obowiązków przejrzystości dotyczących zasobów obliczeniowych, zużycia energii i wielkości modelu – poprzez złożenie jednej deklaracji klasyfikującej model jako mały / średni / duży.

- Usunięcie zbędnych wymogów dotyczących ocen adekwatności, z zaznaczeniem, że oceny dotyczące konkretnego modelu są wystarczające.

- Wyeliminowanie powielania aktualizacji między ramami odniesienia a kodeksem praktyk – aktualizacje powinny dotyczyć wyłącznie tego kodeksu.

- Zawężenie obowiązków aktualizacji raportów o modelach – ograniczenie ich do przypadków, w których aktualizacja jest konieczna, ponieważ wcześniejszy raport stał się nieaktualny, oraz dopuszczenie rozsądnych odstępów czasowych między aktualizacjami (np. nie rzadziej niż raz na 12 miesięcy).

- Stworzenie przyjaznego środowiska dla rozwoju modeli sztucznej inteligencji na otwartych licencjach, w oparciu o naukowy konsensus co do definicji “open source” i ochronę tajemnicy biznesowej.

Rekomendacje szczegółowe

UPROSZCZENIE #1 – PRZYJĘCIE PROPORCJONALNEGO I OPARTEGO NA RYZYKU PODEJŚCIA DO DOSTRAJANIA	
Proponowana zmiana	Uzasadnienie
Przyjąć proporcjonalne, oparte na ryzyku podejście do dostrajania (poprzez wytyczne Urzędu ds. AI lub akt wykonawczy): **1.** Uznanie obowiązujących przepisów: Należy przyjąć, że ryzyka są przede wszystkim zarządzane przez pierwotnego dostawcę albo, na poziomie systemu AI, przez podmiot, który dokonuje dostrajania. Dostawca pierwotnego modelu AI ogólnego przeznaczenia nie powinien być odpowiedzialny za przestrzeganie przepisów w odniesieniu do tego modelu zmodyfikowanego przez podmiot trzeci, poza obowiązkiem udostępnienia dokumentacji, która umożliwi temu podmiotowi działanie zgodnie z prawem. **2.** Modyfikacje powinny być klasyfikowane według ich technicznego charakteru, a nie podmiotu, który je wykonuje W przypadku modyfikacji dokonywanych na późniejszym etapie (forków), próg obliczeniowy powinien mieć zastosowanie wobec wszystkich podmiotów, zarówno wewnętrznych, jak i trzecich, zapewniając równe warunki działania i koncentrując się na istotności wprowadzanych zmian.	Korzyści z przyjęcia tej rekomendacji: Bezpośrednio wspiera konkurencyjność i innowacyjność UE poprzez uniknięcie nieproporcjonalnych obciążeń dla potencjalnie setek tysięcy podmiotów działających na dalszych etapach łańcucha dostaw. Zapewnia, że regulacje pozostają ukierunkowane, oparte na ryzyku i proporcjonalne, zgodnie z pierwotnym zamysłem Aktu w sprawie sztucznej inteligencji. Daje pewność prawną podmiotom dostrajającym modele. Uznaje istniejące ramy regulacyjne na poziomie modelu pierwotnego oraz systemu AI. Umożliwia przedsiębiorstwom (zwłaszcza MŚP) wykorzystanie dostrajania na potrzeby konkretnych zastosowań (często niskiego ryzyka) bez konieczności ponoszenia wysokich kosztów, jakie już obciążają dostawców modeli AI ogólnego przeznaczenia. Ryzyka braku działania: Znaczące rozszerzenie zakresu regulacji, które może zahamować wdrażanie i rozwój AI w gospodarce UE, ponieważ dostosowywanie modeli AI ogólnego przeznaczenia może być bardzo uciążliwe, co ograniczy ich użyteczność i przyjęcie

3. Doprecyzować możliwości obalenia domniemania: Dostawcy modeli powinni mieć możliwość zakwestionowania statusu modelu AI ogólnego przeznaczenia dla zmodyfikowanych modeli, wykazując że końcowa integracja modelu w systemie AI służy jedynie realizacji wąskiego zestawu zadań, lub że możliwości istotnie ulepszone w wyniku modyfikacji nie odpowiadają ogólnemu charakterowi pierwotnego modelu. **4.** Wzór w celu podsumowania nie powinien mieć zastosowania do nowych modeli powstałych w wyniku modyfikacji, a aktualizacje podsumowania dla wersji modeli AI ogólnego przeznaczenia powinny być przedstawiane w formie opisowej. Ponadto, modyfikacje o charakterze de minimis lub takie, które nie powodują „istotnej zmiany ogólnego charakteru i zdolności w porównaniu z modelem pierwotnym" nie powinny wymagać aktualizacji wzoru w celu podsumowania – również wtedy, gdy są dokonywane przez dostawcę pierwotnego modelu AI ogólnego przeznaczenia. **5.** Wprowadzić stopniowane obowiązki: *a) Ograniczone obowiązki:* Mają zastosowanie wyłącznie wtedy, gdy dostrojony model (bez istotnych zmian) jest udostępniany bezpośrednio podmiotom trzecim (np. aktualizacja dokumentacji technicznej, dostarczenie dokumentów uzupełniających). *b) Pełne obowiązki (rzadko):* Mają zastosowanie wyłącznie w przypadku „istotnego" dostrojenia (można ponownie wykorzystać elementy przygotowane przez pierwotnego dostawcę). *c) Brak dodatkowych obowiązków:* Ma zastosowanie, jeżeli dostrajanie służy wyłącznie do użytku wewnętrznego i nie jest istotne	przez przedsiębiorstwa. Nieproporcjonalnie negatywny wpływ na MŚP oraz konkurencyjność UE w porównaniu do podmiotów korzystających z gotowych modeli lub działających poza UE. Niepewność prawna utrudniająca inwestycje i rozwój. Regulacja traci swój ukierunkowany, oparty na ryzyku charakter.

UPROSZCZENIE #2 - OGRANICZENIE ZAKRESU TERYTORIALNEGO OBOWIĄZKÓW ZWIĄZANYCH Z PRAWEM AUTORSKIM, W SZCZEGÓLNOŚCI WYŁĄCZEŃ W ZAKRESIE TEXT I DATA MININGU	
Proponowana zmiana	Uzasadnienie

1. Ograniczenie zakresu terytorialnego art. 53: Doprecyzowanie, że obowiązki wynikające z art. 53 mają zastosowanie wyłącznie w przypadkach, gdy dane działanie podlega unijnemu prawu autorskiemu (np. wprowadzenie na rynek UE), z poszanowaniem zasady terytorialności. Środki przewidziane w kodeksach praktyk dotyczących modeli AI ogólnego przeznaczenia muszą wyraźnie zawierać sformułowanie „jeśli dotyczy". Należy unikać rozszerzania materialnych przepisów UE na szkolenie modeli poza jej terytorium. **2.** Dostosowanie polityki do obowiązującego prawa: Zapewnienie, aby wymogi polityki w zakresie prawa autorskiego (art. 53 ust. 1 lit. c)) były zgodne z obowiązującym prawem autorskim i nie wykraczały poza jego ramy. Należy unikać nakładania obowiązków w zakresie zgodności na dalszych lub wcześniejszych etapach łańcucha dostaw, które wykraczają poza kontrolę dostawcy. **3.** Doprecyzowanie kwestii text i data miningu oraz Robots.txt Skoncentrować się na konsensusie lub standaryzacji zasad dotyczących zastrzeżeń wobec wykorzystywania danych do szkolenia modeli AI ogólnego przeznaczenia, unikając interpretacji obejmujących wszelkie indeksowanie stron lub pozostających w sprzeczności z funkcjami wyszukiwarek.	Korzyści z przyjęcia tej rekomendacji: Zapewnia pewność prawną z poszanowaniem przepisów prawa autorskiego, ogranicza trudności związane z zapewnieniem zgodności w przypadku modeli AI rozwijanych globalnie, ułatwia dostęp do różnorodnych modeli, wspiera innowacyjność poprzez koncentrację na zachowaniu na rynku UE oraz zapobiega niezamierzonym skutkom dla ekosystemu internetu. Ryzyka braku działania: Utrzymujące się spory prawne; istotna niepewność prawna dla globalnych twórców AI ubiegających się o dostęp do rynku UE; trudności z egzekwowaniem przepisów po stronie UE; problemy techniczne w przypadku, gdy dostawcy byliby zobowiązani do retroaktywnego stosowania unijnych mechanizmów opt-out do działań szkoleniowych, które były zgodne z prawem w miejscu ich przeprowadzenia; znaczne obciążenia regulacyjne utrudniające wejście na rynek; ograniczona dostępność modeli w UE; zahamowanie innowacyjności z powodu obaw związanych z pozyskiwaniem danych i koniecznością ponownego szkolenia modeli; potencjalny negatywny wpływ na funkcjonowanie szerszego ekosystemu internetu.

UPROSZCZENIE #3 – WERYFIKACJA PROGÓW OBLICZENIOWYCH DLA MODELI AI OGÓLNEGO PRZEZNACZENIA ORAZ RYZYK SYSTEMOWYCH	
Proponowana zmiana	Uzasadnienie
1. Podniesienie progów obliczeniowych do 10^{23} dla modeli AI ogólnego przeznaczenia oraz do 10^{26} dla modeli AI ogólnego przeznaczenia z ryzykiem systemowym. **2.** Ustalenie progów modyfikacji w odniesieniu do rzeczywistej mocy obliczeniowej modelu bazowego (np. jednej trzeciej obliczeń pierwotnego modelu AI ogólnego przeznaczenia),	Korzyści z przyjęcia tej rekomendacji: Natychmiastowe ograniczenie obciążeń regulacyjnych dla modeli poniżej progu 10^{26} FLOP-ów, co pozwala skoncentrować zasoby i jest zgodne z unijnymi celami upraszczania regulacji Powiązanie progów modyfikacji z modelem bazowym zapewnia spójność i zapobiega zakłóceniom na rynku poprzez niezniechęcanie do korzystania z modeli o wysokiej wydajności. Uwzględnienie mapy drogowej dla ocen

zamiast stosowania stałego, niezależnego od modelu progu. **3.** Opracowanie mapy drogowej określającej, w jaki sposób progi te będą z czasem uzupełniane lub zastępowane oceną opartą na możliwościach, w celu zapewnienia odporności na zmiany w przyszłości.	opartych na możliwościach zapewnia, że ramy regulacyjne pozostaną adekwatne i skuteczne wraz z rozwojem technologii AI, co ogranicza konieczność częstych, reaktywnych zmian przepisów. Spójne z podejściem międzynarodowym. Politycznie wykonalne. Stanowi praktyczne rozwiązanie przejściowe, uwzględniające ograniczenia metryki obliczeniowej, zanim gotowe będą metody oparte na ocenie możliwości. Obejmuje kolejną generację modeli (przy założeniu kontynuacji skalowania etapu wstępnego szkolenia), bez nadmiernego skupiania się na obecnie znanych i przetestowanych modelach. Ogranicza obciążenia administracyjne dla Komisji Europejskiej. Ryzyka braku działania: Utrzymujące się niewłaściwe określanie zakresu regulacji w oparciu o przestarzałą metrykę. Nieuczciwe praktyki rynkowe wynikające z luki związanej z niskim progiem obliczeniowym. Potencjalne luki w zakresie bezpieczeństwa, jeśli modele o dużych możliwościach pozostaną poza zakresem regulacji.

UPROSZCZENIE #4 - UPROSZCZENIE SAMOOCENY AI WYSOKIEGO RYZYKA	
Proponowana zmiana	Uzasadnienie
1. Przyspieszenie wydania wytycznych Komisji: Komisję powinna opublikować wytyczne na długo przed terminem przypadającym na luty 2026 roku – zawierających jasne, obiektywne i praktyczne kryteria oceny „istotnego ryzyka” oraz „znaczącego wpływu na podejmowanie decyzji”. Wytyczne powinny zawierać konkretne przykłady systemów, które prawdopodobnie spełniają warunki wyłączenia (np. realizujących wąskie zadania proceduralne, usprawniających wcześniejsze działania człowieka, wykonujących zadania przygotowawcze bez zastępowania ludzkiej oceny).	Korzyści z przyjęcia tej rekomendacji: Zapewnia pewność prawną, umożliwiając dostawcom stosowanie wyłączenia w sposób uzasadniony i świadomy. Gwarantuje, że oparte na ryzyku podejście przyjęte w Akcie w sprawie sztucznej inteligencji działa zgodnie z jego zamierzeniem, zapobiegając nieproporcjonalnym obciążeniom dla systemów o niższym poziomie ryzyka. Wspiera innowacje, wskazując przejrzystą ścieżkę wdrażania użytecznych rozwiązań AI w obszarach wrażliwych, bez zbędnego obciążenia związanego z kwalifikacją jako system AI wysokiego ryzyka. Ogranicza obciążenia administracyjne związane z dokumentowaniem ocen na podstawie

2. Utrzymanie samooceny dostawcy: Ukształtować proces w taki sposób, aby udokumentowana samoocena, przeprowadzona przez dostawcę w sposób racjonalny i w dobrej wierze oraz na podstawie jasnych kryteriów określonych w wytycznych Komisji, stanowiła wystarczającą podstawę do zastosowania wyłączenia przewidzianego w art. 6 ust. 3. Potencjalna kontrola regulacyjna powinna koncentrować się na ocenie adekwatności udokumentowanej samooceny względem tych kryteriów, a nie na podważaniu wniosków dostawcy bez przedstawienia przeciwnych dowodów. **3.** Proporcjonalność dokumentacji: Zachęcić Komisję, aby w swoich wytycznych wyraźnie dopuściła możliwość dostosowania wymaganej dokumentacji do kontekstu systemu, w tym sugerując uproszczone formaty w przypadkach, gdy brak istotnego ryzyka jest oczywisty na podstawie jasno określonych kryteriów.	nieprecyzyjnych kryteriów. Zwiększa przewidywalność w zakresie projektowania i wdrażania produktów. Ryzyka braku działania: Nadmierna kwalifikacja systemów jako systemów AI wysokiego ryzyka. Hamowanie innowacji w obszarach wymienionych w załączniku III z powodu obaw związanych z zapewnieniem zgodności z wymogami. Znaczne zasoby marnowane są na radzenie sobie z niejasnościami oraz tworzenie dokumentacji, która może okazać się nadmiarowa. Osłabienie zakładanej elastyczności i proporcjonalności ram oceny ryzyka przewidzianych w Akcie w sprawie sztucznej inteligencji.

UPROSZCZENIE #5 - REWIZJA PODEJŚCIA DO REGULACJI SZTUCZNEJ INTELIGENCJI OGÓLNEGO PRZEZNACZENIA (GPAI)	
Proponowana zmiana	Uzasadnienie
4. Powrót do oryginalnego, technologicznie neutralnego i nakierowanego na ograniczanie ryzyka kierunku Aktu. **5.** Usunięcie rozdziału V i towarzyszących mu motywów Aktu.	Korzyści z przyjęcia tej rekomendacji: Obecne ramy prawne dotyczące modeli GPAI stanowią poważne wyzwanie nie tylko dla dostawców, ale także dla organizacji, które korzystają z tych modeli, dostosowują je lub wdrażają. Nakładając ograniczenia, UE ryzykuje zahamowanie innowacyjności i wydajności operacyjnej, uniemożliwiając organizacjom wykorzystanie technologii sztucznej inteligencji na takim samym poziomie, jak ich globalni konkurenci. Ta złożoność regulacyjna ma wpływ nie tylko na poszczególne podmioty, ale także na całą gospodarkę UE, tworząc bariery dla postępu technologicznego i konkurencyjności rynkowej.

UPROSZCZENIE #5 - PRZYJĘCIE SPRAWNEGO MECHANIZMU ROZSTRZYGANIA SPRAW TRANSGRANICZNYCH	
Proponowana zmiana	Uzasadnienie
6. Należy ponownie przeanalizować rozdział VII Aktu o sztucznej inteligencji w celu uwzględnienia usprawnionego mechanizmu rozstrzygania spraw transgranicznych.	Korzyści z przyjęcia tej rekomendacji: Elastyczność Aktu o sztucznej inteligencji w zakresie wyznaczania krajowych organów regulacyjnych doprowadziła do powstania propozycji utworzenia wielu organów o zróżnicowanej wiedzy specjalistycznej w państwach członkowskich, co znacznie komplikuje sytuację przedsiębiorstw prowadzących działalność transgraniczną. Bez mechanizmu dotyczącego spraw transgranicznych wiele organów regulacyjnych w różnych krajach mogłoby potencjalnie mieć jurysdykcję w tej samej sprawie. Mogłoby to prowadzić do niestabilnej sytuacji w sprawach transgranicznych, utrudniając przedsiębiorstwom prowadzenie działalności w UE i powodując, że organy regulacyjne ds. sztucznej inteligencji nie byłyby zobowiązane do zachowania równowagi między prawami podstawowymi a innymi celami regulacyjnymi, takimi jak konkurencja, innowacje, prywatność i bezpieczeństwo.

