

Warszawa, 05-03-2025



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

DPNT.401.13.2025.WL.MWR

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU

L.dz. SPS-III.020.12.2025.

Data wpływu 06. 03. 2025

**Pan
Dariusz Salamończyk
Zastępca Szefa
Kancelarii Sejmu RP**

adres ePUAP: /KSRP/SkrytkaESP

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 17 stycznia br., znak: SPS-III.020.12.2025, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych², uprzejmie informuję, że do przedstawionego **obywatelskiego projektu ustawy o ochronie małoletnich przed treściami pornograficznymi w Internecie oraz o zmianie ustawy – Prawo telekomunikacyjne**, dalej jako „projekt”, Prezes Urzędu Ochrony Danych Osobowych jako organ nadzorczy zgłasza następujące uwagi.

I. Uwagi o charakterze ogólnym

Projektowane przepisy mają realizować niezwykle doniosły cel, jakim jest ochrona dobrostanu dzieci i młodzieży, a **kierunek zmian legislacyjnych zaproponowany przez projektodawcę i zmierzający do realizacji tej wartości jest niewątpliwie słuszny i zasługuje na aprobatę**. Osoby najmłodsze są mniej świadome zagrożeń związanych z korzystaniem z usług cyfrowych i często bezbronne wobec takich zagrożeń, co rodzi **potrzebę objęcia tych osób**

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.), dalej: „rozporządzenie 2016/679”.

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

szczególną ochroną. W zasadzie nieograniczony dostęp osób małoletnich do treści pornograficznych w Internecie stanowi poważny problem społeczny i wpływa jednoznacznie negatywnie na zdrowie psychiczne i fizyczne młodzieży, w szczególności ze względu na generowanie uzależnienia od tego typu treści, na co autorzy projektu sami obszernie wskazują w jego uzasadnieniu.

Kwestia ochrony praw dzieci i młodzieży jest szczególnie bliska także Prezesowi UODO, który w swojej działalności wielokrotnie podnosił tematy dotyczące zabezpieczenia praw tych osób, nie tylko w kontekście prawa do ochrony ich danych osobowych. Przykładem takiej działalności są chociażby uwagi do „Strategii Cyfryzacji Polski do 2035 roku”³, w których Prezes UODO wskazał m. in. na potrzebę właściwego edukowania dzieci i młodzieży w zakresie bezpiecznego korzystania z narzędzi cyfrowych. W opinii tej zaapelowałem m.in. o zwiększanie wśród młodzieży świadomości o bezpieczeństwie, prywatności i przysługujących środkach ochrony swoich danych osobowych (zarówno technicznych, organizacyjnych, jak i prawnych). Należy też zwrócić uwagę na liczne kontrole sektorowe planowane przez Prezesa UODO na bieżący rok, które mają mieć za przedmiot m. in. poszanowanie ochrony danych osobowych dzieci. Warto też wspomnieć o tegorocznej edycji Nagrody im. Michała Serzyckiego, w której Prezes UODO wyróżnił m. in. dra Konrada Ciesiołkiewicza⁴ – działacza społecznego propagującego m. in. prawa dziecka, autora licznych publikacji dotyczących tej materii, w szczególności publikacji „Empatyczne instytucje. Prawa dziecka jako prawa człowieka w praktyce organizacji” (2023), w której poruszono także problematykę przemocy seksualnej wobec małoletnich. Wczoraj, tj. 4 marca 2025 r., wziąłem także udział w Sejmie RP w konferencji Komisji ds. Dzieci i Młodzieży, podczas której uczestniczyłem w dyskusji panelowej poświęconej opublikowanemu raportowi „Internet dzieci”, gdzie zagrożenia obecne w Internecie zostały przedstawione na podstawie wiarygodnych empirycznych polskich badań.

Podzielając konieczność rozwiązania problemu przedstawionego przez autorów projektu i uznając kierunek proponowanych rozwiązań za jednoznacznie słuszny wskazać trzeba, że koncepcja ta jest ściśle związana z koniecznością skutecznej weryfikacji wieku oraz wykracza poza zagadnienia jedynie z zakresu przetwarzania danych osobowych. Co więcej, **aby projektowane przepisy skutecznie spełniały cel założony przez projektodawcę, jakim jest ochrona dobrostanu małoletnich, regulacje te powinny być przejrzyste oraz w sposób jasny i precyzyjny określać obowiązki określonych podmiotów związane z weryfikacją wieku** (w tym również w zakresie przetwarzania przez te podmioty danych osobowych), o której mowa w projekcie.

