**PREZES**
**URZĘDU OCHRONY**
**DANYCH OSOBOWYCH**

**Mirosław Wróblewski**

Warszawa, 17 kwietnia 2026 r.

**sygn. DEI.730.1.2025**

**Pani**
**Barbara Nowacka**
**Minister Edukacji Narodowej**

*Szanowna Pani Minister,*

jako Prezes Urzędu Ochrony Danych Osobowych, realizujący zadania wynikające z rozporządzenia Parlamentu Europejskiego i Rady 2026/679 (RODO) oraz ustawy o ochronie danych osobowych, których przepisy podkreślają konieczność szczególnej ochrony prawnej najmłodszych członków społeczeństwa, pragnę wyrazić pełną aprobatę dla decyzji Pani Minister dotyczącej obowiązkowego nauczania przedmiotu *edukacja zdrowotna* w klasach IV-VIII szkoły podstawowej oraz przez dwa lata w szkołach ponadpodstawowych, począwszy od roku szkolnego 2026/2027. **Obecny kierunek działań Ministerstwa Edukacji Narodowej w tym obszarze nie tylko odpowiada na realne potrzeby młodych ludzi, ale stanowi jeden z kluczowych elementów systemowej ochrony ich zdrowia (fizycznego, psychicznego i społecznego), prywatności i praw podstawowych.**

Jestem pełen uznania dla determinacji Pani Minister w dążeniu do skutecznej realizacji tego trudnego zadania. Pani wytrwałość, zaangażowanie i wiara w słuszność obranego kierunku polityki edukacyjnej, niewątpliwie złożyły się na sukces tego przedsięwzięcia – za co jeszcze raz bardzo Pani Minister dziękuję.

Informacje dotyczące ochrony danych osobowych obecne są już w programach przedmiotów, takich jak informatyka, etyka, edukacja obywatelska czy edukacja zdrowotna. **Niemniej jednak chciałbym zwrócić uwagę na konieczność ich rozwinięcia i większego wyeksponowania, przede wszystkim z uwagi na gwałtownie zwiększającą się liczbę negatywnych zjawisk w sieci.** Dzieci nie mają świadomości zagrożeń cyfrowych, zwykle łatwo i bez głębszej refleksji podają dane w grach online, klikają w podejrzane linki, instalują złośliwe aplikacje, udostępniają zdjęcia i dane osobowe obcym osobom. Na dane dziecka tworzone są fałszywe profile wykorzystywane do oszustw, rozsyłania phishingu, cyberprzemocy, co może prowadzić do konsekwencji prawnych i reputacyjnych. Dzieci często

bywają celem **ataków phishingowych**. Bywa, że nieświadome dziecko podaje login i hasło na fałszywej stronie, traci dostęp do konta, albo na skutek działania dziecka przestępca uzyskuje dostęp do danych i zapisanej karty płatniczej rodzica. Dzieci i młodzież mają też niekiedy trudności z odróżnieniem reklam od wiadomości, fikcji od informacji i często nie radzą sobie z właściwą oceną w odniesieniu do treści pojawiających się w mediach społecznościowych i na platformach cyfrowych. Sprzyja temu zjawisku popularna obecnie technologia **deepfake**, umożliwiająca tworzenie fałszywych obrazów, dźwięków, filmów, które mogą negatywnie wpływać na zachowania zarówno indywidualnych odbiorców, jak i grup społecznych. Sprawa zamieszczenia w internecie zdjęcia nagiej uczennicy wygenerowanego z użyciem narzędzi sztucznej inteligencji (AI) przez jej szkolnych kolegów, czy zamieszczenie zdjęcia nagiej nauczycielki pod jej postem w mediach społecznościowych – które to sprawy zostały przeze mnie zgłoszone do prokuratury – są wymownym przykładem, jak w niewłaściwych rękach technologia ta może być niebezpieczna. Stąd potrzeba zwrócenia szczególnej uwagi na ochronę danych osobowych podczas korzystania z tego narzędzia.

Niebezpiecznym zjawiskiem jest również **kradzież tożsamości dzieci** (*child identity theft*) – rosnący i szczególnie niebezpieczny rodzaj przestępstwa cyfrowego. Dzieci nie monitorują swojej historii ani aktywności finansowej, dlatego przestępstwo może pozostać niewykryte nawet przez wiele lat. Skutkami kradzieży tożsamości dziecka może być stres i trauma psychologiczna, długotrwałe postępowania wyjaśniające, ryzyko dalszej wiktymizacji, utrata reputacji oraz problemy finansowe po osiągnięciu pełnoletności.