PROPOZYCJE UPROSZCZEŃ W ZAKRESIE TREŚCI

Podsumowanie

Rekomendujemy:

- Powstrzymanie się od wprowadzania nowych przepisów dotyczących moderowania treści, interfejsów i systemów rekomendacji – np. w ramach Aktu o sprawiedliwości cyfrowej czy Tarczy demokracji – ponieważ już teraz wiele aktów prawnych (takie, jak Akt o usługach cyfrowych, Dyrektywa dotycząca nieuczciwych praktyk handlowych, RODO, Akt w sprawie sztucznej inteligencji, Dyrektywa o audiowizualnych usługach medialnych, Rozporządzenie platform-to-business) nakłada rozbudowane obowiązki w tych obszarach.

- Sprawozdawczość w zakresie przejrzystości. Należy podjąć skoordynowane działania w celu wyeliminowania powielających się obowiązków sprawozdawczych dotyczących regulacji treści w różnych unijnych aktach prawnych, aby zwiększyć pewność prawa i ułatwić prowadzenie działalności gospodarczej w UE. Główną osią sprawozdawczości powinny być raporty przejrzystości zgodnie z Aktem o usługach cyfrowych, natomiast nakładające się lub nadmiernie uciążliwe obowiązki powinny zostać zniesione lub uproszczone.

    - Należy wycofać wymogi dotyczące sprawozdawczości w zakresie przejrzystości zawarte w Rozporządzeniu w sprawie treści o charakterze terrorystycznym w internecie.

        - Działania podejmowane wobec treści terrorystycznych będą uwzględniane w raportach przejrzystości na mocy Aktu o usługach cyfrowych, publikowanych od lutego 2026 roku.

    - Należy uchylić wszelkie obowiązki sprawozdawcze przyjęte przez państwa członkowskie na podstawie Dyrektywy o audiowizualnych usługach medialnych.

    - Należy wycofać wymogi dotyczące sprawozdawczości w zakresie przejrzystości zawarte w Rozporządzeniu platform-to-business.

        - Raporty dotyczące przejrzystości na mocy Aktu o usługach cyfrowych zawierają informacje o odwołaniach dotyczących czynności moderacyjnych zarówno wobec użytkowników końcowych, jak i biznesowych.

    - Należy zmienić częstotliwość raportowania w ramach Kodeksu postępowania w sprawie dezinformacji z półrocznej na roczną oraz usunąć obowiązek raportowania szczegółowych statystyk i załączników ad hoc dotyczących konkretnych zdarzeń.

        - Raport z realizacji Kodeksu postępowania w sprawie dezinformacji jest wyjątkowo obciążający i wymaga zarówno opisowych, jak i liczbowych odpowiedzi w odniesieniu do 44 zobowiązań. Opisy te zwykle zmieniają się nieznacznie między kolejnymi edycjami raportu, przez co

raportowanie co pół roku jest zbędne i nieproporcjonalne, a jego wartość dla odbiorców zewnętrznych jest znikoma.

- Jest to działanie powielające się; czynności podjęte w związku z dezinformacją i informacjami wprowadzającymi w błąd będą uwzględnione w raportach przejrzystości na mocy Aktu o usługach cyfrowych od lutego 2026 roku.

- Należy wydłużyć termin na sporządzenie raportów przejrzystości co najmniej do 2 miesięcy po zakończeniu okresu sprawozdawczego.
  - Raporty sporządzane na podstawie tymczasowego Rozporządzenia w sprawie CSAM, Rozporządzenia w sprawie treści o charakterze terrorystycznym w internecie oraz Kodeksu postępowania w sprawie dezinformacji muszą obecnie zostać złożone w terminie 1 miesiąca od zakończenia okresu sprawozdawczego.
  - W każdym cyklu termin złożenia raportu z realizacji Kodeksu postępowania w sprawie dezinformacji jest wydłużany o około 2,5 miesiąca, jednak informacja o tym dociera do sygnatariuszy dopiero tuż przed pierwotnym terminem. Powoduje to zakłócenia i wprowadza niepotrzebną niepewność przy każdej publikacji.

- Podjęcie skoordynowanych działań w celu usunięcia duplikujących się obowiązków w tych instrumentach, aby zwiększyć pewność prawa i ułatwić prowadzenie działalności w UE:
  - Należy usunąć obowiązki dotyczące moderowania treści i ochrony małoletnich wynikające z Dyrektywa o audiowizualnych usługach medialnych. Dyrektywa ta wymaga implementacji w państwach członkowskich, co prowadzi do fragmentacji przepisów w UE i utrudnia harmonizację przewidzianą w Akcie o usługach cyfrowych dla platform internetowych.
  - Należy usunąć wymogi dotyczące systemów rekomendacyjnych zawarte w Rozporządzeniu platform-to-business, ponieważ dublują one przepisy Aktu o usługach cyfrowych.
  - Należy uchylić art. 25 Aktu o usługach cyfrowych dotyczący zwodniczych interfejsów, ponieważ wprowadza on niepewność prawną wynikającą z nakładania się regulacji z RODO i Dyrektywą o nieuczciwych praktykach handlowych.
  - Należy wydać niewiążące wytyczne wspierające przedsiębiorstwa w spełnianiu pokrywających się obowiązków w zakresie oceny ryzyka na gruncie RODO, Aktu w sprawie sztucznej inteligencji, Aktu o usługach cyfrowych i Rozporządzenia w sprawie treści o charakterze terrorystycznym w internecie.

- Wprowadzenie większej elastyczności przy wyznaczaniu VLOP-ów i bardzo dużych wyszukiwarek internetowych w ramach Aktu o usługach cyfrowych:
  - Dopuszczenie możliwości wyłączenia z kwalifikacji usług o niskim profilu ryzyka w drodze uzgodnień z Komisją.
  - Liczba użytkowników nie powinna być jedynym kryterium wyznaczenia.

- Wzmocnienie ochrony tajemnicy przedsiębiorstwa w zestawieniu z wymogami związanymi z ujawnianiem informacji z Dyrektywy ws. prawa autorskiego, Aktu w sprawie danych i Aktu w sprawie AI. Należy wydać instrumenty uzupełniające doprecyzowujące zakres tej ochrony.

- W interpretacji i egzekwowaniu obowiązków regulacyjnych należy zapewnić dostawcom usług elastyczność w projektowaniu wewnętrznych systemów zgodności i nadzoru – w ramach Aktu o usługach cyfrowych, Aktu o rynkach cyfrowych, Akt w sprawie sztucznej inteligencji, RODO oraz Dyrektywy NIS2.

Rekomendacje szczegółowe

Proponowana zmiana	Uzasadnienie
UPROSZCZENIE #1 - SYSTEMY REKOMENDACYJNE	
1. Należy powstrzymać się od dalszego regulowania tego obszaru. Z niepokojem odbieramy pogłoski, jakoby w Akcie o sprawiedliwości cyfrowej miały się pojawić kolejne obowiązki regulacyjne dotyczące systemów rekomendacyjnych stosowanych przez platformy internetowe. 2. Należy wycofać wymóg dotyczący systemów rekomendacyjnych zawarty w Rozporządzeniu platform-to-business.	1. Instytucje UE powinny dążyć do uproszczenia ram regulacyjnych mających zastosowanie do systemów rekomendacyjnych wykorzystywanych przez platformy internetowe, zamiast dalej je rozbudowywać. 2. Wymóg dotyczący systemów rekomendacyjnych zawarty w Rozporządzeniu platform-to-business nie jest już potrzebny. Rozporządzenie to reguluje systemy rekomendacyjne w odniesieniu do użytkowników biznesowych. Artykuł 27 Aktu o usługach cyfrowych reguluje obecnie systemy rekomendacyjne zarówno względem użytkowników końcowych, jak i biznesowych, w ramach bardziej scentralizowanego modelu egzekwowania przepisów.
UPROSZCZENIE #2 - ZWODNICZE INTERFEJSY	
1. Należy powstrzymać się od dalszego regulowania tego obszaru. Z niepokojem odbieramy pogłoski, jakoby w Akcie o sprawiedliwości cyfrowej miały się pojawić kolejne przepisy, które jeszcze bardziej rozdrobnią już i tak niejednolite ramy regulacyjne dotyczące interfejsów. 2. Należy rozważyć uchylenie artykułu 25 Aktu o usługach cyfrowych.	1. Instytucje UE powinny dążyć do uproszczenia ram regulacyjnych mających zastosowanie do zwodniczych interfejsów online, zamiast dalej je rozbudowywać. 2. Zgodnie z art. 25 ust. 2 Aktu o usługach cyfrowych, regulacje dotyczące interfejsów zwodniczych zawarte w tym akcie nie mają zastosowania do praktyk objętych Dyrektywą o nieuczciwych praktykach handlowych oraz RODO. Nie jest jasne, jaki dodatkowy cel ma realizować artykuł 25 Aktu o usługach cyfrowych.

UPROSZCZENIE #3 - SPRAWOZDAWCZOŚĆ W ZAKRESIE PRZEJRZYSTOŚCI	
1. Należy zadbać o to, aby nie dochodziło do powielania obowiązków dotyczących wskaźników w różnych sprawozdaniach z przejrzystości (również w kontekście przyszłych regulacji). Terminy na sporządzenie takich sprawozdań powinny zostać wydłużone co najmniej do 2 miesięcy po zakończeniu okresu sprawozdawczego. 2. Należy zmienić wymóg dotyczący częstotliwości sprawozdań z Kodeksu praktyk w zakresie dezinformacji, tak aby były one składane raz w roku, a nie co pół roku. 3. Należy wycofać wymogi dotyczące sprawozdawczości w zakresie przejrzystości zawarte w Rozporządzeniu platform-to-business.	1. Uprościłoby to proces raportowania i zapobiegło dublowaniu wysiłków. Ułatwiłoby to również przegląd przez podmioty trzecie. 2. Sporządzanie sprawozdania z Kodeksu praktyk w zakresie dezinformacji jest bardzo obciążające ze względu na konieczność uwzględnienia szczegółowych danych oraz obszernych opisów. W przypadku wielu zobowiązań brak jest jakichkolwiek zmian w ciągu ostatnich 6 miesięcy, co sprawia, że obowiązek składania raportu co pół roku jest nieproporcjonalny. 3. Obowiązek sprawozdawczości z przejrzystości zawarty w Rozporządzeniu platform-to-business nie jest już potrzebny, ponieważ Akt o usługach cyfrowych obejmuje sprawozdawczość w zakresie skarg dotyczących moderacji treści zarówno użytkowników końcowych, jak i biznesowych.
UPROSZCZENIE #4 - OCHRONA NIELETNICH W SIECI	
1. Należy uchylić artykuł 28b Dyrektywy o audiowizualnych usługach medialnych, aby zapobiec mnożeniu się rozdrobnionych i sprzecznych przepisów krajowych implementujących ten przepis. Należy skupić się na wdrażaniu artykułu 28 Aktu o usługach cyfrowych.	1. Akt o usługach cyfrowych w pełni harmonizuje zasady ochrony małoletnich w internecie, zastępując krajowe implementacje wcześniej obowiązujących przepisów Dyrektywy o audiowizualnych usługach medialnych.
UPROSZCZENIE #5 - WYMOGI DOTYCZĄCE MODERACJI TREŚCI	
1. Należy uchylić artykuł 28b Dyrektywy o audiowizualnych usługach medialnych, aby zapobiec nakładaniu się regulacji z Aktem o usługach cyfrowych oraz mnożeniu się rozdrobnionych i sprzecznych przepisów krajowych implementujących ten przepis. Należy skupić się na egzekwowaniu pokrywających się obowiązków wynikających z Aktu o usługach cyfrowych.	1. Akt o usługach cyfrowych w pełni ujednolica zasady dotyczące moderowania treści, które mają zastosowanie do usług pośrednich (w tym platform do udostępniania wideo). Oznacza to, że podobne przepisy zawarte w Dyrektywie o audiowizualnych usługach medialnych stają się nieaktualne, a państwa członkowskie nie muszą ich już wdrażać.
UPROSZCZENIE #6 - OCENY RYZYKA	
1. Należy powstrzymać się od dalszego regulowania tego obszaru. Z niepokojem obserwujemy propozycje wprowadzenia odrębnego obowiązku oceny ryzyka dla	1. Oceny ryzyka przygotowywane przez bardzo duże platformy internetowe i bardzo duże wyszukiwarki w ramach Aktu o usługach cyfrowych już uwzględniają ryzyka

usług pośrednich, które są już objęte regulacjami Aktu o usługach cyfrowych, w odniesieniu do obecności materiałów przedstawiających seksualne wykorzystywanie dzieci (CSAM) w tych usługach. 2. Należy wydać niewiążące wytyczne dotyczące nakładania się przepisów prawa unijnego w zakresie ocen ryzyka.	związane z CSAM. Nie ma potrzeby wprowadzania odrębnej, dodatkowej oceny ryzyka. 2. Takie wytyczne pomogą firmom zrozumieć: a) jak tworzyć oceny ryzyka w sposób spełniający jednocześnie wymagania różnych regulacji, oraz b) kiedy są zwolnione z obowiązku sporządzania dodatkowych ocen ryzyka.
UPROSZCZENIE #7 - WYZNACZANIE VLOP-ów i BARDZO DUŻYCH WYSZUKIWAREK INTERNETOWYCH W AKCIE O USŁUGACH CYFROWYCH	
1. Należy nadal stosować kryterium liczby aktywnych odbiorców miesięcznie przy ocenie, czy dana usługa kwalifikuje się jako VLOP lub VLOSE, ale jednocześnie należy umożliwić Komisji Europejskiej prowadzenie dialogu z danym dostawcą w celu ewentualnego wyłączenia usługi z tej kwalifikacji, jeśli jej profil ryzyka na to pozwala.	1. Obecny proces wyznaczania statusu VLOP-ów lub VLOSE nie uwzględnia profilu ryzyka danej usługi, przez co wielu dostawców podlega najbardziej obciążającym wymogom Aktu o usługach cyfrowych wyłącznie z tego powodu, że ich usługi cieszą się popularnością wśród użytkowników.
UPROSZCZENIE #8 - ŁAD WEWNĘTRZNY	
1. Dostawcom usług cyfrowych należy pozostawić szeroką swobodę w zakresie wewnętrznego zarządzania nadzorem nad zgodnością z przepisami. 2. Wymogi dotyczące „niezależności”, „uprawnień” i „struktury” wewnętrznych mechanizmów zapewniania zgodności powinny zostać ujednolicone.	1. Każdy podmiot jest inny i powinien mieć możliwość wdrażania takich przepływów informacji i procesów, które najlepiej odpowiadają jego strukturze i sposobowi działania. 2. Różnice w wymaganiach dotyczących wewnętrznych struktur ds. zgodności powodują zbędne skomplikowanie w organizacji.
UPROSZCZENIE #9 - OCHRONA TAJEMNIC PRZEDSIĘBIORSTWA	
1. Należy zapewnić spójną i solidną ochronę tajemnicy przedsiębiorstwa poprzez odpowiednią interpretację przepisów unijnych – w szczególności Aktu w sprawie danych, Dyrektywy w sprawie prawa autorskiego oraz Aktu w sprawie sztucznej inteligencji. 2. Należy wydać instrumenty uzupełniające (np. w ramach kodeksu praktyk lub wzoru dokumentacji w Akcie w sprawie sztucznej inteligencji), które doprecyzują, w jaki sposób zapewniona zostanie ochrona tajemnic przedsiębiorstwa.	1. Aby utrzymać bodźce do innowacyjności, organy regulacyjne muszą jasno sygnalizować i wskazywać w wytycznych, że obowiązki w zakresie udostępniania danych i przejrzystości nie mogą być wykorzystywane jako furtka do uzyskania dostępu do tajemnic przedsiębiorstwa innych firm. 2. Tajemnice przedsiębiorstwa są chronione przez szereg aktów prawnych – międzynarodowych (art. 39 Porozumienia TRIPS), regionalnych i krajowych (Dyrektywa o ochronie tajemnic handlowych

Zgodnie m.in. z motywem 14 Dyrektywy w spawie ochronie tajemnic handlowych, instrumenty te powinny odzwierciedlać powszechnie przyjętą i stosowaną przez sądy wykładnię przesłanki „wartości handlowej" – jako odnoszącej się do faktycznej lub potencjalnej wartości informacji wynikającej z jej poufności i przewagi konkurencyjnej, jaką zapewnia jej posiadaczowi.	została implementowana we wszystkich państwach członkowskich).

REFORMA AKTU O RYNKACH CYFROWYCH (DMA)

Komisja Europejska zapowiedziała, że deregulacja, szybsze cykle zatwierdzania i ograniczenie obowiązków sprawozdawczych będą jej głównym priorytetem w kadencji 2024–2029. Równolegle, Enrico Letta w swoim głośnym raporcie wzywa UE do odejścia od obecnego, rozproszonego ustawodawstwa dotyczącego cyfryzacji i stworzenia spójnych ram, które będą działać skutecznie w całej Europie. Chociaż Akt o rynkach cyfrowych (DMA) opiera się na art. 114 TFUE, będącym podstawą działania rynku wewnętrznego, to jego praktyczne wdrożenie nie odzwierciedla jeszcze w pełni tego celu.