Przede wszystkim należy zwrócić uwagę, że projekt wywiera znaczny wpływ na szeroko pojęte prawa podstawowe, prawa i wolności obywatelskie, w szczególności

³ Pismo Prezesa UODO do Ministra Cyfryzacji, znak DOL.401.502.2024, dostępne na stronie internetowej Urzędu: „Uwagi PUODO do Strategii Cyfryzacji Polski do 2035” (<https://uodo.gov.pl/pl/138/3492>).

⁴ „Nagrody za działania na rzecz ochrony danych przyznane” (<https://uodo.gov.pl/pl/138/3571>).

prawo do prywatności. Przewidziana bowiem przez autorów projektu weryfikacja wieku, a w konsekwencji, konieczność identyfikacji osoby uzyskującej dostęp do określonych treści w Internecie, będzie wiązała się z poważną ingerencją w życie prywatne tej osoby, a także będzie związana z przetwarzaniem jej danych osobowych. Projekt wywiera także wpływ na konstytucyjnie chronioną wolność **słowa, sumienia oraz komunikacji**. Podzielając przekonanie o doniosłości problemu przedstawionego przez autorów projektu wskazać trzeba, że prawo dostępu do rozpowszechnianych w środkach masowego przekazu treści, w tym także treści pornograficznych, mieści się w zakresie wyżej wymienionych praw i wolności, zaś projekt – poprzez ustanowienie ograniczeń w dostępie do określonych treści – stanowi ingerencję w powyższe wolności i prawa. Powyższe prawa i wolności stanowią również prawa podstawowe ustanowione w Karcie Praw Podstawowych Unii Europejskiej (dalej jako: KPP UE), w tym prawo do ochrony danych osobowych, wolność wypowiedzi i informacji czy wolność myśli, sumienia i religii. Z kolei wszelkie ograniczenia w wyżej wymienionych praw i wolności – jak wymaga tego regulacja konstytucyjna – powinny wynikać wyłącznie z aktu rangi ustawy i nie jest dopuszczalne regulowanie tej materii w rozporządzeniu. Jak zostanie wykazane dalej, **projektodawca zasadniczej części regulacji dotyczących powyższych ograniczeń nie zawarł w projekcie ustawy, lecz pozostawił je do uregulowania w akcie niższego rzędu, tj. w akcie wykonawczym do ustawy – rozporządzeniu**. Należy też pamiętać, że ustanawianie ww. ograniczeń powinno odbywać się z poszanowaniem zasady proporcjonalności i konieczności, o której mowa w art. 31 ust. 3 Konstytucji RP oraz w art. 52 ust. 1 KPP UE.

Co więcej, projekt nakłada na dostawców treści pornograficznych „obowiązek stosowania skutecznych systemów weryfikacji wieku odbiorcy w celu uniemożliwienia osobom małoletnim dostępu do takich treści”. Sformułowany w taki sposób obowiązek nie będzie możliwy do realizacji i nie pozwoli na skuteczne osiągnięcie słusznego celu projektu. Projektodawca w żaden sposób nie określa bowiem, co należy rozumieć przez „skuteczne systemy weryfikacji wieku”, na czym miałyby polegać przedmiotowe systemy, jak miałyby one funkcjonować ani jakie kryteria miałyby one spełniać. Ustawodawca nie powinien tymczasem nakładać na podmioty prawa obowiązków sformułowanych na tyle nieostro, że nie jest możliwe określenie na podstawie treści przepisu, w jaki sposób obowiązek ten ma zostać spełniony.