W tym miejscu chciałem też przytoczyć dane z raportu na temat monitoringu aktywności dzieci w środowisku cyfrowym pn. „Internet Dzieci", przedstawione na posiedzeniu sejmowej Komisji do Spraw Dzieci i Młodzieży (DIM) w dniu 6 listopada 2025 r. W raporcie tym odnotowana jest niepokojąca stała obecność dzieci w świecie cyfrowym, jeszcze przed ukończeniem przez nie 13. roku życia – 1 mln 400 tys. dzieci w Polsce.

Spośród ponad 2 mln dzieci w wieku 7-12 lat w naszym kraju, prawie 800 tys. korzysta z TikToka, ponad 500 tys. z Facebooka, 400 tys. z Instagrama, ponad 700 tys. z Messengera i tyle samo z WhatsAppa.

Podsumowując te informacje – ponad 1mln 400 tys. dzieci w wielu 7-12 lat jest aktywna w sieci. Co również niepokojące – ponad 930 tys. badanych dzieci w wielu 7-14 lat przynajmniej 1 raz odwiedziło serwis pornograficzny.

W świetle powyższych przykładów, wprowadzenie obowiązkowego przedmiotu *edukacja zdrowotna* stwarza okazję do tego, aby treści związane z ochroną danych osobowych zostały wyraźnie wyeksponowane i by stanowiły w programie nauczania punkt wyjściowy do omawiania kolejnych, równie ważnych zagadnień. Trwałe i systemowe uwzględnianie w procesie edukacyjnym zagadnień ochrony danych osobowych i prawa do prywatności, w kontekście bezpieczeństwa psychicznego dzieci i młodzieży jest ogromnie ważne i należy je postrzegać jako element prewencji systemowej, ukierunkowanej na zapobieganie naruszeniom praw dzieci jeszcze przed ich wystąpieniem, a nie tylko jako reakcję następczą na zaistniałe nieprawidłowości.

W tym miejscu chciałbym z całą mocą podkreślić, że planowane lub już przyjęte w innych krajach rozwiązania w zakresie doskonalenia procesu edukacji dzieci i młodzieży,

współgrają z założeniami **Reformy26. Kompas Jutra**, przygotowanej przez MEN, co w świetle odnotowanych światowych trendów świadczy o wyborze przez Panią Minister właściwego kierunku zmian programowych w polskim szkolnictwie. Ponadto wzmacnia argumentację Pani resortu co do konieczności zapewnienia kompleksowej obowiązkowej edukacji dla wszystkich szkół podstawowych i średnich.

Dla przykładu, w **USA,** stan Kalifornia w 2023 r. wprowadził do Kodeksu Edukacyjnego Kalifornii (ang. *California Education Code)* – regulującego kwestie obowiązkowych programów nauczania na wszystkich poziomach edukacji – obowiązkowy przedmiot ***edukacja medialna***, a w jego ramach kompetencje: „obywatelstwo cyfrowe", które ma wspierać młodych ludzi w zetknięciu z nowymi technologiami. Edukacja medialna ma budować umiejętność krytycznego myślenia i analizowania treści przekazów medialnych, budując strategie wspierające dzieci i młodzież we właściwym ich odbiorze.
(źródło:https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB873).

Stan Kalifornia pracuje nad kolejnym projektem ustawy, która dotyczyć będzie *cyfrowego zdrowia* i planowanego rozszerzenia zajęć z zakresu dobrostanu cyfrowego w kalifornijskich szkołach publicznych.
(źródło: https://calmatters.digitaldemocracy.org/bills/ca_202520260ab2071).

Z kolei **Australia** opracowała krajowe ramy i curriculum dla bezpiecznej edukacji online. „Online safety" promuje podejście obejmujące całą szkołę (*whole-school*), gdzie w ramach różnych przedmiotów uczy się bezpiecznego korzystania z sieci i krytycznego podejścia do treści cyfrowych.
(źródło: https://www.esafety.gov.au/educators/best-practice-framework).

W **Irlandii** obowiązuje ustawa z 2022 r. o bezpieczeństwie online i regulacji mediów, która wraz z programem nauczania o nazwie SPHE (*Social Personal and Health Education*), a także Junior Cycle SPHE, kładzie duży nacisk na edukację dzieci i młodzieży w zakresie bezpiecznego poruszania się w sieci. Podobnie jak w Australii – „Online safety" jest w pełni włączone do programu szkolnego.
(źródło:https://www.gov.ie/en/department-of-culture-communications-and-sport/publications/online-safety-and-media-regulation-act-2022/).