DMA wyznacza Komisję Europejską jako jedyny organ odpowiedzialny za egzekwowanie tych przepisów, co przynosi korzyści zarówno w krótkim, jak i w długim terminie. Centralizacja tych kompetencji ma na celu zapobieganie dublowaniu postępowań, skraca czas prowadzenia spraw poprzez usunięcie sporów kompetencyjnych i pozwala organom krajowym skupić się na działaniach uzupełniających. Taka struktura jest kluczowa dla zapewnienia pewności prawa i jego spójności, które pozwalają przedsiębiorstwom na inwestowanie i innowacje w całym jednolitym rynku. Niemniej, na przeszkodzie osiągnięcia tego celu stoją następujące problemy:

- Regulatorzy DMA są osadzeni w strukturach Komisji Europejskiej: Komisja odpowiada za tworzenie polityk i odgrywa rolę polityczną; połączenie jej tradycyjnej roli z egzekwowaniem DMA zwiększa ryzyko upolitycznienia procesu egzekwowania, co z kolei prowadzi do niepewności wśród wszystkich uczestników rynku.

- Nakładanie się reżimów *ex ante* i *ex post*: Praktyki objęte obowiązkami *ex ante* z DMA mogą nadal być sankcjonowane *ex post* na podstawie art. 102 TFUE. Obecnie art. 1 ust. 5 i 1 ust. 6 DMA pozwalają państwom członkowskim stosować prawo konkurencji do praktyk, które już zostały uregulowane przez DMA. To otwiera drzwi do strategicznego wyboru jurysdykcji i równoległych postępowań egzekucyjnych oraz zwiększa ryzyko stosowania rozbieżnych standardów prawnych do identycznych praktyk biznesowych. Aby zapewnić spójność i pewność prawa, konieczna jest większa przejrzystość w zakresie rozgraniczenia między DMA a tradycyjnym prawem konkurencji. Nie powinny one być stosowane przez strony jako zamienne ścieżki prawne.

- Równoległe krajowe postępowania na gruncie DMA: Postępowaia przygotowawcze prowadzone przez organy krajowe oraz procesy z powództwa prywatnego w państwach członkowskich pojawiają się równolegle z egzekwowaniem DMA. Tego rodzaju rozproszone praktyki niepotrzebnie powielają pracę tak publicznych, jak i prywatnych interesariuszy, oraz zwiększają prawdopodobieństwo niejednolitej lub sprzecznej wykładni prawa. Trend ten bezpośrednio podważa cel harmonizacji określony w motywie 6 DMA i tworzy ryzyko ponownego rozdrobnienia regulacyjnego, które to Akt miał wyeliminować.

- Obecne wdrażanie DMA przez Komisję Europejską pomija szersze skutki regulacji dla innowacji, prywatności i bezpieczeństwa. Szeroka interpretacja obowiązków wynikających z DMA (np. w zakresie interoperacyjności) rodzi pytania dotyczące roli zabezpieczeń integralności, bezpieczeństwa i prywatności, a także kompetencji oraz

wiedzy regulatora w kwestiach bezpieczeństwa platform i użytkowników. Aktualne podejście KE do egzekwowania DMA już stworzyło wyzwania zarówno dla konsumentów, jak i dla firm korzystających z platform cyfrowych (w tym MŚP).

- DMA również zahamował lub opóźnił wprowadzanie na rynek nowych innowacyjnych produktów w UE. Odnotowano kilka przykładów produktów i usług, które zostały opóźnione lub w ogóle nie zostały wprowadzone na rynek w UE z powodu niepewności związanej z DMA, w tym jego powiązania z innymi regulacjami lub rygorystycznych przepisów podważających prawa własności intelektualnej (IP). Bariery regulacyjne zmniejszają użyteczność dla konsumentów i prowadzą do obniżenia jakości doświadczeń online użytkowników usług cyfrowych w UE. Opóźnienia odzwierciedlają trudności w opracowaniu produktów zgodnych z DMA, które jednocześnie właściwie chroniłyby prywatność, bezpieczeństwo i ochronę użytkowników.

Pewność prawa jest kluczowa dla przedsiębiorstw planujących długofalowe inwestycje i działających w unijnej cyfrowej gospodarce. Podstawowe zasady rzetelnego postępowania, przewidywalności, proporcjonalności i przejrzystości procedur powinny być lepiej określone i konsekwentnie stosowane w ramach DMA.

- Przewidywalność wymaga, by przedsiębiorstwa wiedziały z wyprzedzeniem, jakie są priorytety organów i czego oczekuje się od nich w zakresie zgodności z przepisami. Jej zapewnienie staje się trudne, gdy na późnym etapie postępowań pojawiają się nowe teorie szkody. Standardy proceduralne dotyczące dochodzeń prowadzonych na podstawie DMA powinny być dostosowane do standardów stosowanych w sprawach antymonopolowych. Obejmuje to ustanowienie jasnych protokołów operacyjnych, zapewnienie pełnego dostępu do akt spraw oraz stosowanie bardziej rygorystycznej analizy kosztów i korzyści przy rozpatrywaniu opinii stron trzecich.
    - Podmioty sprawujące kontrolę nad dostępem do rynku także potrzebują jasnych i spójnych wytycznych dotyczących interpretacji kluczowych przepisów DMA przez Komisję, a Komisja powinna aktywnie rozwiązywać wszelkie konflikty między DMA a innymi przepisami UE.
    - Niezbędne jest, aby podmioty sprawujące kontrolę nad dostępem do rynku otrzymały jednoznaczne wytyczne dotyczące interpretacji przez Komisję obowiązków wynikających z DMA, zwłaszcza w odniesieniu do kluczowych terminów (np. znaczenia pojęć „połączenie” i „wykorzystanie krzyżowe” w art. 5 ust. 2).
    - Stosowanie i interpretacja tych obowiązków powinny uwzględniać dodatkowe czynniki, które wspierają cele DMA w zakresie konkurencyjności i sprawiedliwości, takie jak wspieranie innowacji i dostarczanie produktów wysokiej jakości.
    - Aby zapewnić skuteczne i spójne wdrożenie, wszelkie potencjalne konflikty z obowiązującym prawodawstwem UE powinny zostać zidentyfikowane i rozwiązane przed wydaniem przez Komisję decyzji o niezgodności. Proaktywne rozwiązywanie niespójności prawnych ma kluczowe znaczenie dla pewności

prawa, przewidywalności działalności gospodarczej i integralności ram regulacyjnych UE.

- Proporcjonalność zakłada, że działania regulatora opierają się na dowodach, są precyzyjnie dostosowane do konkretnego przypadku i wyważone względem spodziewanych skutków oraz potencjalnych ryzyk.
    - Istotne jest również, aby interpretacja obowiązków wynikających z DMA przez Komisję pozostawała skoncentrowana na zakresie DMA, unikając wpływu szerszych celów politycznych. Dopuszczenie takich rozważań grozi podważaniem wiarygodności DMA i narażeniem jej na krytykę na arenie międzynarodowej.

- Sprawiedliwy proces to nie tylko dostęp do dowodów i odpowiedni czas na kontakt z regulatorem, ale też dokładniejsza selekcja skarg. Bez takiej selekcji istnieje ryzyko, że nawet słabe lub czysto spekulacyjne mogą skutkować oficjalnym wystąpieniem o udzielenie informacji, co zwiększa koszty przestrzegania przepisów dla przedsiębiorstw i biurokrację. Kluczowe dla utrzymania skuteczności i zaufania dla mechanizmu egzekwowania jest to, by priorytetyzować skargi, w których podniesiono wiarygodne i poważne zastrzeżenia.
    - Komisja musi prowadzić dochodzenia w sposób skuteczny, ale nie powinno to odbywać się kosztem praw proceduralnych, takich jak zapewnienie podmiotom sprawującym kontrolę dostęp do materiałów dotyczących sprawy. Obecnie dochodzenia prowadzone na podstawie DMA nie zapewniają wystarczających gwarancji proceduralnych, co utrudnia skuteczną współpracę i powoduje niepewność operacyjną. Te niedociągnięcia podkreślają potrzebę bardziej ustrukturyzowanego i przejrzystego procesu regulacyjnego w odniesieniu do DMA. Bez jasno określonych procedur i przejrzystej odpowiedzialności istnieje ryzyko, że DMA nie osiągnie swojego celu, jakim jest wspieranie uczciwych i konkurencyjnych rynków cyfrowych.

- Komisja Europejska czasami nadmiernie opierała się na wkładzie niektórych przedsiębiorstw, z których część jest bezpośrednimi konkurentami strażników dostępu i przedstawia sprzeczne interpretacje DMA przy ocenie zgodności.

- Co więcej, podejście KE do decyzji specyfikacyjnych polegało na narzucaniu szczegółowych rozwiązań zgodności zamiast prowadzenia autentycznego dialogu regulacyjnego ze strażnikami dostępu w oparciu o wspólne zrozumienie unikalnych cech ich platform.

- Nie jest jasne, kiedy KE decyduje się na wszczęcie postępowań specyfikacyjnych, a kiedy na nałożenie obowiązków wynikających z niezgodności. Dotychczasowe postępowania specyfikacyjne KE były w praktyce wykorzystywane do obchodzenia tekstu DMA i rozszerzania obowiązków, zamiast podążania za literą prawa. Ponadto proces specyfikacyjny nie zawiera gwarancji proceduralnych umożliwiających rzeczywisty dialog regulacyjny, co w praktyce zmusza strażników dostępu do dostosowania się do interpretacji KE dotyczącej tego, jak DMA powinien być rozumiany, aż do czasu rozstrzygnięcia takich spraw w toku odwołania.

- Ponadto terminy zgodności przewidziane w DMA, w szczególności dla decyzji specyfikacyjnych, nie doszacowują zakresu prac inżynieryjnych (oraz harmonogramów przeglądów/kontroli jakości) wymaganych do ich realizacji. Prowadzi to do pośpiesznych rozwiązań technicznych, w przypadku których KE nie uwzględniła właściwie kompromisów ani procedury zgodności, pozostawiając bardzo niewiele miejsca na rzeczywisty dialog regulacyjny ukierunkowany na znalezienie najlepszych dostępnych rozwiązań technicznych. Powoduje to również, że bardzo istotne zasoby są odciągane od działań innowacyjnych.

- Strażnicy dostępu, użytkownicy biznesowi i inne zainteresowane strony nie mają wystarczających mechanizmów, aby angażować się w prace prowadzone przez Wysoką Grupę Roboczą ds. DMA (HLG). W praktyce prace i wpływ HLG są całkowicie niejawne, a nie istnieje żaden sposób, aby ustalić jej działania lub wpływ na egzekwowanie DMA.

Ramy działania Brytyjskiego Urzędu Konkurencji i Rynków (CMA), oparte na czterech zasadach: tempie, przewidywalności, proporcjonalności i rzetelnej procedurze, stanowią wartościowy punkt odniesienia. Przewidują one m.in. wczesny dialog, jasne zasady ustalania priorytetów i zabezpieczenia proceduralne – wszystko po to, by wzmocnić jakość i zaufanie do egzekwowania. Omawiane usprawnienia nie spowalniają postępowań – wręcz przeciwnie, przyczyniają się do lepszego zapewnienia zgodności z prawem i budują zaufanie do całego systemu regulacyjnego.

Wspólny rynek działa najlepiej, gdy wszyscy jego uczestnicy, od globalnych platform po małe startupy, mogą działać na podstawie jednolitych i spójnych zasad. Pełna harmonizacja, na mocy DMA, ogranicza niepewność prawną i zmniejsza koszty jego przestrzegania – nie tylko dla wyznaczonych „strażników dostępu", ale także dla tysięcy europejskich przedsiębiorstw, których wzrost i konkurencyjność zależy od dostępu do platform. Upraszczając mechanizmy egzekwowania i wzmacniając zabezpieczenia proceduralne, Komisja może zrealizować swój priorytet upraszczania prawa, jednocześnie zwiększając wiarygodność i skuteczność DMA w długim okresie.

Komisja Europejska powinna jednak skoncentrować się na stosowaniu przepisów DMA (np. w zakresie interoperacyjności) w obszarach, w których istnieje wyraźne ryzyko ograniczenia konkurencyjności oraz gdzie istnieje sprawdzony rynek dla mniejszych konkurentów. KE mogłaby wzorować się na brytyjskim CMA, które ogłosiło, że będzie skupiać się na obszarach o wyraźnym zapotrzebowaniu i nie będzie wymagać interoperacyjności z założenia, ponieważ jest to niepraktyczne.

- KE powinna zasięgać szczegółowych opinii ekspertów technicznych w odniesieniu do niektórych aspektów wdrażania DMA na wszystkich etapach egzekwowania. Można to realizować poprzez:

    - Konsultacje z innymi dyrekcjami generalnymi Komisji posiadającymi odpowiednie kompetencje (np. DG JUST w zakresie prywatności, jednostki DG CNECT w zakresie bezpieczeństwa i innowacji) oraz z krajowymi organami ochrony danych.

    - Konsultacje z Wysoką Grupą Roboczą ds. DMA (HLG), w której skład wchodzą eksperci ds. prywatności (EDPB/EDPS), w sposób bardziej systematyczny w całym procesie zapewniania zgodności z DMA. Dodatkowo ENISA, posiadająca wiedzę ekspercką w dziedzinie cyberbezpieczeństwa, powinna zostać zaproszona do udziału w pracach HLG.

- KE powinna opracować wytyczne dotyczące swoich priorytetów w zakresie zgodności, określając, w jaki sposób będzie nadawać priorytety wdrażaniu i egzekwowaniu DMA, aby zapewnić strażnikom dostępu i beneficjentom większą pewność prawną. Powinno to obejmować większą przejrzystość w zakresie celów politycznych regulatorów.

- KE mogłaby zwiększyć przejrzystość i rzetelność proceduralną w zakresie włączania stron trzecich poprzez wydanie wytycznych konsultacyjnych dotyczących kryteriów, procedur i wykorzystania wkładu stron trzecich. Powinna również rozważyć, jak ustanowić bardziej ustrukturyzowane i inkluzywne podejście do pozyskiwania opinii stron trzecich, które zapewniałyby zróżnicowane perspektywy.

- KE powinna odejść od rozumienia „skutecznej zgodności" jako zmiany w wynikach rynkowych, a zamiast tego definiować ją przez pryzmat tego, czy proponowane plany zgodności skutecznie spełniają progi prawne. Jak wskazuje przygotowywane opracowanie kancelarii King & Spalding (sponsorowane przez CCIA), istnieje wiele usprawnień proceduralnych, które Komisja może wprowadzić, aby ułatwić strażnikom dostępu skuteczne przestrzeganie DMA. Należą do nich m.in. prawa do przesłuchania ustnego, domniemanie zgodności lub bardziej szczegółowe wytyczne dotyczące procesu.

- DMA powinno być docelowo egzekwowane przez w pełni niezależny organ, co zminimalizowałoby ryzyko ingerencji politycznej i pomogłoby stworzyć większą pewność prawną.

- KE powinna udzielać bardziej precyzyjnych wskazówek dotyczących szczegółowych celów do osiągnięcia dla każdej podstawowej usługi platformowej i związanych z nią obowiązków, a także więcej informacji zwrotnych na temat tego, czy potencjalne środki proponowane przez strażników dostępu zostaną uznane za zgodne. Informacja zwrotna mogłaby wskazywać rezultaty, które strażnik dostępu ma osiągnąć, aby mógł on samodzielnie zidentyfikować najbardziej odpowiednie rozwiązania techniczne do realizacji tego celu.

- KE powinna opublikować wytyczne określające okoliczności, w których wszczyna postępowania specyfikacyjne, a kiedy postępowania w sprawie naruszeń.

- Rola Wysokiej Grupy Roboczej ds. DMA (HLG) jest kluczowa i wymaga poprawy w zakresie przejrzystości oraz zaangażowania interesariuszy. Ulepszenia mogłyby obejmować publikowanie rocznego planu prac oraz informacji o obszarach działań prowadzonych przez podgrupy.

- Strażnicy dostępu, użytkownicy biznesowi i inne zainteresowane strony powinni mieć możliwość udziału w konsultacjach i/lub składania uwag do prac prowadzonych przez HLG.

PROPOZYCJE UPROSZCZEŃ W ZAKRESIE PRYWATNOŚCI

Podsumowanie

- Należy doprowadzić to tego, aby RODO było faktycznie oparte na analizie ryzyka – poprzez wyraźne uznanie zasady proporcjonalności, uwzględniającej rzeczywiste ryzyko i koszty związane z zapewnieniem zgodności z przepisami.

- Potrzeba więcej elastyczności, gdy chodzi o podstawę przetwarzania związaną z uzasadnionym interesem, dodając domniemanie posiadania takiego interesu w przypadku wpisania danego rodzaju przetwarzania na białą listę, a także większy margines oceny dla administratorów.

- Należy uprościć międzynarodowe przekazywanie danych poprzez:

    - uproszczoną procedurę dla przekazywania w ramach zwykłej działalności między podmiotami z tej samej grupy przedsiębiorstw;

    - zwiększenie elastyczności oceny przepisów państw trzecich w braku decyzji dotyczącej adekwatności, w tym poprzez wzięcie pod uwagę rzeczywistego prawdopodobieństwa dostępu władz publicznych do danych osobowych z UE.

- Potrzeba zawęzić zakres szczególnych kategorii danych, przyjmując wyjątek dla danych dostępny publicznie – w przypadku, gdy wprowadzono odpowiednie zabezpieczenia.