Należy też zwrócić uwagę na brak spójności projektu z obowiązującymi przepisami prawa karnego w zakresie dopuszczalności dostępu do pornografii przez osoby małoletnie. Zgodnie bowiem z art. 200 § 3 Kodeksu karnego⁵, „kto małoletniemu **poniżej lat 15** prezentuje treści pornograficzne lub udostępnia mu przedmioty mające taki charakter albo rozpowszechnia treści pornograficzne w sposób umożliwiający takiemu małoletniemu zapoznanie się z nimi, podlega karze pozbawienia wolności do lat 3”. Z kolei zgodnie z projektem zabronione byłoby udostępnianie treści pornograficznych osobom małoletnim, tj. takim, które nie

⁵ Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2024 r. poz. 17 ze zm.).

ukończyły **18. roku życia**. Prawo karne ustanawia więc niższy niż zaproponowany w projekcie wiek osoby, której prezentowanie treści pornograficznych jest penalizowane. Nie jest jasne, czy powyższa rozbieżność jest przez projektodawcę zamierzona, tj. czy jej celem jest zmiana obowiązującej cezury wieku w tym zakresie. Jeśli tak, zmiana taka być ona odpowiednio przez projektodawcę odpowiednio uzasadniona, a debata w tym zakresie powinna się odbyć w gremium specjalistów z zakresu kodyfikacji.

Na marginesie należy również zauważyć, że wymieniona w tytule projektu ustawa Prawo telekomunikacyjne⁶ została uchylona i nie obowiązuje już w porządku prawnym.

II. Uwagi z zakresu ochrony danych osobowych

Rozwiązania ustanawiane projektowaną ustawą będą wiązać się z przetwarzaniem znacznej ilości danych osobowych na dużą skalę, co wiąże się z ryzykiem naruszenia praw i wolności osób fizycznych. **Powyższe determinuje zasadność przeprowadzenia testu prywatności – projektowania ochrony danych osobowych w procesie tworzenia prawa⁷, w tym przeprowadzenia oceny skutków dla ochrony danych⁸.** Jeżeli dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, projektodawca powinien uwzględnić przy określaniu sposobów przetwarzania ochronę danych w fazie projektowania. Celem takiego testu jest uwzględnienie oceny skutków przewidywanych rozwiązań prawnych dla ochrony danych, w tym przyjęcie przepisów szczegółowych zawierających rozwiązania zapewniające wyczerpującą, przejrzystą, prawidłową, właściwie wpisaną w system prawny regulację zapewniającą stosowanie przepisów o ochronie danych osobowych. Tymczasem z treści

⁶ Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34 ze zm.).

⁷ Art. 25 ust. 1 rozporządzenia 2016/679 stanowi: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą”.

⁸ Zgodnie z art. 35 ust. 1 jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Uzasadnionym jest dokonanie oceny skutków dla ochrony danych – zgodnie z art. 35 ust. 10 rozporządzenia 2016/679 - już w ramach oceny skutków regulacji w związku z przyjmowaniem określonej podstawy prawnej przetwarzania danych, co przy dokonaniu prawidłowej oceny i wypracowaniu przepisów szczególnych uwzględniających stosowanie ogólnego rozporządzenia o ochronie danych może zastąpić dokonywanie takiej oceny przez podmioty stosujące / wykonujące następnie tak ustalone przepisy.

projektowanych przepisów i uzasadnienia projektu nie wynika, aby taka ocena została przeprowadzona przez projektodawcę.

Co więcej, ponieważ projekt nie określa w żaden sposób systemów weryfikacji wieku ani modelu przetwarzania danych osobowych za ich pomocą, nie można wykluczyć, że przetwarzanie to będzie wiązało się z **profilowaniem** użytkowników⁹. Ma to szczególne znaczenie w przypadku, gdyby w celu weryfikacji wieku miałyby być stosowane algorytmy sztucznej inteligencji. Zgodnie bowiem z art. 6 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689¹⁰ systemy sztucznej inteligencji, należące do kategorii określonych w załączniku III do tego rozporządzenia, zawsze uważa się za **systemy AI wysokiego ryzyka**, jeżeli system dokonuje profilowania osób fizycznych. W takim wypadku system ten musi spełniać określone warunki wynikające z rozporządzenia 2024/1689.

Należy wskazać, że 11 lutego 2025 r. Europejska Rada Ochrony Danych (EROD) przyjęła **oświadczenie 1/2025 w sprawie zapewnienia wieku**¹¹. Dokument ten ma na celu znalezienie równowagi między ochroną dzieci a ochroną danych osobowych w kontekście mechanizmów weryfikacji wieku. W oświadczeniu tym zawarto podstawowe zasady ochrony danych, na których powinny opierać się mechanizmy ochrony danych. Priorytetowo potraktowano spełnienie wymogów dotyczących głównych zasad określonych w art. 5 rozporządzenia 2016/679 (zgodność z prawem, rzetelność, przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, ograniczenie przechowywania, poufność, integralność i rozliczalność) oraz zapewnienie, aby te zasady ochrony danych były właściwie wdrażane i pozostawały trwałe, jak określono w art. 25 i art. 32 rozporządzenia 2016/679.