**Portugalia,** w ramach *edukacji medialnej* i *edukacji obywatelskiej* zapewniła uczniom bezpieczne korzystanie z sieci i nowych mediów od przedszkola po szkołę średnią. Edukacja medialna jest integralną częścią edukacji obywatelskiej, realizowanej w ramach programu „Citizenship and Development".
(źródło: https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/portugal/68-media-literacy-and-safe-use-of-new-media).

Podkreślenia wymaga, że edukacja medialna obejmuje nie tylko techniczne umiejętności obsługi narzędzi cyfrowych, ale przede wszystkim analizę, ocenę i tworzenie przekazów medialnych, a także odporność na dezinformację.

W oparciu o ustawę o bezpieczeństwie w Internecie z 2023 r. szkoły w **Wielkiej Brytanii** prowadzą nauczanie o bezpieczeństwie w sieci w ramach programu *edukacja zdrowotna, informatyka, edukacja obywatelska* (*health education, computing* i *citizenship*). W systemie edukacji w Wielkiej Brytanii te trzy terminy występują razem w kontekście

nowoczesnych programów nauczania, gdzie edukacja zdrowotna oznacza dbanie o zdrowie fizyczne i psychiczne, informatyka – rozwijanie umiejętności cyfrowych, programowanie i bezpieczeństwo w sieci, natomiast edukacja obywatelska – to wiedza o prawach i obowiązkach, zaangażowanie w społeczność, cyfrowe obywatelstwo.
(źródło: https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools).

Na uwagę zasługuje także stanowisko Komitetu Praw Dziecka ONZ – organu monitorującego wdrażanie Konwencji o prawach dziecka przez państwa będące jej stronami – który w zaleceniach wydanych 4 marca 2025 r. wzywa Polskę do wzmożonej ochrony praw dzieci w środowisku cyfrowym. ONZ rekomenduje, by umiejętności cyfrowe były nauczane przez cały okres edukacji, od przedszkola do końca szkoły, z naciskiem na ryzyka, treści i odpowiedzialne korzystanie z narzędzi cyfrowych.
(źródło: https://www.right-to-education.org/ar/node/1339).

W świetle opisanych przykładów zagrożeń dla bezpieczeństwa dzieci i młodzieży w cyfrowym świecie, jestem głęboko przekonany, że **edukacja zdrowotna jako przedmiot obowiązkowy stwarza wyjątkową okazję do wzmocnienia świadomości młodych ludzi w zakresie prawa do prywatności, bezpiecznego funkcjonowania w sieci oraz ochrony danych osobowych, w tym danych szczególnej kategorii, jakimi są dane dotyczące zdrowia fizycznego i psychicznego.**

Warto też zauważyć, że na poziomie europejskim rozwijane są inicjatywy, takie jak wprowadzenie Europejskiej Przestrzeń Danych dotyczących Zdrowia (EHDS), które w przyszłości pozwolą każdemu z nas aktywnie zarządzać swoimi danymi dotyczącymi zdrowia. Aby uczniowie mogli w pełni korzystać z tych rozwiązań, muszą już dziś zdobywać wiedzę o ochronie danych i prawie do prywatności.

Edukacja zdrowotna jest ważnym elementem wzmacniającym odporność uczniów na zagrożenia cyfrowe. Wprowadzenie edukacji zdrowotnej jako obowiązkowego przedmiotu to ważny krok na drodze realizacji podstawowych celów edukacyjnych i wychowawczych szkoły, który służy ochronie praw uczniów, ich bezpieczeństwu oraz dobrostanu fizycznego, psychicznego i społecznego w środowisku, w którym nowe technologie odgrywają coraz większą rolę.

Uwzględniając znaczenie zagadnień ochrony danych osobowych i prawa do prywatności dla przedstawionych w niniejszym piśmie zagadnień, deklaruję swoją gotowość do współpracy i pełne wsparcie przy doskonaleniu rozwiązań edukacyjnych, które w sposób trwały i proporcjonalny wzmacniają ochronę prywatności i danych osobowych dzieci i młodzieży w środowisku cyfrowym.

Łączę wyrazy szacunku
Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

Do wiadomości:

**Pani Monika Rosa**
**Przewodnicząca Komisji**
**ds. Dzieci i Młodzieży**
**Sejm RP**

**Pan Krzysztof Gawkowski**
**Wiceprezes Rady Ministrów**
**Minister Cyfryzacji**