- Należy wprowadzić kluczowe poprawki w Dyrektywie o e-prywatności, w szczególności wyłączenie plików cookie dotyczących reklamy kontekstowej, pomiarów odbiorców czy bezpieczeństwa, z wymogu zgody, jak również banerów cookie.

- Istnieje konieczność ograniczenia dublującej się dokumentacji wymaganej na potrzeby zgodności z RODO, zmniejszenia obciążenia związanego z odpowiadaniem na wnioski o dostęp do danych i inne uprawnienia osób, których dane dotyczą, doprecyzowania warunków współadministrowania na gruncie RODO oraz zawężenia zakresu zastosowania Aktu w sprawie danych w celu ograniczenia kosztów zapewnienia zgodności i wyeliminowania nakładających się i sprzecznych przepisów.

RODO

- Należy doprowadzić to tego, aby RODO było faktycznie oparte na analizie ryzyka – aby zrealizować jego założenia i nadać przepisom większą elastyczność.

    - Wyraźnie uznać, w nowym artykule, zasadę proporcjonalności – w szczególności w oparciu o 1) ryzyko związane z przetwarzaniem danych oraz 2) obciążenia związane z zapewnieniem zgodności.

    - Wprowadzić analizę proporcjonalności do przepisów dotyczących przekazywania danych – tak aby zapewnić większą elastyczność dla przepływów danych o niskim poziomie ryzyka.

    - Ograniczyć obowiązki związane z wnioskami o dostęp do danych ze strony osób, których dane dotyczą.

- Zmniejszyć papierologię związaną z zapewnieniem zgodności.
    - Szczególnie w przypadku oceny ryzyka na potrzeby uzasadnionego interesu: wprowadzić domniemanie, że taki interes ma miejsce w przypadku typów przetwarzania wymienionych na „białej liście", dając administratorowi większy margines oceny.
    - Mniej powielającej się dokumentacji.

- Ograniczyć obciążenia związane z realizacją wniosków dotyczących praw osób, których dane dotyczą
    - Zmniejszyć obciążenia związane z wnioskami osób, których dane dotyczą, poprzez wyłączenia związane z „nadmiernymi wysiłkami".
    - Mniej indywidualnego dostosowywana przekazywanych informacji – gdy jest to możliwe.

- Zawęzić zakres szczególnych kategorii danych
    - Dane, które wyraźnie i bezpośrednio dotyczą wrażliwych kategorii (lub z których dane wrażliwe mogą potencjalne być wywnioskowane)
    - Wyjątek dla danych dostępnych publicznie, przy zastosowaniu odpowiednich zabezpieczeń.

- Poprawić reżim przekazywania danych
    - Uprościć przekazywanie danych między podmiotami należącymi do tej samej grupy kapitałowej, dokonywane w ramach zwykłej działalności, poprzez uznanie domniemania stosowania odpowiednich zabezpieczeń w przypadku samo-certyfikacji ich przestrzegania przez daną spółkę.
    - Wprowadzić większą elastyczność oceny przepisów państw trzecich w braku decyzji dotyczącej adekwatności, w tym poprzez wzięcie pod uwagę rzeczywistego prawdopodobieństwa dostępu władz publicznych do danych osobowych z UE.

- Doprecyzować warunki współadministrowania
- Uzupełnić mandat organów ochrony danych w RODO o wyraźne uznanie interesów gospodarczych i innowacyjnych oraz zapewnić jasność co do wymaganej równowagi między ochroną danych a innymi prawami i interesami
- Wzmocnić balans między prawem do prywatności a innymi prawami podstawowymi i powiązanymi interesami

Dyrektywa o e-prywatności

- Wyłączyć cookie dla bezpieczeństwa z wymogów uzyskania zgody

- Wyłączyć cookie dotyczące pomiarów odbiorców z wymogów uzyskania zgody
- Wyłączyć cookie dotyczące spersonalizowanej reklamy kontekstowej z wymogów uzyskania zgody
- Doprecyzować, że w przypadku stosowania wyłączeń nie jest wymagane wyświetlanie banerów cookie.
- Doprecyzować, że wymogi zgody nie mają na celu obejmowania krótkotrwałego przechowywania lub informacji przesyłanych w ramach zwykłego połączenia internetowego.
- Częściowo zrewidować przepisy dot. marketingu bezpośredniego.
- Częściowo zrewidować i zharmonizować przepisy dot. danych o ruchu.
- Uwzględnić wyjątek od zgody na rozwiązania zwiększające/zachowujące prywatność.

Akt w sprawie danych

- Ograniczyć katalog urządzeń objętych Aktem w sprawie danych, tak aby wyłączyć kluczowe urządzenia konsumenckie: komputery osobiste, tablety, smartfony i smartwatche.
- Zawęzić zakres objętych danych w celu uniknięcia dublowania z RODO oraz sprzeczności z Aktem o rynkach cyfrowych.
- Ograniczyć wymóg udostępniania danych na linii przedsiębiorstwa - sektor publiczny (który stosuje się obecnie do nieokreślonych „danych") wyłącznie do danych z produktu i danych związanych z usługą.

Rekomendacje szczegółowe

RODO

UPROSZCZENIE #1 - Wyraźnie uznać zasadę proporcjonalności w RODO	
Proponowana zmiana	Uzasadnienie
Zmiana w art. 24 ust. 1, uznająca proporcjonalność środków stosowanych do wykazania przestrzegania RODO: *1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie i proporcjonalne środki*	• Zmiany 1 i 2 zmierzają do wyraźnego uznania zasady proporcjonalności w art. 24 RODO. Uzasadnieniem dla tych zmian jest to, że uznanie tej zasady zapewni administratorom większą elastyczność w interpretacji obowiązków wynikających z RODO w sposób proporcjonalny do ryzyka i kosztów – co w rezultacie zmniejszy obecne obciążenia związane z zapewnieniem

techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Dodać nowy art. 24 ust. 4 RODO, uznający bardziej ogólnie zasadę proporcjonalności: *4. Obowiązki nałożone niniejszym rozporządzeniem na administratorów należy interpretować zgodnie z zasadą proporcjonalności, uwzględniając stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także rozsądną ocenę przez administratora ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.*	zgodności z tymi przepisami. • Ponadto, przyczyniłoby się to do zwiększenia pewności prawa dla podmiotów zobowiązanych do przestrzegania obowiązków wynikających z RODO. Mogłyby one liczyć na pewną swobodę ze strony organów nadzorczych, które interpretowałyby te obowiązki w sposób proporcjonalny, m.in. do ryzyka związanego z przetwarzaniem. • Te zmiany podkreślałyby też to, że to właśnie administratorzy mogą być najlepiej predysponowani do oceny rzeczywistego ryzyka dla osób, których dane dotyczą, oraz do określenia, które środki zapewniające zgodność są proporcjonalne.

UPROSZCZENIE #2 - Uprościć oraz zapewnić administratorom większą elastyczność w zakresie przestrzegania zasady rozliczalności wynikającej z RODO – szczególnie, gdy podstawą zgodności przetwarzania z prawem jest art. 6 ust. 1 lit. f) RODO.	
Proponowana zmiana	Uzasadnienie
Zmienić art. 6 ust. 1 lit. f) RODO, wprowadzając „białą listę” czynności przetwarzania, które domniemywa się jako zgodne z prawem. *(f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Komisja, w drodze procedury sprawdzającej, o której mowa w art. 93 ust. 2, przyjmuje akt wykonawczy zawierający wykaz rodzajów operacji przetwarzania, które domniemywa się jako zgodne z prawem na podstawie art. 6 lit. f) niniejszego rozporządzenia.*	• Zmiana ma na celu wprowadzenie w art. 6 RODO „białej listy” prawnie uzasadnionych interesów, w przypadku których przyjmuje się, że wynik „testu równowagi” przemawia na korzyść administratora. Lista ta mogłaby obejmować określone rodzaje czynności przetwarzania o niższym poziomie ryzyka, takie jak ochrona przed oszustwami lub nadużyciami, ulepszanie produktów, ich debugowanie lub utrzymanie (czyli *de facto* przeciwieństwo wykazów rodzajów operacji przetwarzania wysokiego ryzyka, o których mowa w art. 35, i które przyjmują organy nadzorcze). Poprawka zmierza także do przyznania administratorom „marginesu uznania” przy stosowaniu testu oceny prawnie uzasadnionych interesów dla tych czynności przetwarzania. Jej uzasadnieniem jest wprowadzenie pewnego stopnia pewności prawa, gdy chodzi o stosowanie kryterium prawnie uzasadnionego interesu jako podstawy

Zmienić art. 5 ust. 2 w celu ograniczenia powtarzających się środków. *Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”). Może on opierać się na jednym zestawie środków w celu wykazania zgodności w odniesieniu do zbioru operacji przetwarzania o podobnym charakterze, zakresie, kontekście i celu.*	zgodności przetwarzania z prawem (które to jest zasadniczo podstawą, na której opierają się podmioty m.in. w celach ulepszania produktów czy prowadzenia badań), a także zapewnienie administratorom większej elastyczności przy dokonywaniu wspomnianej oceny, o ile spełnione są określone podstawowe kryteria. Obecnie podmioty nie mogą być jednoznacznie pewne co do tego, czy wskazana przez nie podstawa zgodności przetwarzania z prawem zostaną uznana za prawidłową – nawet gdy przeprowadzają one oceny skutków zgodnie ze wskazówkami organów nadzorczych. Prowadzi to do niepewności prawnej i utrudnia innowacje. Propozycja może też otworzyć możliwość skodyfikowania niektórych wytycznych dotyczących nowych technologii, np. poprzez przyznanie mocy prawnej Opinii EROD w sprawie modeli sztucznej inteligencji, zgodnie z którą trenowanie modeli AI na publicznie dostępnych danych jest co do zasady zgodne z prawem. ● Druga rekomendowana zmiana zmierza do wprowadzenia poprawki w art. 5 ust. 2 i uznania wprost, że administratorzy mogą opierać się na tych samych środkach, związanych z rozliczalnością, oraz tej samej dokumentacji dla podobnych zbiorów operacji przetwarzania. Jej celem jest również zwiększenie elastyczności i umożliwienie administratorom oparcie się na jednej ocenie skutków w przypadku podobnych zbiorów czynności przetwarzania. Pozwoliłoby to zmniejszyć obciążenia, jakie obecnie ciążą na podmiotach, np. w zakresie przetwarzania danych osobowych na potrzeby działalności badawczo-rozwojowej.

UPROSZCZENIE #3 - Wnioski osób, których dane dotyczą: wprowadzenie wyjątku od obowiązku stosowania art. 15–22 RODO w przypadku „niewspółmiernie dużego wysiłku” po stronie administratora

Proponowana zmiana	Uzasadnienie
Zmienić art. 12 ust. 5 wprowadzając kryterium „niewspółmiernie dużego wysiłku” jako wyjątek od obowiązku udzielania odpowiedzi na wnioski osób, których dane dotyczą *5. Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 są wolne od opłat.* *Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter albo, biorąc pod uwagę zakres przetwarzania i koszt wdrażania, gdy udzielenie odpowiedzi wymagałoby niewspółmiernie dużego wysiłku, administrator może:* *(a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo* *(b) odmówić podjęcia działań w związku z żądaniem.* *Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, albo że udzielenie odpowiedzi wymagałoby niewspółmiernie dużego wysiłku, spoczywa na administratorze.* Zezwolić administratorom na przekazywanie ustandaryzowanych informacji w celu wypełnienia obowiązku udzielania informacji na podstawie art. 15 RODO *(1) Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji*	• Pierwsza z proponowanych zmian zmierza do wprowadzenia, w art. 12 ust. 5, kryterium „niewspółmiernie dużego wysiłku” jako wyjątku od obowiązku udzielania odpowiedzi na wnioski osób, których dane dotyczą. Celem tej zmiany jest dopuszczenie ograniczonego wyjątku, umożliwiającego administratorom wykazanie, że udzielenie odpowiedzi na żądania wymagałyby niewspółmiernie dużego wysiłku. Podobne wyjątki obowiązują w innych przepisach RODO (art. 14). Wprowadzenie tej zmiany dałoby podmiotom możliwość odmowy udzielenia odpowiedzi na żądania, jeżeli koszt i nakład operacyjny z tym związany byłyby całkowicie nieproporcjonalne. • Druga z proponowanych zmian zakłada umożliwienie administratorom, którzy świadczą usługi użytkownikom na jednolitych zasadach, udzielania odpowiedzi na żądania dostępu do informacji, na podstawie art. 15, z wykorzystaniem ustandaryzowanych powiadomień lub informacji (np. poprzez odesłanie osoby, której dane dotyczą, do publicznie dostępnej polityki prywatności). Dzięki temu administratorzy nie musieliby przekazywać informacji odnoszących się indywidualnie do osoby, której dane dotyczą, kiedy to informacje te są wspólne dla wielu osób. Obecny tekjst RODO jest niejednoznaczny co do tego, czy jest to dopuszczalne. Interpretacja wymagająca przekazywania informacji dostosowanych indywidualnie byłaby całkowicie niewykonalna i niepotrzebnie obciążająca dla wielu administratorów (ponieważ wymagałoby to szeroko zakrojonego przeszukiwania systemów oraz identyfikacji i weryfikacji informacji dla każdego

można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. W przypadkach, gdy administrator świadczy usługi lub dostarcza produkty na jednolitych zasadach, w szczególności w związku ze świadczeniem usług internetowych, może on podać informacje, o których mowa w art. 13 i 14, oraz wszelką komunikację podejmowaną na mocy art. 15–22 i 34, w ustandaryzowanej formie, w tym poprzez ich publiczne udostępnienie. Propozycja nowego motywu *(..) Niniejsze rozporządzenie uznaje, że wielu administratorów świadczy usługi w sposób ustandaryzowany, w szczególności w przypadku usług internetowych, gdzie podstawowe funkcje i cechy tych usług są jednakowe dla wszystkich użytkowników, oferowane na podstawie wspólnych warunków świadczenia usług i obejmujące zasadniczo te same kategorie danych osobowych, cele przetwarzania oraz operacje przetwarzania. W takim przypadku – zwłaszcza gdy użytkownikom zapewniono wymagane informacje w zakresie przejrzystości i dobrowolnie korzystają z usług poprzez utworzenie konta internetowe – wymóg realizacji prawa do informacji i dostępu do danych osobowych w sposób zindywidualizowany byłby nieproporcjonalny, jeżeli ten sam skutek można osiągnąć w równym stopniu poprzez udostępnienie wszystkim użytkownikom ustandaryzowanych informacji lub narzędzi.*	żądania), w tym dla małych i średnich przedsiębiorstw. Poprawka ta zmierzałaby do zważenia, z jednej strony, konieczności zapewnienia użytecznych informacji osobom, których dane dotyczą, a z drugiej ograniczenia obciążeń nakładanych na administratorów.

UPROSZCZENIE #4 - Zawęzić zakres danych osobowych uznawanych za szczególne kategorie danych zgodnie z art. 9 RODO i/lub wprowadzić bardziej elastyczne wyjątki w art. 9 ust. 2 RODO	
Proponowana zmiana	Uzasadnienie
Zawęzić definicję szczególnych kategorii danych osobowych w art. 9 ust. 1 *(1) Zabrania się:* *(a) przetwarzania danych osobowych, które dotyczą wyraźnie i bezpośrednio następujących kategorii: ~~ujawniających~~ pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub*	• Pierwsza zmiana zmierza do doprecyzowania pojęcia szczególnych kategorii danych w art. 9 RODO poprzez ograniczenie jego zakresu do takich danych, które mają charakter „wyraźny” (koncepcja ta ma swoje źródło w wytycznych wydanych przez EROD) oraz „nie-wyraźny”, jeśli administrator zamierza stosować wnioskowania dedukcyjne na podstawie tych szczególnych kategorii. Pojęcie szczególnych kategorii danych, tak jak

światopoglądowe albo przynależność do związków zawodowych; ~~*oraz*~~ *(b) przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej;* *(c)* przetwarzania *danych dotyczących zdrowia, oraz danych, które dotyczą wyraźnie i bezpośrednio seksualności lub orientacji seksualnej tej osoby.* *(d) przetwarzania danych osobowych dla celów profilowania lub wnioskowania dedukcyjnego o osobie, której dane dotyczą, na podstawie kategorii informacji wymienionych w lit. a) i c).* *Artykuł 4* *15) „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – wyraźnie i bezpośrednio ujawniające informacje o stanie jej zdrowia;* Rozszerzyć wyjątki dotyczące szczególnych kategorii danych osobowych w art. 9 ust. 2 *2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:* *[..]* *e) przetwarzanie dotyczy danych osobowych, które są publicznie dostępne, a administrator wdraża odpowiednie środki ochrony praw i wolności osoby, której dane dotyczą, oraz jej uzasadnionych interesów, zapewniając w szczególności poszanowanie zasady minimalizacji danych;* ~~*w sposób oczywisty upublicznionych przez*~~	jest ono aktualnie interpretowane, jest zbyt szerokie – do tego stopnia, że potencjalnie jakiekolwiek dane osobowe mogą należeć do szczególnych kategorii, jeżeli umożliwiają one na wyciągnięcie wniosków o charakterze wrażliwym. Tego rodzaju niepewność prawna blokuje innowację, ponieważ podmioty nie są pewne co do tego, czy mają podstawę do przetwarzania danych tego rodzaju. • Druga zmiana zakłada rozszerzenie wyjątków z art. 9 ust. 2, aby umożliwić podmiotom większą elastyczność w przetwarzaniu danych szczególnie chronionych, o ile zostaną przyjęte odpowiednie zabezpieczenia. Rozszerzenie wyjątków przewidzianych w art. 9 ust. 2 pomogłoby wielu podmiotom, w tym MŚP chcącym wprowadzać innowacje w obszarze sztucznej inteligencji poprzez trenowanie LLM-ów i innych modeli w sposób zgodny z unijnym Aktem w sprawie sztucznej inteligencji. • Trzecia z proponowanych zmian ma na celu wprowadzenie pragmatycznego podejścia, jeśli chodzi o odpowiedzialności administratora za przestrzeganie art. 9, wypracowanego przez TSUE w sprawie *GC. i in. (Usunięcie linków do danych wrażliwych)* Uznanie tych zasad w RODO, w sposób bardziej ogólny, umożliwiłoby podmiotom większą elastyczność we wprowadzaniu innowacji w obszarze sztucznej inteligencji, poprzez przyjęcie, że odpowiedzialność administratora za zgodność z artykułem 9 powinna uwzględniać specyfikę danego przetwarzania.