W powyższym oświadczeniu zaznaczono, że dobro dziecka (najlepszy interes dziecka) powinno być kwestią nadrzędną dla wszystkich stron zaangażowanych w zapewnienie wieku (punkt 11). **Z uregulowań projektu ustawy w zakresie mechanizmów weryfikacji wieku nie wynika, aby mechanizmy te opierały się na podobnych założeniach.** Zgodnie z oświadczeniem, „zapewnienie wieku powinno być zawsze wdrażane w sposób oparty na analizie ryzyka. Dostawcy usług powinni przyjąć podejście oparte na analizie ryzyka przy projektowaniu i świadczeniu swoich usług. Należy wykazać konieczność i proporcjonalność stosowania środków

⁹ Zgodnie z art. 4 pkt. 4 rozporządzenia 2016/679 "profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

¹⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. UE z 2024 r. poz. 1689).

¹¹ Zob. https://www.edpb.europa.eu/news/news/2025/edpb-adopts-statement-age-assurance-creates-task-force-ai-enforcement-and-gives_pl

bezpieczeństwa, takich jak zapewnienie wieku, z uwzględnieniem związanego z tym ryzyka" (punkt 12). Projekt ustawy nie przewiduje żadnych wytycznych w tym zakresie.

W oświadczeniu stwierdzono również, że „**zapewnienie wieku powinno wyraźnie osiągnąć poziom skuteczności adekwatny do celu, dla którego jest przeprowadzane.** Środki, za pomocą których przeprowadzane jest zapewnienie wieku, powinny być odpowiednie do osiągnięcia celu przetwarzania. W szczególności skuteczność wszelkich prawnie umocowanych środków zapewnienia wieku należy uznać za warunek wstępny spełnienia zasad konieczności i proporcjonalności". (punkt 21). **Mechanizmy weryfikacji wieku powinny więc być skuteczne.** W projektowanej regulacji stwierdzono, że „systemy weryfikacji wieku odbiorcy uważa się za skuteczne, nawet gdy ich obejście przez osoby małoletnie jest możliwe, jeżeli wymaga to zastosowania przez takie osoby małoletnie nadzwyczajnych środków i działań, których nie można oczekiwać od przeciętnego odbiorcy" (art. 3 ust. 3 projektu ustawy). **Projekt powinien w miarę możliwości dookreślić pojęcie nadzwyczajnych środków.** Ponadto, jak stwierdzono w oświadczeniu EROD, „dostawcy usług i wszelkie osoby trzecie zaangażowane w zapewnianie wieku powinny wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka. Rozporządzenie 2016/679 wymaga, aby zarówno administratorzy, jak i podmioty przetwarzające dysponowali odpowiednimi środkami technicznymi i organizacyjnymi w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka, jakie stwarzają przetwarzane dane osobowe (motyw 83 i art. 32 rozporządzenia 2016/679)".

Przechodząc do szczegółowych uwag dotyczących poszczególnych przepisów projektu, należy w pierwszej kolejności zwrócić uwagę na **art. 3**, który ustanawia obowiązek stosowania przez podmiot udostępniający treści pornograficzne **metod skutecznej weryfikacji wieku** osoby uzyskującej dostęp do tych treści. Zgodnie z **ust. 2 i 3** tego przepisu weryfikacja ta „musi być przeprowadzona w sposób chroniący prywatność użytkowników i zgodny z przepisami o ochronie danych osobowych", a systemy weryfikacji uważa się za skuteczne nawet, gdy ich obejście jest możliwe za pomocą „nadzwyczajnych środków i działań, których nie można oczekiwać od przeciętnego odbiorcy". **Wskazane regulacje mają charakter czysto blankietowy** – ich brzmienie jest lakoniczne i nie stanowi dla wykonawcy normy żadnej wskazówki co do sposobu ochrony prywatności użytkowników, w tym prawa do autonomii informacyjnej jednostki, ani co do tego, jakie środki i działania umożliwiające obejście systemu weryfikacji są wystarczające dla uznania ww. systemów za skuteczne. Z tego powodu pozostawienie powyższych regulacji w proponowanym brzmieniu jest bezprzedmiotowe. Z proponowanych regulacji powinien wynikać sposób, w jaki podmiot stosujący weryfikację wieku ma zapewnić prywatność użytkownika, którego wiek jest weryfikowany, oraz powinna ona określać,

co należy rozumieć przez „nadzwyczajne środki i działania, których nie można oczekiwać od przeciętnego odbiorcy”, o których mowa w projektowanym art. 3 ust. 3.

Jak wynika z kolei z **ust. 4 art. 3 projektu, szczegółowe kryteria, jakim powinny odpowiadać skuteczne systemy weryfikacji zostaną określone, w drodze rozporządzenia**, przez ministra właściwego ds. informatyzacji, w porozumieniu z Prezesem Urzędu Komunikacji Elektronicznej i **po zaopiniowaniu przez Prezesa UODO oraz z zapewnieniem odpowiedniego poziomu ochrony danych osobowych i prywatności**. Projektodawca, wbrew zasadom konstytucyjnym, nie określił więc w żaden sposób, na czym miałyby polegać skuteczna weryfikacja wieku osoby uzyskującej dostęp do treści pornograficznych i pozostawił tę kwestię do uregulowania w rozporządzeniu. W szczególności nie jest jasne, co w zamyśle projektodawcy oznacza „odpowiedni poziom ochrony danych osobowych i prywatności”. Co więcej, z projektowanej delegacji do wydania ww. rozporządzenia wynika, że akt ten nie miałby określać samego sposobu weryfikacji wieku, lecz jedynie szczątkowo dotyka problemu i odnosi się tylko do ustalania kryteriów, jakim mają odpowiadać ww. systemy, które następnie byłyby opracowywane i wdrażane przez dostawców treści pornograficznych. W związku z tym nie są spełnione wymagania określone w art. 92 ust. 1 Konstytucji RP, który określa, że „Rozporządzenia są wydawane przez organy wskazane w Konstytucji, na podstawie **szczegółowego upoważnienia** zawartego w ustawie i w celu jej wykonania. Upoważnienie powinno określać organ właściwy do wydania rozporządzenia i **zakres spraw** przekazanych do uregulowania oraz **wytyczne dotyczące treści aktu**”.

Powyższa regulacja **nie jest do przyjęcia jednak przede wszystkim z punktu widzenia przepisów rozporządzenia 2016/679 oraz konstytucyjnych zasad systemu prawa**. Weryfikacja wieku na podstawie projektowanych przepisów stanowić będzie poważną ingerencję w konstytucyjne prawa i wolności człowieka i obywatela, w szczególności w prawo do prywatności, jak i w prawo do ochrony danych osobowych. Dlatego **regulacje dotyczące przedmiotowej materii jak wprowadzające prawa i obowiązki powinny wynikać bezpośrednio z aktu rangi ustawy**, a nie rozporządzenia wydanego na jej podstawie (zob. art. 47 i 51 Konstytucji RP w zw. z art. 31 ust. 3 Konstytucji RP, a także art. 7 i 8 KPP UE w zw. z art. 52 ust. 1 KPP). Z powyższych względów nie jest także dopuszczalne, aby sposób weryfikacji wieku użytkownika był ustalany przez podmiot udostępniający treści objęte ograniczeniem wiekowym. Projektodawca nie powinien ograniczać się tylko do wskazania na niezbędne kryteria, jakie miałyby spełniać przedmiotowe systemy, **konieczne jest określenie w przepisach o odpowiedniej randze (ustawy) co najmniej podstawowych założeń, na których miałyby się opierać systemy weryfikujące wiek użytkownika**.

Co więcej, ze względu na wyżej opisaną poważną ingerencję w prywatność osoby fizycznej i w jej autonomię informacyjną, **regulacje zawarte w projekcie powinny odnosić się wprost także do kwestii przetwarzania danych osobowych**

w przedmiotowych systemach weryfikacji wieku. W szczególności nie jest jasne, czy powyższe systemy miałyby służyć wyłącznie weryfikacji wieku, czy też dane osobowe gromadzone w tych systemach miałyby być przetwarzane także w innych celach, niewyrażonych w projektowanej ustawie. Dlatego konieczne jest dookreślenie w projektowanych przepisach precyzyjnych **celów**, w których dane osobowe gromadzone w powyższych systemach będą przetwarzane. Ponadto, z przedstawionego projektu nie wynika w żaden sposób, jakich miałyby być zakres przetwarzanych danych, jakie podmioty będą przetwarzać dane osobowe gromadzone w systemach i kto będzie miał do nich dostęp, w jaki sposób dane będą przetwarzane, jaki jest okres przechowywania tych danych osobowych, jakie są gwarancje bezpieczeństwa dla tych danych i przetwarzania ich w celach innych niż „weryfikacja wieku”.