~~osobę, której dane dotyczą;~~ *[...]* *j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. Rozwój modeli AI ogólnego przeznaczenia, zgodnie z art. 89 ust. 1 i rozdziałem V rozporządzenia (UE) 2024/1689, stanowi cel badań naukowych na użytek niniejszego rozporządzenia;* *k) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.* Skodyfikować wyrok TSUE w sprawie C-136/17 (Usunięcie linków do danych wrażliwych) w nowym art. 9 ust. 5 *5. Każda ocena zgodności działania administratora z tym artykułem powinna być przeprowadzana w ramach spoczywającej na nim odpowiedzialności. Zakres odpowiedzialności administratora za zapewnienie zgodności powinien uwzględniać specyfikę danej operacji przetwarzania.*	

UPROSZCZENIE #5 - Uprościć system przekazywania danych osobowych w ramach RODO	
Rekomendowana zmiana	Uzasadnienie
Dodać nowy ust. 6 w art. 46, ustanawiający mechanizm certyfikacji przekazywania danych osobowych wewnątrz grupy przedsiębiorstw	• Proponowana zmiana zmierza do określenia w RODO mechanizmu certyfikacji dla przekazywania danych osobowych wewnątrz grupy przedsiębiorców. Przystąpienie do tego

6. Komisja, w drodze procedury sprawdzającej, o które mowa w art. 93 ust. 2, przyjmie akt wykonawczy określający zasady oraz kategorie zabezpieczeń, które administrator może stosować przy przekazywaniu danych osobowych do państw trzecich w ramach transferów transgranicznych pomiędzy podmiotami należącymi do tej samej grupy przedsiębiorstw, w przypadku braku decyzji na podstawie art. 45 ust. 3. Zasady te mają ułatwiać globalny transfer danych osobowych przetwarzanych w ramach zwykłej działalności biznesowej między podmiotami w grupie oraz uwzględniać zróżnicowaną strukturę korporacyjną i prawną globalnych przedsiębiorstw, a także ochronę osób, których dane dotyczą, wynikającą z przestrzegania, również dobrowolnego, niniejszego rozporządzenia przez grupę poza EOG, jak również z wdrożenia odpowiednich środków technicznych i organizacyjnych w całej grupie. *7. Domniemywa się, że administrator, który dokonał samocertyfikacji zgodności swojej grupy z zasadami, o których mowa w art. 46 ust. 6, zapewnił odpowiednie zabezpieczenia w rozumieniu ust. 1 – w odniesieniu do przekazywania danych osobowych pomiędzy podmiotami należącymi do tej samej grupy – bez obowiązku przeprowadzania indywidualnej oceny poziomu ochrony danych w odnośnych państwach trzecich.* Zmienić art. 46 w celu wprowadzenia większej elastyczności przy dokonywaniu ocen ustawodawstwa państw trzecich na potrzeby standardowych klauzul umownych *1. W razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki*	systemu samocertyfikacji wyeliminowałoby konieczność przeprowadzania ocen skutków przekazywania oraz stosowania standardowych klauzul umownych przy przekazywaniu danych poza EOG, co znacząco zmniejszyłoby obciążenia związane z przestrzeganiem przepisów po stronie podmiotów. Potrzebne byłyby dalsze informacje dotyczące szczegółów takiego mechanizmu. • Druga z proponowanych zmian zakłada zmniejszenie obciążeń tych podmiotów, które stosują standardowe klauzule przy przekazywaniu danych poza EOG – poprzez uznanie, że podmioty te mogą opierać się na tej samej ocenie w przypadku zestawu podobnych przekazywań, jeśli stosowany jest ten sam zestaw zabezpieczeń. Intencją tej zmiany jest umożliwienie podmiotom przeprowadzenie tzw. „globalnej oceny skutków przekazywania", tam gdzie jest to właściwe, w celu ograniczenia znacznych obciążeń, jakie wiążą się z koniecznością przeprowadzania wielu, często powielających się, ocen dla każdego realizowanego przekazywania danych. • Trzecia zawiera prostą zmianę obowiązującej decyzji dotyczącej standardowych klauzul umownych, odnoszącą się do obecnej luki lub niepewności prawnej, z jaką ma do czynienia wiele podmiotów, które przekazują dane poza EOG do podmiotów, które podlegają RODO. Pozwoli to uniknąć konieczności przyjmowania nowej decyzji przez Komisję.

ochrony prawnej. W tym celu, administrator lub podmiot przetwarzający przekazujący dane osobowe do państwa trzeciego przeprowadzi ocenę poziomu ochrony przyznanej w kontekście takiego przekazania, biorąc pod uwagę: *a) właściwe zabezpieczenia wykorzystywane przez administratora lub podmiot przetwarzający dla celów przekazywania, oraz* *b) w odniesieniu do dostępu organów publicznych danego państwa trzeciego do przekazywanych danych osobowych – istotne aspekty systemu prawnego tego państwa trzeciego, w szczególności te wskazane w sposób niewyczerpujący w art. 45 ust. 2 niniejszego rozporządzenia, oraz praktyczne prawdopodobieństwo, że organy publiczne będą dążyć do uzyskania dostępu do przekazywanych danych osobowych lub że taki dostęp zostanie im przyznany* *Pojedyncza ocena może obejmować zestaw podobnych przekazywań, w tym w przypadkach, gdy stosowany jest ten sam lub podobny zestaw odpowiednich zabezpieczeń.* Znowelizować art. 1 decyzji wykonawczej Komisji w sprawie standardowych klauzul umownych, tak aby klauzule te miały zastosowanie do przekazywania danych do podmiotów mających siedzibę w państwach trzecich, które podlegają RODO. *Artykuł 1* *Uznaje się, że standardowe klauzule umowne określone w załączniku zapewniają odpowiednie zabezpieczenia w rozumieniu art. 46 ust. 1 i art. 46 ust. 2 lit. c) rozporządzenia (UE) 2016/679 dotyczące przekazywania przez administratora lub podmiot przetwarzający danych osobowych przetwarzanych zgodnie z tym rozporządzeniem (podmiot przekazujący*	

dane) administratorowi lub podmiotowi przetwarzającemu (podwykonawcy przetwarzania) ustanowionemu w państwie trzecim~~, w przypadku których przetwarzanie danych nie podlega temu rozporządzeniu (podmiot odbierający dane).~~	

UPROSZCZENIE #6 - Doprecyzować okoliczności, w których podmioty uznaje się za „współadministratorów”	
Proponowana zmiana	Uzasadnienie
Zdefiniować pojęcie współadministrowania w art. 4 i zmienić art. 26 *(27) „współadministratorzy” oznaczają co najmniej dwóch administratorów, którzy wyraźnie, w drodze uzgodnienia, wspólnie ustalają cele i sposoby przetwarzania.* Artykuł 26 *Współadministratorzy* *1. ~~Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami.~~ We wspólnych uzgodnieniach ~~W drodze wspólnych uzgodnień~~ współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.* Jako rozwiązanie alternatywne wobec powyższej propozycji należy zmienić art. 26 ust. 1	• Rekomendowane zmiany mają na celu doprecyzowanie definicji współadministratora, tak aby strony były uznawane za współadministratorów tylko wtedy, gdy wyraźnie zgodzą się na taką rolę – czy to w umowie, czy w innym wyraźnym porozumieniu o podobnym charakterze. Celem tej zmiany jest ograniczenie istotnej niepewności prawnej, która obecnie występuje, gdy podmioty mogą nieumyślnie ponosić odpowiedzialność za przetwarzanie danych – wbrew swoim intencjom oraz warunkom uzgodnionym z kontrahentami. • Trzecia z proponowanych zmian ma na celu ograniczenie odpowiedzialności administratorów wyłącznie do przetwarzania, które pozostaje pod ich kontrolą (a nie do każdego przetwarzania, w którym „uczestniczą”). Intencją tej zmiany jest ograniczenie sytuacji, w których niezależny administrator zostaje uznany za odpowiedzialnego za przetwarzanie, nad którym nie sprawuje wyłącznej kontroli. Dodatkowo, proponowana zmiana art. 83 ust. 2 ma na celu ograniczenie przypadków, w których strony ponoszą solidarną odpowiedzialność, gdy działają jako współadministratorzy – pod warunkiem, że taka współpraca została przez nie wyraźnie uzgodniona, zgodnie z proponowanymi zmianami w art. 26 ust. • Ogólnym celem tych zmian jest zapewnienie podmiotom większej pewności prawnej co do ich

Jeżeli co najmniej dwóch administratorów wspólnie ustala, w drodze wyraźnego uzgodnienia, cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. Zmienić art. 82, aby ograniczyć odpowiedzialność współadministratorów *2. ~~Każdy~~ administrator ~~uczestniczący w przetwarzaniu~~ odpowiada za szkody spowodowane przetwarzaniem , które jest pod jego kontrolą, naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.* *3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli ~~udowodnią, że~~ w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.* *4. Jeżeli w tym samym przetwarzaniu uczestnicz~~y więcej niż jeden administrator lub podmiot przetwarzający~~ą współadmistratorzy lub uczestniczy w nim zarówno administrator jak i podmiot*	odpowiedzialności na gruncie RODO, gdy podejmują czynności przetwarzania lub zawierają umowy z innymi podmiotami.

przetwarzający, którzy ~~i~~ zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.	

UPROSZCZENIE #7 - Uzupełnić mandat organów ochrony danych w RODO o wyraźne uznanie interesów gospodarczych i innowacyjnych oraz zapewnić jasność co do wymaganej równowagi między ochroną danych a innymi prawami i interesami.	
Proponowana zmiana	Uzasadnienie
• Proponujemy w art. 51 ust. 1 wprowadzić ochronę innowacji i interesów gospodarczych oraz równowagę praw i interesów do obowiązków organów ochrony danych, oprócz „odpowiedzialności za monitorowanie stosowania niniejszego rozporządzenia w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii”.	Organy ochrony danych nie potrafią właściwie wyważyć praw podstawowych i innych interesów w interpretacji, stosowaniu i egzekwowaniu RODO, co skutkuje podejściem opartym na zerowym ryzyku i absolutnym pierwszeństwie ochrony danych przed wszelkimi innymi konkurencyjnymi wartościami, w tym innymi prawami i wolnościami podstawowymi, w szczególności gdy w grę wchodzą względy ekonomiczne. W rezultacie administratorzy danych są narażeni na absolutystyczne podejście organów ochrony danych, nieproporcjonalne obowiązki w zakresie zgodności, nadmierne obciążenia i niepewność prawną, co utrudnia im nie tylko przestrzeganie przepisów, ale także wprowadzanie innowacji i zachowanie konkurencyjności.

UPROSZCZENIE #8 - Wzmocnienie balansu między prawem do prywatności a innymi prawami podstawowymi i powiązanymi interesami	
Proponowana zmiana	Uzasadnienie
• Proponujemy włączenie treści motywu 4 dotyczącego równoważenia praw do art. 1, aby zapewnić pełną pewność prawną w odniesieniu do tego kluczowego obowiązku organów regulacyjnych i podmiotów podlegających regulacji. • Postulujemy dostosowanie do innych przepisów UE w celu promowania innowacyjności i	Przedsiębiorcy mogą napotykać ograniczenia w prowadzeniu działalności gospodarczej i wprowadzaniu innowacji z powodu nadmiernego nacisku na ochronę danych. Niepewność prawna i potencjalne konflikty z innymi prawami, takimi jak wolność wypowiedzi i wolność prowadzenia działalności gospodarczej.

konkurencyjności.	

Dyrektywa o e-prywatności

UPROSZCZENIE #1 - Rozszerzenie wyjątku od wymogu uzyskania zgody zgodnie z art. 5 ust. 3 Dyrektywy o e-prywatności odniesieniu do plików cookie i innych form dostępu do danych lub ich przechowywania na urządzeniu w celach związanych z bezpieczeństwem	
Proponowana zmiana	Uzasadnienie
Zmiana art. 5 ust. 3 Dyrektywy o e-prywatności i rozszerzenie zakresu wyjątków o cookies związane z bezpieczeństwem *3. Państwa Członkowskie zapewniają, że przechowywanie informacji lub uzyskanie dostępu do informacji przechowanej na terminalu abonenta lub użytkownika jest dozwolone wyłącznie pod warunkiem że abonent lub użytkownik otrzymą jasną i wyczerpującą informację zgodnie z dyrektywą 95/46/WE, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla technicznego przechowywania danych lub dostępu do danych:* *a) jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej; ~~lub~~* *b) gdy jest to szczególnie niezbędne w celu dostarczania usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika;* *c) niezbędnych do zapewnienia lub przywrócenia bezpieczeństwa albo wykrycia usterki technicznej lub błędów w sieciach łączności elektronicznej lub usługach (oraz powiązanych usługach lub urządzeniach).* *d) niezbędnych do wykrycia lub*	• Proponowana zmiana ma na celu dostosowanie przepisów art. 5 ust. 3 dotyczących przetwarzania danych na urządzeniu do realiów, w jakich podmioty obecnie przetwarzają dane w środowisku online. Obecne przepisy są zbyt restrykcyjne i tworzą niepotrzebne bariery dla wielu uzasadnionych zastosowań plików cookie i podobnych technologii o niskim wpływie na prywatność. • Co więcej, obecny stan prawny sprawia, że przechowywanie lub dostęp do danych na urządzeniu podlega bardziej rygorystycznym zasadom niż np. przetwarzanie w chmurze – mimo że rozwój technologiczny prowadzi do projektowania produktów i funkcji, które celowo przechowują dane lokalnie, właśnie ze względu na ich większą zgodność z zasadami ochrony prywatności. • Sugerowane dodanie lit. c) i d) do art. 5 ust. 3 ma umożliwić dostęp do informacji na urządzeniu użytkownika lub ich przechowywanie (np. za pomocą plików cookie), gdy jest to niezbędne w uzasadnionych przypadkach, takich jak bezpieczeństwo, utrzymanie produktu czy wykrywanie nadużyć i oszustw – również wtedy, gdy nadużycia lub manipulacje usługą naruszają prawa lub interesy innych podmiotów (np. klientów polegających na tej usłudze). Zmiana ta przyniesie korzyści zarówno użytkownikom, jak i branży, ponieważ zapewni bezpieczne świadczenie usług online z wykorzystaniem metod

zapobiegania oszustwom, nadużyciom lub manipulacjom dotyczącym sieci łączności elektronicznej i usług (oraz powiązanych usług i urządzeń) przez użytkownika, abonenta lub inną stronę, w tym w przypadkach, gdy takie działania naruszają prawa i uzasadnione interesy innych osób lub podważają integralność sieci lub usługi;	przetwarzania lokalnego. ● Ogólnie rzecz biorąc, zmiany te mają na celu zwiększenie pewności prawnej dla podmiotów działających w środowisku cyfrowym (w tym MŚP), z których wiele polega na plikach cookie lub podobnych technologiach w celu zapewnienia bezpieczeństwa swoich usług. ● Z perspektywy użytkownika, bardziej elastyczne zasady dotyczące uzyskiwania zgody mogłyby prowadzić do ograniczenia liczby banerów cookie oraz związanego z tym „zmęczenia klikaniem", które obecnie doskwiera internautom. Doprecyzowanie przepisów pozwoliłoby również ograniczyć niepewność prawną i zakłócenia w funkcjonowaniu rynku wewnętrznego, wynikające z niespójnej interpretacji obecnych regulacji przez organy nadzorcze.