W ocenie Prezesa UODO uwzględnienie powyższych elementów jest niezbędne z punktu widzenia poszanowania zasad ochrony danych osobowych określonych w art. 5 rozporządzenia 2016/679¹². Pamiętać należy, że przetwarzanie danych osobowych związane z weryfikacją wieku na podstawie projektowanych przepisów będzie znajdowało podstawę w przesłance określonej w art. 6 ust. 1 lit. c rozporządzenia 2016/679. **Z tego względu przepisy ustanawiające systemy weryfikacji wieku i regulujące przetwarzanie w nich danych osobowych**

¹² „1. Dane osobowe muszą być:

- a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
 - b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
 - c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
 - d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
 - e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
 - f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).
2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).”

powinny uwzględniać elementy regulacji krajowej, wymienione w art. 6 ust. 3 rozporządzenia 2016/679¹³.

Powyższe ma tym większe znaczenie ze względu na prawdopodobne przetwarzanie w przedmiotowych systemach tzw. danych sensytywnych, wymienionych w art. 9 ust. 1 rozporządzenia 2016/679¹⁴, tj. danych dotyczących seksualności lub orientacji seksualnej osoby fizycznej. Co do zasady istnieje zakaz przetwarzania wspomnianych kategorii danych osobowych, o ile nie następuje w sytuacjach wyjątkowych, stosownie do regulacji art. 9 ust. 2 rozporządzenia 2016/679. Szczególne kategorie danych osobowych zostały poddane szczególnemu reżimowi ochrony prawnej, a zwłaszcza podstawa do ich ewentualnego przetwarzania powinna wynikać z przepisów rangi ustawy, a nie aktu niższego rzędu w postaci aktów wykonawczych do ustawy. Co więcej, przetwarzanie tych kategorii danych wiąże się z istotną ingerencją w prywatność i autonomię informacyjną jednostki i rozważyć należy wnikliwie, czy przetwarzanie tych danych jest niezbędne do założonego w projekcie celu, jakim jest skuteczna weryfikacja wieku osoby fizycznej. Z tego względu, w ocenie organu nadzorczego, tym bardziej konieczne jest **przejrzyste i rzetelne oraz wyczerpujące uregulowanie w projekcie ww. aspektów przetwarzania danych osobowych, w tym w przedmiotowych systemach, w celu zabezpieczenia praw i wolności osób, których dane dotyczą.** Powyższe pozwoli zapewnić zgodność projektu z ww. zasadami wyrażonymi w art. 5 rozporządzenia 2016/679, w szczególności z zasadami zgodności z prawem, rzetelności i przejrzystości oraz zasadą rozliczalności, zapewniając realizację celu projektu. Z kolei gdyby w systemach weryfikacji wieku nie miały być przetwarzane dane sensytywne, zasadne jest wskazanie w projekcie, tj. w przepisach rangi ustawy, że w systemach weryfikacji wieku, o których mowa w art. 3, zakazane jest

¹³ „Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:

a) w prawie Unii; lub

b) w prawie państwa członkowskiego, któremu podlega administrator.

Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) - musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.”

¹⁴ „Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby”. Wyjątki od tego zakazu zostały określone w art. 9 ust. 2 rozporządzenia 2016/679.

przetwarzanie danych osobowych należących do kategorii wymienionych w art. 9 ust. 1 rozporządzenia 2016/679, dla celów powyższej weryfikacji wieku użytkownika.