UPROSZCZENIE #2 - Rozszerzenie wyjątku od wymogu uzyskania zgody zgodnie z art. 5 ust. 3 Dyrektywy o e-prywatności odniesieniu do plików cookie i innych form dostępu do danych lub ich przechowywania na urządzeniu w celach analitycznych	
Proponowana zmiana	Uzasadnienie
Zmiana art. 5 ust. 3 Dyrektywy o e-prywatności i rozszerzenie zakresu wyjątków o analityczne cookies *3. Państwa Członkowskie zapewniają, że przechowywanie informacji lub uzyskanie dostępu do informacji przechowanej na terminalu abonenta lub użytkownika jest dozwolone wyłącznie pod warunkiem że abonent lub użytkownik otrzyma jasną i wyczerpującą informację zgodnie z dyrektywą 95/46/WE, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla technicznego przechowywania danych lub dostępu do danych:* *a) jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej;* ~~*lub*~~	● Proponowana zmiana ma na celu dostosowanie przepisów art. 5 ust. 3 dotyczących przetwarzania danych na urządzeniu do realiów, w jakich podmioty obecnie przetwarzają dane w środowisku online. Obecne przepisy są zbyt restrykcyjne i tworzą niepotrzebne bariery dla wielu uzasadnionych zastosowań plików cookie i podobnych technologii o niskim wpływie na prywatność. ● Co więcej, obecny stan prawny sprawia, że przechowywanie lub dostęp do danych na urządzeniu podlega bardziej rygorystycznym zasadom niż np. przetwarzanie w chmurze – mimo że rozwój technologiczny prowadzi do projektowania produktów i funkcji, które celowo przechowują dane lokalnie, właśnie ze względu na ich większą zgodność z zasadami ochrony

b) gdy jest to szczególnie niezbędne w celu dostarczania usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika; *c) niezbędnych dla pomiarów korzystania z treści lub usług internetowych.* Nowy motyw: *Pojęcie pomiaru korzystania z treści lub usług internetowych, o którym mowa w art. 5 ust. 3 lit. e) niniejszej dyrektywy, obejmuje pomiar ruchu na stronie internetowej, w aplikacji lub usłudze w celu zrozumienia, w jaki sposób dana strona, aplikacja lub usługa jest wykorzystywana, pod warunkiem że pomiar ten nie wiąże się z profilowaniem użytkowników z różnych stron, aplikacji lub usług.*	prywatności. • Sugerowane dodanie lit. c) do art. 5 ust. 3 oraz odpowiadającego mu motywu ma na celu umożliwienie dostępu do informacji na urządzeniu lub ich przechowywania w przypadkach użycia związanych z analizą danych. Jaśniejsze i bardziej elastyczne zasady określające, kiedy taki dostęp lub przechowywanie jest dopuszczalne w celach analitycznych, zmniejszą bariery dla innowacji oraz ograniczą niepewność prawną wynikającą z obecnych przepisów. • Ogólnie rzecz biorąc, zmiany te mają na celu zwiększenie pewności prawnej dla podmiotów działających w środowisku cyfrowym (w tym MŚP), z których wiele opiera swój model biznesowy na reklamie internetowej oraz innych zastosowaniach technologii cookie i podobnych – czy to w celu generowania przychodów, czy zapewnienia bezpieczeństwa i poprawy jakości usług. • Z perspektywy użytkownika, bardziej elastyczne zasady dotyczące uzyskiwania zgody mogłyby prowadzić do ograniczenia liczby banerów cookie oraz związanego z tym „zmęczenia klikaniem”, które obecnie doskwiera internautom. Doprecyzowanie przepisów pozwoliłoby również ograniczyć niepewność prawną i zakłócenia w funkcjonowaniu rynku wewnętrznego, wynikające z niespójnej interpretacji obecnych regulacji przez organy nadzorcze.

UPROSZCZENIE #3 - Rozszerzenie wyjątku od wymogu uzyskania zgody zgodnie z art. 5 ust. 3 Dyrektywy o e-prywatności odniesieniu do plików cookie i innych form dostępu do danych lub ich przechowywania na urządzeniu w celach wyświetlania użytkownikom reklamy kontekstowej	
Proponowana zmiana	Uzasadnienie
Zmiana art. 5 ust. 3 Dyrektywy o e-prywatności i rozszerzenie zakresu wyjątków o zezwolenie na wyświetlanie użytkownikom reklamy kontekstowej	• Proponowana zmiana ma na celu dostosowanie przepisów art. 5 ust. 3 dotyczących przetwarzania danych na urządzeniu do realiów, w jakich podmioty obecnie przetwarzają dane w środowisku online. Obecne przepisy są

3. Państwa Członkowskie zapewniają, że przechowywanie informacji lub uzyskanie dostępu do informacji przechowanej na terminalu abonenta lub użytkownika jest dozwolone wyłącznie pod warunkiem że abonent lub użytkownik otrzyma jasną i wyczerpującą informację zgodnie z dyrektywą 95/46/WE, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla technicznego przechowywania danych lub dostępu do danych: *a) jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej;* ~~*lub*~~ *b) gdy jest to szczególnie niezbędne w celu dostarczania usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika;* *c) niezbędnych do wyświetlania użytkownikowi reklamy kontekstowej.* Nowy motyw - reklama kontekstowa *Pojęcie reklamy kontekstowej, o którym mowa w art. 5 ust. 3 lit. f), oznacza reklamę internetową wybieraną na podstawie danych zebranych podczas jednej sesji, w trakcie której użytkownik wchodzi w interakcję ze stroną internetową, aplikacją lub usługą. Może to obejmować wybór reklamy w oparciu o: (i) treść, z którą użytkownik aktualnie się zapoznaje, (ii) w przypadku wyszukiwarki – jego bieżące zapytanie, a także (iii) aktualnie używane urządzenie użytkownika.*	zbyt restrykcyjne i tworzą niepotrzebne bariery dla wielu uzasadnionych zastosowań plików cookie i podobnych technologii o niskim wpływie na prywatność. ● Co więcej, obecny stan prawny sprawia, że przechowywanie lub dostęp do danych na urządzeniu podlega bardziej rygorystycznym zasadom niż np. przetwarzanie w chmurze – mimo że rozwój technologiczny prowadzi do projektowania produktów i funkcji, które celowo przechowują dane lokalnie, właśnie ze względu na ich większą zgodność z zasadami ochrony prywatności. ● Sugerowane dodanie lit. c) do art. 5 ust. 3 oraz odpowiadającego mu motywu ma na celu umożliwienie dostępu do informacji na urządzeniu lub ich przechowywania w celu wyświetlania użytkownikom reklamy kontekstowej. Jaśniejsze i bardziej elastyczne zasady określające, kiedy taki dostęp lub przechowywanie jest dopuszczalne w celach reklamy kontekstowej, zmniejszą bariery dla innowacji oraz ograniczą niepewność prawną wynikającą z obecnych przepisów. ● Ogólnie rzecz biorąc, zmiany te mają na celu zwiększenie pewności prawnej dla podmiotów działających w środowisku cyfrowym (w tym MŚP), z których wiele opiera swój model biznesowy na reklamie internetowej oraz innych zastosowaniach technologii cookie i podobnych w celu generowania przychodów. ● Z perspektywy użytkownika, bardziej elastyczne zasady dotyczące uzyskiwania zgody mogłyby prowadzić do ograniczenia liczby banerów cookie oraz związanego z tym „zmęczenia klikaniem”, które obecnie doskwiera internautom. Doprecyzowanie przepisów pozwoliłoby również ograniczyć niepewność prawną i zakłócenia w funkcjonowaniu rynku wewnętrznego, wynikające z niespójnej interpretacji obecnych regulacji przez organy nadzorcze.

UPROSZCZENIE #4 - Doprecyzowanie, że wyświetlanie banera cookie nie jest wymagane w przypadku skorzystania z jednego z wyjątków przewidzianych w art. 5 ust. 3 (tj. gdy zgoda użytkownika nie jest wymagana)	
Proponowana zmiana	Uzasadnienie
Dodanie nowego art. 5 ust. 4 w Dyrektywie o e-prywatności, który precyzuje, że baner cookie nie musi być wyświetlany użytkownikowi, gdy zgoda na mocy Dyrektywy o e-prywatności nie jest wymagana *4. Jednostkom podejmującym czynności objęte art. 5 ust. 3 przyznaje się swobodę określenia, w jaki sposób informacja, o której mowa w tym przepisie, będzie przedstawiana w sposób jasny i wyczerpujący.* Nowy motyw *Zapewnienie jasnej i wyczerpującej informacji, o której mowa w art. 5 ust. 3 niniejszej dyrektywy, nie wymaga, w odniesieniu do czynności obętych lit. [a) - e) w art. 5 ust. 3], stosowania tzw. „banerów cookie", pod warunkiem że wymagane informacje są przedstawione w powiadomieniu, które jest łatwo dostępne dla użytkownika. Informacje przekazane na potrzeby art. 5 ust. 3 powinny być wyczerpujące dla celów przetwarzania. Nie jest wymagane zapewnianie wyczerpującej informacji w odniesieniu do cookies lub innych podobnych technologii wykorzystywanych do przechowywania lub uzyskania dostępu do informacji przechowywanej na terminalu użytkownika.*	• Podobnie jak wcześniejsze uproszczenia, ta zmiana ma na celu doprecyzowanie zasad dotyczących dostępu do informacji na urządzeniu i ich przechowywania (w szczególności wykorzystywania plików cookie) oraz zwiększenie pewności prawnej dla podmiotów działających w środowisku cyfrowym. Wiele podmiotów (w tym MŚP) polega na plikach cookie i podobnych technologiach w celu zapewnienia bezpieczeństwa swoich usług lub ich ulepszania (np. poprzez wykorzystanie analityki). Doprecyzowanie przepisów pozwoliłoby ograniczyć istotną niepewność prawną i zakłócenia w rynku wewnętrznym wynikające z niespójnej interpretacji obecnych zasad przez organy nadzorcze. • Z perspektywy użytkownika, bardziej elastyczne zasady dotyczące uzyskiwania zgody mogłyby prowadzić do ograniczenia liczby banerów cookie oraz związanego z tym „zmęczenia klikaniem", które obecnie doskwiera internautom. W sytuacjach, gdy zgoda nie jest wymagana, obciążanie użytkownika taką informacją nie przynosi istotnych korzyści dla prywatności – tym bardziej że może on z łatwością uzyskać do niej dostęp w polityce prywatności lub odpowiednim powiadomieniu, jeśli tylko będzie chciał.

UPROSZCZENIE #5 - Doprecyzowanie, że „przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanych" nie ma na celu obejmowania krótkotrwałego przechowywania lub informacji przesyłanych w ramach zwykłego połączenia internetowego	
Proponowana zmiana	Uzasadnienie
Zmiana art. 5 ust. 3 Dyrektywy o e-prywatności w celu doprecyzowania, co należy (a raczej czego nie należy) rozumieć	• Celem proponowanej zmiany jest wyraźne wskazanie, że informacje przesyłane w ramach zwykłego działania internetu (np. w ramach

przez „przechowywanie” i „dostęp” *3. Państwa Członkowskie zapewniają, że przechowywanie informacji lub uzyskanie dostępu do informacji przechowanej na terminalu abonenta lub użytkownika jest dozwolone wyłącznie pod warunkiem że abonent lub użytkownik otrzyma jasną i wyczerpującą informację zgodnie z dyrektywą 95/46/WE, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla technicznego przechowywania danych lub dostępu do danych jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub gdy jest to szczególnie niezbędne w celu dostarczania usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika. Przechowywanie i uzyskiwanie dostępu, o których mowa w ust. 3, nie obejmują tymczasowego lub krótkotrwałego przechowywania ani operacji stanowiących część zwykłej wymiany informacji z terminalem, gdy użytkownik lub abonent uzyskuje dostęp do usługi społeczeństwa informacyjnego.*	protokołów TCP/IP) lub urządzenia, które nie są celowo kierowane do konkretnego odbiorcy czy nadawcy, nie podlegają przepisom art. 5 ust. 3. • Zbyt szeroka interpretacja art. 5 ust. 3, która przypadkowo obejmuje dane przesyłane w ramach zwykłego działania internetu, nie realizuje głównego celu Dyrektywy o e-prywatności, jakim jest ochrona prywatności użytkowników. • Przeciwnie, niesie ze sobą ryzyko: (i) dalszego zwiększenia liczby codziennych interakcji online wymagających zgody, co prowadzi do „zmęczenia zgodami” i zmniejszenia zaangażowania użytkowników wobec rzeczywistych technologii śledzących; (ii) dalszego pogorszenia doświadczenia użytkowników w UE, którzy mogliby zostać zmuszeni do podejmowania nierealistycznych decyzji dotyczących zgody na kluczowe procesy funkcjonowania ekosystemu internetowego; oraz (iii) niemal całkowitego pokrycia się zakresów Dyrektywy o e-prywatności i RODO w odniesieniu do wszelkich danych osobowych zbieranych w środowisku online. Co istotne, podważa to zasadę ograniczenia celu przetwarzania w RODO, która w przeciwnym razie umożliwiałaby dalsze przetwarzanie takich danych w zgodnych celach.

UPROSZCZENIE #6 - Częściowe zniesienie przepisów dot. marketingu bezpośredniego	
Proponowana zmiana	Uzasadnienie
Proponujemy częściowe zniesienie przepisów ePD dot. marketingu bezpośredniego poprzez usunięcie art. 13 ust. 3 dotyczącego niechcianych wiadomości. RODO będzie nadal miało zastosowanie do marketingu bezpośredniego, o ile wiąże się to z wykorzystaniem danych osobowych. Ponadto, postulujemy wymóg dostosowania krajowego wdrożenia ePD do zmian w ePD.	Przepisy ePD dotyczące marketingu bezpośredniego miały pierwotnie na celu ochronę przed niechcianymi komunikatami 1:1 od reklamodawców do ich obecnych i potencjalnych klientów poprzez wykorzystanie adresów e-mail lub numerów SMS tych ostatnich do celów kampanii marketingowych. Przepisy ePD dotyczące marketingu bezpośredniego różnią się w zależności od sposobu ich wdrożenia przez państwa członkowskie, a system ten jest zbędny i niezgodny z RODO (marketing

	bezpośredni w RODO podlega podstawom prawnym uzasadnionego interesu zgodnie z motywem 47, ale podlega zgodzie zgodnie z ePD), co powoduje niepewność prawną i utrudnia rentowność wielu usług internetowych.

UPROSZCZENIE #7 - Częściowe zniesienie i harmonizacja przepisów dot. danych o ruchu	
Proponowana zmiana	Uzasadnienie
● Proponujemy częściowe zniesienie przepisów poprzez rewizję Art. 5 ust. 1 i usunięcie odniesienia do „i powiązanych danych o ruchu", a także usunięcie art. 6 dotyczącego danych o ruchu. ● Ponadto, postulujemy zapewnienie dostosowania krajowego wdrożenia ePD do zmian w ePD. ● Postulujemy także ujednolicenie interpretacji minimalizacji danych i ograniczenia celu w celu zapewnienia spójności przepisów RODO i powiązanych przepisów UE	Urządzenia podłączone do sieci mają kluczowe znaczenie dla innowacji w UE, a nowoczesne pojazdy są w zasadzie komputerami na kołach, które nieustannie gromadzą i przesyłają dane za pośrednictwem wbudowanych kart SIM (np. do nawigacji, diagnostyki, systemów informacyjno-rozrywkowych, połączeń alarmowych itp.). Komunikacja ta jest często kierowana przez sieci komórkowe, co oznacza, że generuje dane o ruchu zgodnie z definicją zawartą w ePD.

PROPOZYCJE UPROSZCZEŃ W ZAKRESIE BEZPIECZEŃSTWA

Podsumowanie - należy:

- Nadać ENISA uprawnienia do przeprowadzania ocen wpływu na bezpieczeństwo dla wszystkich nowych aktów prawnych dotyczących technologii. W tym także w odniesieniu do istniejących regulacji, takich jak DMA poprzez Wysoką Grupę Roboczą.

- Uprościć procesy certyfikacyjne i obowiązki sprawozdawcze oraz zapewnić rozsądny czas na ich realizację przez przedsiębiorstwa.

- Uprościć wymogi w zakresie zarządzania cyberbezpieczeństwem i ograniczyć zróżnicowane rozwiązania krajowych.

- Uprościć certyfikację dostępu do rynku.
    - Zharmonizowane specyfikacje norm w ramach dyrektywy radiowej (RED) powinny być publikowane co najmniej 12 miesięcy przed datą, od której ich stosowanie stanie się obowiązkowe. Jeśli norma nie będzie gotowa na czas, data wejścia w życie powinna zostać odpowiednio przesunięta.
    - W procesie przechodzenia od wymagań RED do wymagań Aktu dotyczącego cyberodporności (CRA), certyfikacja uzyskana na podstawie RED powinna umożliwiać wstępną zgodność z CRA – wymagając jedynie dodatkowej weryfikacji cyklu życia bezpiecznego rozwoju po stronie producenta.
    - Branżowe programy certyfikacyjne powinny być uznawane za spełniające wymagania.
    - Certyfikacja sprzętu i oprogramowania w ramach RED powinny zostać rozdzielone, co ma kluczowe znaczenie dla urządzeń takich jak telefony i tablety.

- Zharmonizować wymogi dotyczące zgłaszania incydentów.
    - Upoważnić i wyposażyć w odpowiednie kompetencje jeden ogólnounijny organ uprawniony do przyjmowania zgłoszeń, który utworzy jeden portal i jeden wzór formularza do zgłaszania incydentów na podstawie RODO, Rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA), dyrektywy NIS 2, CRA oraz Aktu o sztucznej inteligencji (AI Act).
    - Ujednolicić progi i terminy zgłaszania incydentów.
    - Ujednolicić sposób obliczania momentu, od którego zaczyna biec termin na zgłoszenie, wzorując się na podejściu przyjętym w Dyrektywie NIS2.
    - Wprowadzić jednolite zgłaszanie – doprecyzować, że zgłoszenie dokonane na podstawie jednej dyrektywy lub rozporządzenia spełnia wymagania pozostałych.