W kontekście powyższych systemów weryfikacji wieku **należy też zwrócić uwagę na przepisy Aktu o usługach cyfrowych**¹⁵, którym mogą podlegać podmioty mające zostać objęte przepisami projektowanej ustawy. Szczególną uwagę należy poświęcić relacji z art. 28 Aktu, który wymaga od dostawców platform internetowych dostępnych dla małoletnich wprowadzania odpowiednich i proporcjonalnych środków, aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług. Niezależnie od przedstawionych jak dotąd uwag wskazać należy, że akty wykonawcze (rozporządzenia), które miałyby zostać wydane na podstawie przepisów projektu, również musiałyby być zgodne z przepisami ww. Aktu o usługach cyfrowych. Projekt wydaje się pomijać także przepisy **dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1808**¹⁶, w szczególności art. 6a oraz art. 28b, które stanowią o obowiązku stosowania odpowiednich środków w celu zapewnienia, by audiowizualne usługi medialne świadczone przez dostawców usług medialnych, które mogą zaszkodzić fizycznemu, psychicznemu lub moralnemu rozwojowi małoletnich, były udostępniane jedynie w taki sposób, by małoletni w zwykłych okolicznościach nie mogli ich słuchać ani oglądać. Wdrożenie przepisów dyrektywy nie może kończyć się wyłącznie na przeniesieniu obowiązku ustalenia, co jest „odpowiednie” na dostawców usług. **To ustawodawca powinien określić podstawowe warunki, jakie dany system powinien spełniać.**

Warto również wskazać, że problematyka ochrony danych osobowych użytkownika w Internecie (w tym danych sensytywnych), z którą bezpośrednio wiąże się regulacje przewidziane w projekcie, była przedmiotem **orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej**. W wyroku z 4 października 2024 r. w sprawie C-446/21 Schrems (EU:C:2024:834) Trybunał rozstrzygnął, że operator platformy internetowej sieci społecznościowej nie jest uprawniony do przetwarzania innych danych dotyczących orientacji seksualnej tej osoby, pozyskanych poza tą platformą za pośrednictwem aplikacji i stron internetowych podmiotów zewnętrznych w celu ich agregacji i analizy służących oferowaniu tej osobie zindywidualizowanej reklamy. W wyroku podkreślono też, że „art. 25 ust. 2 tego rozporządzenia [rozporządzenia 2016/679] wymaga od administratora podjęcia odpowiednich środków w celu zapewnienia, by domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Zgodnie z tym przepisem obowiązek ten odnosi się do ilości zbieranych danych osobowych,

¹⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. Urz. UE L 277 z 2022 r., str. 1 ze zm.).

¹⁶ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1808 z dnia 14 listopada 2018 r. zmieniająca dyrektywę 2010/13/UE w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) ze względu na zmianę sytuacji na rynku (Dz. Urz. UE L 303 z 2018 r., str. 69).

zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności”. Z kolei w wyroku z 24 września 2019 r. w sprawie C-136/17 G.C. i in. przeciwko CNIL (EU:C:2019:773) Trybunał orzekł, że operator wyszukiwarki jest co do zasady zobowiązany uwzględniać żądania usunięcia linków prowadzących do stron internetowych zawierających dane osobowe należące do szczególnych kategorii danych.

Należy także zwrócić uwagę na **art. 4 ust. 2 projektu**, zgodnie z którym do zadań Prezesa UKE należałoby m. in. sprawowanie kontroli nad przestrzeganiem przepisów ustawy oraz badanie skuteczności mechanizmów weryfikujących pełnoletniość użytkownika i ich kontrola pod względem zgodności z kryteriami, o których mowa w art. 3 ust. 4, tj. m. in. pod względem ochrony danych osobowych. Takie sformułowanie zadań Prezesa UKE sugeruje, że organ ten miałby sprawować powyższą kontrolę także w przedmiocie przetwarzania danych osobowych, co **godziłoby w kompetencje Prezesa UODO jako organu wyłącznie właściwego ds. ochrony danych osobowych na podstawie rozporządzenia 2016/679**. Projektodawca nie powinien ustanawiać przepisów przewidujących wykonywanie przez inne organy zadań przypisanych jako wyłączne Prezesowi UODO.