- Uprościć wymogi w zakresie zarządzania cyberbezpieczeństwem.
    - Wykorzystać istniejące standardy (ISO, NIST)
    - Ograniczyć stosowanie krajowych systemów certyfikacji.

- Wzmocnić rolę ENISA przy uwzględnianiu kwestii bezpieczeństwa we wszystkich nowych unijnych regulacjach dotyczących technologii. Należy nadać ENISA kompetencje do przeprowadzania ocen wpływu na bezpieczeństwo dla wszystkich nowych przepisów z zakresu nowych technologii, aby uniknąć niezamierzonych skutków dla bezpieczeństwa obywateli.

Rekomendacje szczegółowe

1. Uproszczenie certyfikacji dostępu do rynku (Dyrektywa w sprawie urządzeń radiowych, Akt dotyczący cyberodporności, Europejski program certyfikacji cyberbezpieczeństwa oparty na wspólnych kryteriach, Akt w sprawie danych)

Aktualny i nadchodzący reżim certyfikacji produktów stwarza wiele wyzwań dla producentów. Przykładowo, zgodnie z Dyrektywą w sprawie urządzeń radiowych (RED), zharmonizowane normy ogłaszano zbyt późno, zmuszając przedsiębiorstwa do przeprowadzania testów w oparciu o przyszłe, a nie obowiązujące standardy. Ponadto, RED stwarza problemy łącząc certyfikację sprzętu z harmonogramem wydawania oprogramowania. Oprogramowanie analizuje się znacznie bliżej daty wprowadzenia produktu na rynek, podczas gdy certyfikacja sprzętu jest wymagana przed rozpoczęciem produkcji – co prowadzi do istotnych rozbieżności w harmonogramie (np. 3-miesięcznej przerwy, w której zespoły zajmujące się sprzętem potrzebują certyfikacji na gruncie RED, gdy tymczasem prace nad oprogramowaniem wciąż trwają).

W związku z nadchodzącym Aktem dotyczącym cyberodporności (CRA), brak dostępnych zharmonizowanych norm ogranicza prace przygotowawcze. Co więcej, niektóre przepisy, takie jak potencjalny 5-letni minimalny okres wsparcia, mogą być niewykonalne w przypadku niektórych kategorii produktów (np. słuchawek dousznych). Potrzeba też jasności co do tego, czy aplikacje fabrycznie zainstalowane na urządzeniach, takich jak telefony, tablety i telewizory, wymagać będą odrębnej certyfikacji.

W szerszym ujęciu, regulacje takie jak unijny Akt w sprawie danych skorzystałyby na lepszym dostosowaniu do obowiązujących standardów i programów certyfikacji. Jest ono kluczowe, by zespoły deweloperskie wiedziały, czego dokładnie się od nich oczekuje, i by mogły korzystać z testów prowadzonych przez strony trzecie dla weryfikacji zgodności.

Kwestie te przekładają się na konkretne negatywne skutki, w tym znaczne koszty operacyjne. Zakłóceniu ulegają harmonogramy rozwoju produktów, a poziom niepewności prawnej i operacyjnej wzrasta. Potencjalna konieczność ponownego testowania wszystkich urządzeń zgodnie z CRA, mimo że wcześniej zostały one certyfikowane na podstawie RED, oznaczałaby ogromne obciążenie dla branży, przy wątpliwym wpływie na realne zwiększenie bezpieczeństwa produktów.

Proponowane rozwiązania:

- Terminowe publikowanie norm: Zharmonizowane normy w powinny być publikowane co najmniej 12 miesięcy przed datą stosowania rozporządzenia. Jeśli normy nie są przygotowane, data stosowania przepisów powinna być odpowiednio odłożona w czasie.

- Płynne ścieżki przejścia: przejście z RED na CRA powinno obejmować jasną ścieżkę, na mocy której urządzenia certyfikowane zgodnie z RED mogłyby zostać automatycznie uznane lub wstępnie zatwierdzone; w przypadku tych urządzeń zgodność z CRA powinna obejmować weryfikację bezpiecznego cyklu życia u producenta, czyli głównej różnicy między RED a CRA.

- Uznawanie certyfikatów branżowych: ugruntowane programy certyfikacji branżowej powinny być uznawane jako wykazujące zgodność z wymogami regulacyjnymi. Jednostki notyfikowane mogłyby zachować swoją nadzorczą rolę, jednak przyjmowane powinny być też raporty z testów w ramach uznanych programów certyfikacji branżowej. Przykładowo, pomocne byłoby uznanie programu certyfikacji bezpieczeństwa urządzeń mobilnych GSMA (MDSCert), opartego na normie ETSI TS 103 732-1 („Consumer Mobile Device Protection Profile"), jako wystarczającego dowodu zgodności w zakresie bezpieczeństwa urządzeń mobilnych.

- Uznawanie standardów międzynarodowych: Unia Europejska powinna w większym stopniu korzystać z istniejących standardów międzynarodowych, zamiast tworzyć nowe normy europejskie, które mogą prowadzić do dodatkowych wymogów zgodności, barier handlowych i opóźnień we wdrażaniu rozwiązań technicznych oraz realizacji celów regulacyjnych.

- Rozdzielenie certyfikacji sprzętu i oprogramowania: W przypadku urządzeń takich jak telefony i tablety, kluczowe jest rozdzielenie procesów certyfikacji sprzętu i oprogramowania w ramach RED (a w odpowiednich przypadkach także CRA), tak aby odpowiadały one rzeczywistym cyklom rozwoju produktu.

Zmiany te zapewniłyby przewidywalność niezbędną dla skutecznego rozwoju produktów, który zazwyczaj rozpoczyna się na 12 miesięcy przed ich wprowadzeniem na rynek. Jasne i odpowiednio wczesne wymagania są kluczowe dla planowania zasobów i funkcjonalności. Uznawanie certyfikatów branżowych może pomóc wypełnić lukę między ogólnym urzędowym językiem a konkretnymi wymaganiami inżynieryjnymi, ponieważ certyfikaty te często zawierają szczegółowe plany testów i kryteria akceptacji dostosowane do danej kategorii produktów. Takie podejście ogranicza dublowanie wysiłków, obniża koszty zapewnienia zgodności i pozwala branży skoncentrować zasoby na realnym zwiększaniu bezpieczeństwa produktów – co ostatecznie przynosi korzyści konsumentom i przedsiębiorstwom w UE.

2. Harmonizacja wymogów dotyczących zgłaszania incydentów

Ekosystem cyfrowy UE podlega różnym reżimom regulacyjnym (np. RODO, Akt w sprawie operacyjnej odporności cyfrowej, Dyrektywa NIS2, CRA, Akt o sztucznej inteligencji), które nakładają obowiązek zgłaszania incydentów związanych z dostępnością, bezpieczeństwem, prywatnością i ochroną. Pojedynczy incydent może się wiązać z obowiązkiem zgłoszenia na gruncie wielu uregulowań – a każde z nich przewiduje różne kryteria (np. „poważne" [„significant"] incydenty w Dyrektywie NIS2 i „poważne" [„severe"] incydenty w CRA), terminy zgłaszania i właściwe organy. Może to skutkować koniecznością zgłoszenia tego samego incydentu w nawet 27 państwach członkowskich UE, za pośrednictwem różnych formularzy i narzędzi raportowania.

Takie powielające się, niespójne i skomplikowane wymogi zgłaszania odciągają kluczowe zasoby od faktycznego reagowania na incydenty i podejmowania działań naprawczych, przekierowując je na potrzeby spełniania obowiązków administracyjnych. To obciążenie w niewielkim stopniu przyczynia się do realizacji zamierzonego celu, jakim jest wzmocnienie cyberbezpieczeństwa i zdolności reagowania na incydenty w całej UE.

Proponowane rozwiązania:

- Jeden unijny mechanizm zgłaszania: upoważnienie i wyposażenie w odpowiednie kompetencje jednego, ogólno-unijnego organu, zajmującego się zgłoszeniami, który utworzy jeden portal i jeden wzór formularza do zgłaszania incydentów na podstawie ww. przepisów.

- Harmonizacja elementów raportowania:
    - Progi: ujednolicenie definicji i progów dla incydentów podlegających zgłoszeniu w różnych regulacjach (np. zharmonizowanie pojęć „poważny" [„severe"] i „poważny" [„significant"]).
    - Terminy: przegląd i ustandaryzowanie terminów zgłaszania incydentów, w oparciu o 72-godzinny deadlinie, celem zapewnienia spójności i zmniejszenia obciążeń pracowników zajmujących się reagowaniem na incydenty.
    - Zasada „zgłoś raz, spełnij wiele obowiązków": zgłoszenie incydentu na podstawie jednej kluczowej regulacji (np. Dyrektywy NIS2) powinno być równoznaczne z wypełnieniem obowiązków zgłoszenia na gruncie innych właściwych aktów prawnych (np. Dyrektywy w sprawie odporności podmiotów krytycznych).

Uproszczony i ujednolicony proces zgłaszania pozwoli podmiotom skuteczniej koncentrować się na działaniach związanych z reagowaniem na incydenty. Przełoży się to na szybsze przywracanie sprawności po incydentach bezpieczeństwa, ograniczenie szkód dla użytkowników i usług, a w efekcie na bardziej odporny i bezpieczny ekosystem cyfrowy w UE.

3. Optymalizacja zarządzania cybezbezpieczeństwem

Wiele unijnych aktów prawnych (np. Dyrektywa NIS2, Akt o odporności cyfrowej, Rozporządzenie ws. operacyjnej odporności cyfrowej, Akt o cybersolidarności, Akt o cyberbezpieczeństwie, RODO) tworzy złożony obraz wymogów w zakresie zarządzania cyberbezpieczeństwem, koordynacji i współpracy. Chociaż celem tych przepisów jest poprawa bezpieczeństwa, mnożenie wymagań może prowadzić do niejasności i obciążeń administracyjnych – zwłaszcza gdy powielają one dobrze ugruntowane międzynarodowe ramy bezpieczeństwa (np. ISO 27001). Co więcej, możliwość przyjmowania przez poszczególne państwa członkowskie UE własnych, niespójnych systemów certyfikacji cyberbezpieczeństwa wprowadza kolejny poziom złożoności.

Niejasne lub powielające się wymogi w zakresie zarządzania cyberbezpieczeństwem stanowią ogromne obciążenie administracyjne dla przedsiębiorstw. Obciążenie to często nie przekłada się na realną poprawę ich poziomu bezpieczeństwa, zwłaszcza gdy zasoby są kierowane na wykazywanie zgodności z wieloma nakładającymi się ramami regulacyjnymi, zamiast na wdrażanie solidnych środków ochrony.

Proponowane rozwiązania:

- Wykorzystywanie standardów międzynarodowych: zachęcanie do stosowania istniejących, uznanych na świecie ram bezpieczeństwa (takich jak ISO 27001 czy ETSI EN 303 645) jako punktu odniesienia przy wykazywaniu zgodności z unijnymi wymogami w zakresie zarządzania cyberbezpieczeństwem – zamiast tworzenia nowych, odrębnych obowiązków tylko dla podmiotów z UE.

- Ograniczanie niespójnych systemów krajowych: aktywne zniechęcanie państw członkowskich do przyjmowania własnych krajowych systemów certyfikacji cyberbezpieczeństwa, które odbiegają od zharmonizowanego podejścia Unii lub uznanych standardów międzynarodowych. ENISA mogłaby odgrywać silniejszą rolę w promowaniu takiej harmonizacji.

Oparcie unijnych wymogów na powszechnie stosowanych standardach międzynarodowych ułatwia współpracę na rynkach globalnych, zmniejsza koszty i obowiązki dla przedsiębiorstw działających międzynarodowo oraz pozwala im korzystać z wcześniej wdrożonych rozwiązań w zakresie bezpieczeństwa. Takie podejście zapewnia, że zasoby są kierowane na realne wzmocnienie bezpieczeństwa, a nie na poruszanie się po rozdrobnionym i powielającym się stanie prawnym.

4. Wzmocnienie roli ENISA w kształtowaniu unijnej polityki technologicznej

Regulacje dotyczące polityki technologicznej, nawet jeśli nie koncentrują się bezpośrednio na cyberbezpieczeństwie, mogą mieć szeroki i daleko idący wpływ na bezpieczeństwo obywateli UE i wykorzystywanych przez nich usług cyfrowych. Przestrzeganie różnych regulacji technologicznych – w tym Aktu w sprawie sztucznej inteligencji i Aktu o rynkach cyfrowych – może w niektórych przypadkach nieumyślnie osłabiać istniejące mechanizmy ochrony, które przedsiębiorcy już wdrożyli. Konieczność dostosowania się do wielu odrębnych aktów prawnych może prowadzić do sytuacji, w których wybory projektowe mające na celu zapewnienie bezpieczeństwa i integralności produktów muszą zostać zmodyfikowane w sposób, który wprowadza nowe ryzyka lub osłabia dotychczasowe zabezpieczenia. Bezpieczeństwo powinno być uwzględniane na każdym etapie procesu legislacyjnego i regulacyjnego, aby zagwarantować bezpieczeństwo cyfrowe dla wszystkich.

Proponowane rozwiązania:

- Niezależna ocena wpływu na bezpieczeństwo dla unijnych regulacji dotyczących polityki technologicznej: Tak jak UE przeprowadza ocenę wpływu nowych inicjatyw na gospodarkę, społeczeństwo i środowisko, tak samo starannie powinna oceniać, czy nowe polityki technologiczne nie zagrażają bezpieczeństwu i prywatności obywateli. Zmieniony Akt o cyberbezpieczeństwie powinien przyznać ENISA jednoznaczną i wzmocnioną rolę jako bezstronnego podmiotu oceniającego projektowane regulacje technologiczne w UE. ENISA mogłaby opracowywać „ocenę wpływu na bezpieczeństwo” dla takich inicjatyw, co pozwoliłoby lepiej kształtować proces legislacyjny i przyniosło lepsze rezultaty dla obywateli.

Zapewnienie decydentom dedykowanej oceny wpływu na bezpieczeństwo – przygotowanej przez wyspecjalizowaną instytucję taką jak ENISA – umożliwiłoby lepsze zrozumienie potencjalnych negatywnych skutków proponowanych regulacji dla bezpieczeństwa cyfrowego ekosystemu UE oraz ich skuteczniejsze ograniczanie. Dzięki temu nowe przepisy, realizując swoje główne cele, nie narażałyby użytkowników na niezamierzone zagrożenia dla ich bezpieczeństwa i ochrony.

- Dostosowanie mandatu do zasobów: ENISA odgrywa kluczową rolę w unijnym ekosystemie cyberbezpieczeństwa, wspierając wdrażanie regulacji takich jak Dyrektywa NIS2 czy Akt dotyczący cyberodporności poprzez dostarczanie niezależnej ekspertyzy technicznej, dzielenie się dobrymi praktykami, konsultacje z sektorem prywatnym oraz wspieranie podmiotów różnej wielkości. Każda nowelizacja Aktu o cyberbezpieczeństwie musi wzmacniać mandat ENISA jako niezależnego, technicznego i doradczego organu, zapewniając jej jednocześnie dodatkowe zasoby wspierające realizację poszerzającej się misji. Przykładowo, ENISA pełni obecnie istotną rolę w koordynowaniu wspólnych działań z przemysłem w zakresie gotowości cybernetycznej w ramach programu Cyber Partnership Program (CPP). CPP wspiera misję ENISA w zakresie wzmacniania odporności Europy na zagrożenia cyfrowe, ułatwiając wymianę informacji o zagrożeniach między ekspertami technicznymi, co z kolei może służyć planowaniu polityk i opracowywaniu ostrzeżeń dla europejskich przedsiębiorstw. ENISA musi dysponować odpowiednimi zasobami i finansowaniem, aby móc kontynuować programy takie jak CPP, nie rezygnując przy tym z realizacji swojej misji w zakresie certyfikacji.

AKT W SPRAWIE DANYCH

W tym rozdziale przedstawiamy rekomendacje zmian upraszczających Akt w sprawie danych.

<table>
<tr><td colspan="2">UPROSZCZENIE #1 - Zawężenie zakresu pojęcia „produktu skomunikowanego”</td></tr>
<tr><td>Proponowana zmiana</td><td>Uzasadnienie</td></tr>
<tr><td>Wyłączenie określonego rodzaju produktów sprzętowych z zakresu zastosowania Aktu w sprawie danych, poprzez zmianę art. 2 pkt 5

5) „produkt skomunikowany” oznacza rzecz, która pozyskuje, generuje lub zbiera dostępne dane dotyczące jej wykorzystywania lub jej otoczenia i która jest w stanie komunikować dane z produktu za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu i której podstawową funkcją nie jest przechowywanie, przetwarzanie ani przesyłanie danych w imieniu strony innej niż użytkownik; nie obejmuje to jednak produktów, które zostały zaprojektowane przede wszystkim w celu wyświetlania lub odtwarzania treści bądź rejestrowania i przesyłania treści, między innymi na potrzeby korzystania z usługi online.