Należy także zwrócić uwagę na **art. 7 ust. 3 i 5 projektu**, zgodnie z którymi każdy może dokonać **zgłoszenia domeny internetowej podlegającej wpisowi do rejestru**, o którym mowa w art. 6 projektu, a sposób dokonania zgłoszenia ma zostać określony w informacji udostępnionej na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej. Z treści tych przepisów można wywnioskować, że ww. informacja będzie regulować także zakres danych osobowych zgłaszającego witrynę oraz środek komunikacji, za pomocą którego dokonuje się zgłoszenia. Jeżeli w związku przedmiotowym zgłoszeniem konieczne będzie wskazanie danych identyfikujących zgłaszającego, w ocenie organu nadzorczego **zakres tych danych nie powinien wynikać z informacji publikowanej przez organ, lecz z przepisów projektowanej ustawy**. Informacja wymieniona w art. 7 ust. 5 projektu nie stanowi bowiem źródła powszechnie obowiązującego prawa, a podstawa prawna do przetwarzania danych osobowych przez organ publiczny w celu realizacji zadania ustawowego powinna wynikać z ustawy. Z kolei jeżeli w zamyśle projektodawcy powyższe zgłoszenie będzie dokonywane w sposób anonimowy, fakt ten powinien wynikać wprost z projektowanej regulacji. Pozwoli to zapewnić zgodność projektowanych przepisów z zasadami zgodności z prawem, rzetelności i przejrzystości oraz minimalizacji danych, wynikającymi z rozporządzenia 2016/679, a także z art. 6 ust. 3 tego rozporządzenia.

Na uwagę zasługuje również **art. 9 ust. 1 projektu** nakładający na przedsiębiorcę komunikacyjnego, świadczącego usługi dostępu do Internetu, obowiązek nieodpłatnego uniemożliwiania dostępu do stron internetowych wpisanych do rejestru, o którym mowa w art. 6. **Blokowanie dostępu do powyższych witryn i przekierowywanie użytkownika do strony internetowej prowadzonej przez Prezesa UKE może wiązać się z przetwarzaniem danych osobowych**

użytkownika próbującego uzyskać dostęp do witryny wpisanej do rejestru, co stanowi ingerencję w prywatność osoby fizycznej. Prezes UKE będzie mógł bowiem potencjalnie pozyskiwać informacje o osobie próbującej uzyskać dostęp do strony internetowej udostępniającej treści pornograficzne. Ponadto nie jest jasne, czy administratorem tych danych osobowych miałby być dostawca witryny wpisanej do rejestru, przedsiębiorca komunikacyjny blokujący dostęp do tej witryny czy też Prezes UKE. Zgodnie z zasadą rozliczalności to na administratorze spoczywa obowiązek wykazania zgodności przetwarzania z prawem oraz zapewnienia bezpieczeństwa przetwarzanych danych. W celu zapewnienia zgodności projektowanego mechanizmu z zasadami ochrony danych osobowych niezbędne jest uwzględnienie w projektowanym przepisie ww. elementów regulacji krajowej, o których mowa w art. 6 ust. 3 rozporządzenia 2016/679, tj. w szczególności wykazanie zasadności celu takiego przetwarzania danych oraz proporcjonalności przetwarzania do wyznaczonego, prawnie uzasadnionego celu.

Aby zapewnić zgodność projektowanych przepisów z unijnym prawem ochrony danych należałoby uwzględnić również wskazówki wynikające z Wytycznych EROD nr 4/2019 dotyczących artykułu 25 rozporządzenia 2016/679 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych” (Wersja 2.0, wytyczne przyjęte 20 października 2020 r.)¹⁷ oraz Wytycznych „Ocena skutków dla ochrony danych Przetwarzanie danych osobowych, z którym wiąże się wysokie ryzyko”, WP248 rev.01, przyjętych 4 października 2017 roku¹⁸. Pomocne okazać się mogą również Wytyczne Europejskiego Inspektora Ochrony Danych w sprawie oceny proporcjonalności środków ograniczających podstawowe prawa do prywatności i ochrony danych osobowych¹⁹.

Jednocześnie pragnę podkreślić, że uwagi organu ochrony danych przedstawiane w toku prac legislacyjnych mają charakter wskazówek dla projektodawcy. To jednak projektodawca (a ostatecznie ustawodawca) podejmuje decyzję co do ostatecznego kształtu przyjmowanych przepisów i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych. Wyrażam zarazem nadzieję, że uwzględnienie powyższych uwag będzie pomocne w tym procesie i przyczyni się do skutecznej realizacji założonego celu ochrony małoletnich, przy jednoczesnym poszanowaniu prawa do ochrony danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu

¹⁷ https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

¹⁸ https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_pl

¹⁹ https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en

Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

Urząd Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

tel. 22 531-03-88
fax 22 531-03-99
www.uodo.gov.pl