Tego rodzaju produkty obejmują m.in. komputery osobiste, tablety, smartfony i smartwatche.</td><td>● Zmiana zmierza do wyłączenia szeregu produktów z zakresu zastosowania Aktu w sprawie danych, celem zmniejszenia obciążeń związanych z wymogami zgodności dla tych kategorii produktów. Motyw 15 w początkowej propozycji Komisji dotyczącej Aktu w sprawie danych zawierał takie wyłączenie, i na tej podstawie przygotowaliśmy niniejszą propozycję zmiany.
● Celem Aktu w sprawie danych było wzmocnienie unijnej gospodarki opartej na danych oraz wspieranie konkurencyjnego rynku danych poprzez zwiększenie dostępności i użyteczności danych (w szczególności danych przemysłowych), promowanie innowacji opartych na danych oraz zwiększenie dostępności danych. W praktyce jednak szeroki zakres obowiązków wynikających z Aktu w sprawie danych hamuje innowacje, nakładając na podmioty istotne obciążenia związane z koniecznością przestrzegania niejasnych przepisów, które w niektórych przypadkach są sprzeczne z innymi reżimami prawnymi UE (zob. dalej uproszczenie #2). Niniejsza zmiana ma na celu zmniejszenie tego obciążenia poprzez zawężenie zakresu stosowania Aktu w sprawie danych.</td></tr>
<tr><td>Propozycja alternatywna wobec wcześniejszej rekomendacji - wyłączenie smartfonów z zakresu zastosowania Aktu w sprawie danych, poprzez zmianę art. 2 pkt 5

5) „produkt skomunikowany” oznacza rzecz, która pozyskuje, generuje lub zbiera dostępne dane dotyczące jej wykorzystywania lub jej otoczenia i która jest w stanie komunikować dane z produktu</td><td>● Propozycja zmierza do zawężenia definicji produktu skomunikowanego poprzez wyłączenie smartfonów z jej zakresu. Smartfony stanowią kategorię „produktu skomunikowanego”, która może istotnie rozszerzyć zakres stosowania Aktu w sprawie danych ze względu na możliwość kwalifikowania szerokiego wachlarza aplikacji jako „usług powiązanych” ze smartfonem.
● W rezultacie ta prosta zmiana mogłaby</td></tr>
</table>

za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu i której podstawową funkcją nie jest przechowywanie, przetwarzanie ani przesyłanie danych w imieniu strony innej niż użytkownik; nie obejmuje to jednak smartfonów. Nowa definicja smartfona w art. 2 Aktu w sprawie danych: *„smartfon" oznacza telefon komórkowy (w rozumieniu art. 2 ust. 1 rozporządzenia 2023/1670) o następujących cechach:* *a) charakteryzuje się połączeniem z siecią bezprzewodową, możliwością mobilnego korzystania z usług internetowych, systemem operacyjnym zoptymalizowanym do korzystania z urządzenia, gdy jest trzymane w dłoni, oraz zdolnością do przyjmowania oprogramowania oryginalnego i oprogramowania osób trzecich; oraz* *b) jest wyposażony w zintegrowany wyświetlacz z ekranem dotykowym.*	znacząco zmniejszyć obciążenia związane z przestrzeganiem wymogów zgodności dla podmiotów, poprzez doprecyzowanie, że rodzaj „produktów skomunikowanych" i „usług powiązanych", dla których trzeba opracowywać rozwiązania zapewniające zgodność z Aktem w sprawie danych, nie obejmuje smartfonów ani powiązanych z nimi usług (tj. aplikacji).

UPROSZCZENIE #2 - Wyłączenie z zakresu rozdziału II danych wygenerowanych w wyniku korzystania z produktów skomunikowanych lub powiązanych usług przez konsumentów	
Proponowana zmiana	Uzasadnienie
Ukierunkowana poprawka w art. 7 Aktu w sprawie danych zawężająca zakres rozdziału II poprzez wyłączenie danych konsumenckich *ROZDZIAŁ II* *DZIELENIE SIĘ DANYMI PRZEZ PRZEDSIĘBIORCÓW ~~Z KONSUMENTAMI I~~ Z INNYMI PRZEDSIĘBIORCAMI*	• Zmiana ma na celu wyłączenie z zakresu rozdziału II danych wygenerowanych w wyniku korzystania z produktów skomunikowanych i powiązanych usług przez konsumentów. • Skutkiem takiej zmiany byłoby to, że jedynie dane wygenerowane w kontekście B2B w wyniku korzystania z produktów skomunikowanych i usług powiązanych podlegałyby obowiązkom w zakresie przenoszenia danych i udzielania informacji określonym w rozdziale II. Ponadto obowiązek przekazywania informacji

[..] *Artykuł 7* *Zakres obowiązków dzielenia się danymi przez przedsiębiorców ~~z konsumentami i~~ z innymi przedsiębiorcami* *1. Obowiązki przewidziane w niniejszym rozdziale nie mają zastosowania do:* *a) danych wygenerowanych w wyniku korzystania przez konsumentów z produktów skomunikowanych lub z usług powiązanych dostarczonych konsumentom;* *b) danych wygenerowanych w wyniku korzystania z wyprodukowanych lub zaprojektowanych produktów skdaneomunikowanych lub z usług powiązanych dostarczonych przez mikroprzedsiębiorstwo lub małe przedsiębiorstwo, pod warunkiem że przedsiębiorstwo to nie ma przedsiębiorstwa partnerskiego ani przedsiębiorstwa powiązanego w rozumieniu art. 3 załącznika do zalecenia 2003/361/WE, które nie kwalifikuje się jako mikroprzedsiębiorstwo lub małe przedsiębiorstwo, a mikroprzedsiębiorstwo lub małe przedsiębiorstwo nie jest podwykonawcą, któremu zlecono wyprodukowanie lub zaprojektowanie produktu skomunikowanego lub też świadczenie usługi powiązanej.* *wyprodukowanych lub zaprojektowanych produktów skomunikowanych lub z usług powiązanych dostarczonych przez mikroprzedsiębiorstwo lub małe przedsiębiorstwo, pod warunkiem że przedsiębiorstwo to nie ma przedsiębiorstwa partnerskiego ani przedsiębiorstwa powiązanego w rozumieniu art. 3 załącznika do zalecenia 2003/361/WE, które nie kwalifikuje się jako mikroprzedsiębiorstwo lub małe przedsiębiorstwo, a mikroprzedsiębiorstwo lub małe przedsiębiorstwo nie jest podwykonawcą, któremu zlecono wyprodukowanie lub zaprojektowanie produktu skomunikowanego lub też*	przedumownych dotyczyłby wyłącznie relacji B2B. Uzasadnieniem tej zmiany jest fakt, że RODO oraz Akt o rynkach cyfrowych wystarczająco realizują prawo do przenoszenia danych w odniesieniu do konsumenckiego wykorzystania produktów skomunikowanych i usług powiązanych, wobec czego nakładanie na organizacje dodatkowych, pokrywających się obowiązków w ramach Aktu w sprawie danych jest zbędne i nadmiernie obciążające. • To samo dotyczy obowiązków informacyjnych przed zawarciem umowy wynikających z art. 3 ust. 2 i 3, które pokrywają się z RODO i mogą prowadzić do nadmiernego obciążenia konsumentów dodatkowymi (choć bardzo podobnymi) informacjami. Przeciętny użytkownik raczej nie odróżni informacji przekazywanych na podstawie RODO od tych wynikających z Aktu w sprawie danych. • Wreszcie, wyłączenie danych wygenerowanych przez produkty konsumenckie (które w wielu przypadkach będą stanowić dane osobowe) z zakresu obowiązków dotyczących przenoszenia danych w rozdziale II ma na celu ograniczenie ryzyka, jakie ponoszą posiadacze danych w związku z potencjalnym naruszeniem RODO.

świadczenie usługi powiązanej. *~~To samo ma zastosowanie do~~ c) danych wygenerowanych w wyniku korzystania z produktów skomunikowanych wyprodukowanych lub z usług powiązanych dostarczonych przez przedsiębiorstwa, które kwalifikują się jako średnie przedsiębiorstwa zgodnie z art. 2 załącznika do zalecenia 2003/361/WE przez okres krótszy niż rok, oraz do produktów skomunikowanych przez okres jednego roku od dnia wprowadzenia ich do obrotu przez średnie przedsiębiorstwo.* *2. Postanowienie umowne, które ze szkodą dla użytkownika wyklucza stosowanie praw użytkownika przewidzianych w niniejszym rozdziale, stanowi odstępstwo od nich lub zmienia ich skutek, nie jest dla użytkownika wiążące.*	
Propozycja alternatywna wobec wcześniejszej rekomendacji - ukierunkowana poprawka w art. 7 celem wyłączenia danych, które nie są użyteczne dla odbiorcy lub użytkownika *Obowiązki przewidziane w niniejszym rozdziale nie mają zastosowania do:* *a) danych wygenerowanych w wyniku korzystania z produktów skomunikowanych lub z usług powiązanych będących w posiadaniu posiadacza danych w formie nieczytelnej, tak że ich ujawnienie nie przyniosłoby odbiorcy ani użytkownikowi żadnej praktycznej korzyści.*	• Celem tej potencjalnej zmiany jest wprowadzenie wyjątku od obowiązku zapewnienia przenoszalności danych na mocy rozdziału II Aktu w sprawie danych w sytuacjach, gdy dane te są nieczytelne lub nie miałyby dla odbiorcy lub użytkownika żadnej praktycznej korzyści. Obecnie znaczna część danych, które posiadacze danych mogą być zobowiązani udostępniać zgodnie z rozdziałem II, nie będzie zrozumiała lub czytelna dla użytkowników lub odbiorców, a ich przekazanie nie przyniesie im realnej korzyści. Mimo to posiadacze danych muszą ponosić nakłady na opracowanie rozwiązań umożliwiających udostępnienie takich danych. Proponowana zmiana ma na celu ograniczenie obciążeń nakładanych na posiadaczy danych przez ten obowiązek.
Znieść zakaz z art. 5 ust. 3 dla strażników dostępu. *3. Przedsiębiorstwo wskazane jako strażnik dostępu na mocy art. 3 rozporządzenia (UE) 2022/1925 ~~nie kwalifikuje się jako osoba~~*	• Zmiana zmierza do zniesienia całkowitego zakazu dla strażników dostępu, o których mowa w Akt o rynkach cyfrowych, na mocy art. 5 ust. 3 Aktu w sprawie danych. Zakaz ten rodzi poważne wątpliwości prawne ze względu na możliwą sprzeczność z art.

~~*trzecia na mocy niniejszego artykułu, a zatem*~~*:* *a) w żaden sposób nie nakłania ani komercyjnie nie zachęca użytkownika, w tym przez zapewnienie rekompensaty pieniężnej lub jakiejkolwiek innej, do udostępnienia danych, które użytkownik pozyskał na podstawie wniosku złożonego zgodnie z art. 4 ust. 1, na potrzeby jednej ze swoich usług;* *b) nie nakłania ani komercyjnie nie zachęca użytkownika do zwrócenia się do posiadacza danych z wnioskiem o udostępnienie danych na potrzeby jednej ze swoich usług zgodnie z ust. 1 niniejszego artykułu;* ~~*c) nie otrzymuje danych od użytkownika, które użytkownik pozyskał na podstawie wniosku złożonego zgodnie z art. 4 ust. 1.*~~	20 RODO oraz art. 6 ust. 9 i 10 Aktu o rynkach cyfrowych. ● W każdym razie całkowity zakaz jest nieodpowiedni, ponieważ mogą występować sytuacje, w których użytkownicy chcą przekazać dane strażnikowi dostępu. Cele tych przepisów można skutecznie osiągnąć poprzez zakaz nakłaniania przez strażników dostępu do uzyskania takich danych. Zob. także dalsze uwagi przedstawione przez CCIA Komisji Europejskiej oraz EROD.

UPROSZCZENIE #3 - Ograniczenie obowiązków udostępniania danych przez przedsiębiorstwa organom sektora publicznego (B2G) określonych w rozdziale V wyłącznie do danych z produktu i danych z usług powiązanych	
Proponowana zmiana	Uzasadnienie
Artykuł 14 *Obowiązek udostępnienia danych na podstawie wyjątkowej potrzeby* *W przypadku gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii wykażą wyjątkową potrzebę, o której mowa w art. 15, wykorzystania określonych danych z produktu lub z usługi powiązanej – w tym odpowiednich metadanych niezbędnych do interpretacji i wykorzystania tych danych – w celu wykonania swoich ustawowych obowiązków realizowanych w interesie publicznym, posiadacze danych będący osobami prawnymi, którzy posiadają te dane, inni niż organy sektora publicznego, udostępniają je w odpowiedzi na należycie uzasadniony wniosek.* *Artykuł 15* *Wyjątkowa potrzeba wykorzystania danych* *1. Wyjątkowa potrzeba wykorzystania określonych danych z produktu lub z usługi*	● Zmiana zmierza do ograniczenia stosowania obowiązków udostępniania danych w relacji B2G, określonych w rozdziale V, wyłącznie do danych z produktów (zgodnie z definicją w art. 2 pkt 15) oraz danych z usług powiązanych (zgodnie z definicją w art. 2 pkt 16). Zmiana ta ma na celu osiągnięcie dwóch efektów: (i) zapewnienie jasności i pewności co do zakresu wniosków składanych na podstawie rozdziału V oraz (ii) ograniczenie przedmiotu tych wniosków wyłącznie do danych z produktów i danych z usług powiązanych. ● Zmiana ta ma na celu istotne zmniejszenie obciążeń operacyjnych związanych z przyjmowaniem i realizacją takich wniosków, ponieważ systemy i procedury mogłyby zostać wdrożone w dziedzinach dotyczących produktów, co umożliwiłoby usprawnienie całego procesu.

powiązanej w rozumieniu niniejszego rozdziału jest ograniczona w czasie i zakresie i uznaje się, że istnieje wyłącznie w następujących okolicznościach: *a) gdy żądane dane są niezbędne do zareagowania na niebezpieczeństwo publiczne, a organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii nie są w stanie skutecznie i na czas pozyskać takich danych w alternatywny sposób na równoważnych warunkach;* *b) w okolicznościach nieobjętych lit. a) i wyłącznie w przypadku danych nieosobowych, gdy:* *(i) organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii działają na podstawie prawa Unii lub prawa krajowego i zidentyfikowały konkretne dane z produktu lub z usługi powiązanej, których brak uniemożliwia im wykonanie konkretnego zadania realizowanego w interesie publicznym, które jest wyraźnie przewidziane prawem, takiego jak tworzenie statystyki publicznej lub łagodzenie niebezpieczeństwa publicznego lub przywracanie stanu wyjściowego po jego wystąpieniu; oraz* *(ii) organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii wyczerpały wszystkie inne dostępne im sposoby pozyskania takich danych produktu lub z usługi powiązanej, w tym zakup danych nieosobowych na rynku poprzez zaoferowanie stawek rynkowych, powołanie się na istniejące obowiązki udostępniania danych lub poprzez przyjęcie nowych środków ustawodawczych, które mogłyby zagwarantować dostępność danych na czas.* *2. Ust. 1 lit. b) nie ma zastosowania do mikroprzedsiębiorstw ani do małych przedsiębiorstw.* *3. Obowiązek wykazania, że organ sektora publicznego nie był w stanie pozyskać danych nieosobowych poprzez ich zakup na rynku, nie ma zastosowania, w przypadku gdy konkretnym zadaniem realizowanym w interesie publicznym jest tworzenie statystyki publicznej i gdy na zakup danych nie zezwala prawo krajowe.*	

Stworzenie listy jednostek, które mogą kierować wnioski na mocy rozdziału V *Artykuł 2, pkt 27* *„organy Unii” oznaczają organy i jednostki organizacyjne Unii określone przez Komisję zgodnie z art. 23 ust. 1, ustanowione na mocy aktów przyjętych na podstawie Traktatu o Unii Europejskiej, TFUE lub Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej lub zgodnie z nimi;* *Artykuł 2, pkt 28* *„organ sektora publicznego” oznacza organy wyznaczone jako takie przez państwa członkowskie, zgodnie z art. 23 ut. 2, które obejmują organy krajowe, regionalne lub lokalne państw członkowskich oraz podmioty prawa publicznego państw członkowskich lub związki złożone z co najmniej jednego takiego organu lub z co najmniej jednego takiego podmiotu (jeżeli został wyznaczony jako taki przez państwo członkowskie);* *Artykuł 23* *1. Komisja jest odpowiedzialna za wyznaczanie podmiotów jako „organy Unii” w rozumieniu art. 2 pkt 27 oraz za prowadzenie ich wykazu.* *2. Państwa członkowskie są odpowiedzialne za wyznaczanie podmiotów jako „organy sektora publicznego” w rozumieniu art. 2 pkt 28 oraz za prowadzenie ich wykazu.*	• Zmiana ta zmierza do zobowiązania Komisji i państw członkowskich do stworzenia i utrzymywania list jednostek, które mogą kierować wnioski na mocy rozdziału V. • Celem tej zmiany jest zapewnienie przejrzystości oraz zapobieżenie sytuacjom, w których posiadacze danych byliby przytłoczeni wnioskami składanymi przez liczne podmioty niemające prawa do występowania z żądaniami na podstawie rozdziału V.