PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa,

DOL.401.502.2024.

Pan
Dariusz Standerski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

w związku ze skierowaniem do konsultacji społecznych projektu „**Strategii Cyfryzacji Polski do 2035 roku**" (dalej jako „Strategia") **Prezes Urzędu Ochrony Danych Osobowych** – realizując zadania nadane mu jako organowi nadzorczemu przez art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] (rozporządzenie ogólne) – niniejszym pismem zgłasza **uwagi do dokumentu**.

W pierwszej kolejności Prezes UODO chciałby wyrazić swoje podziękowania za sformułowanie kompleksowej wizji rozwoju cyfryzacji Polski, jaką zawarto w omawianym projekcie. Organ nadzorczy za materię fundamentalną uznaje uregulowanie kwestii związanych z tak istotnym aspektem społecznym i prawnym jak rozwój nowych technologii, a także inicjatywę do wykorzystania potencjału korzyści jakie technologie te mogą przynieść społeczeństwu. Koncepcja przyjęta w projekcie pozostaje w spójności z ideami towarzyszącymi aktualnym europejskim planom transformacji cyfrowej, która to na przestrzeni ostatnich lat stała się jednym z głównych priorytetów Unii Europejskiej, czego przykładem jest trwający już od lat Program Cyfrowa Europa, czy też Program Cyfrowa Dekada Europy.

[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 jako: rozporządzenie ogólne.

Udostępnienie projektu w drodze konsultacji społecznych pozwala na zaangażowanie w proces opracowywania Strategii samych obywateli, którzy staną się w przyszłości dysponentami planowanych rozwiązań. Istotne jest urzeczywistnianie konstytucyjnej zasady społeczeństwa obywatelskiego, uznawanie podmiotowości obywateli w procesach przemian prawno-społecznych oraz poszerzanie źródeł do czerpania nowych, wartościowych propozycji rozwiązań oraz merytorycznych opinii do Strategii, które mogą przynieść pozytywne rezultaty dla wdrażania i realizacji jej założeń.

Wskazując na pozytywne aspekty opracowania projektu Strategii, które pragnę bardzo docenić, należy jednocześnie zauważyć, że **w dokumencie nie uwzględniono w dostatecznym stopniu materii ochrony danych osobowych**. **W celu wzmocnienia projektu w tym aspekcie, Prezes Urzędu Ochrony Danych Osobowych**, działając z urzędu, uprzejmie **zgłasza swoją opinię do Strategii**, która ma na celu zaprezentowanie zaleceń związanych z ochroną danych osobowych.

I. Uwagi ogólne.

Rozwój nowych technologii stwarza szereg szans dla zrównoważonego rozwoju państwa i jego obywateli, ale również wyzwań związanych z ich zastosowaniem. Wdrożeniu rozwiązań technologicznych powinny towarzyszyć stosowne rozwiązania prawne gwarantujące wymagany poziom poszanowania praw podstawowych, w tym konstytucyjnego prawa do prywatności oraz ochrony danych osobowych. W tym wymiarze prawa te nie mogą być traktowane jako temat poboczny czy dodatkowy. Przeciwnie, wprowadzenie rozwiązań technicznych, organizacyjnych a przede wszystkim prawnych, czyniących zadość zarówno zasadom rozporządzenia ogólnego, jak i normom Konstytucji RP (art. 47 i ar.t 51 Konstytucji RP) ma znaczenie zasadnicze i fundamentalne dla prawidłowego funkcjonowania technologii cyfrowych w społeczeństwie demokratycznym. Priorytetem powinien być człowiek, a nie technologia czy narzędzia, które wobec człowieka, jego godności, praw, autonomii, ale i szeroko pojmowanego dobrobytu powinny mieć zawszę rolę służebną. Rozwiązania technologiczne powinny być dostosowane do wymogów związanych z koniecznością zapewnienia gwarancji i wolności jednostki – nie na odwrót. Zastosowanie rozwiązań technologicznych winno być czynione roztropnie, poprzez wyważenie czynników związanych z rozwojem społeczeństwa z zachowaniem zasad demokratycznego państwa prawa. Wdrażanie konkretnych rozwiązań prawodawczych **w każdym przypadku poprzedzone powinno zostać rozważną, wszechstronną i dogłębną analizą mającą na celu wykazanie ich niezbędności i proporcjonalności, a zatem przede wszystkim oceną czy nie jest możliwe osiągnięcie tych samych**

rezultatów poprzez rozwiązania o charakterze mniej inwazyjnym dla sfery praw i wolności osób, których dane dotyczą. Cyfryzacja, w rozumieniu prawnym i społecznym, powinna być rozumiana szeroko. Nie powinna wiązać się ona jedynie z digitalizacją istniejących procesów. Cyfryzacja stwarza szansę dla systemowego przeobrażenia funkcjonowania administracji. Unowocześnieniu technologii towarzyszyć winno unowocześnienie procedur i struktur, mających na celu m.in. zmniejszenie biurokracji i reformację procesów przetwarzania. Podkreślić należy, że to przede wszystkim prawodawca i władza wykonawcza, projektując kierunki działań państwa, powinni podejmować decyzje kierunkowe, strategiczne, które gwarantują poszanowanie ochrony praw podstawowych, w tym prawa do ochrony danych osobowych i prawa do prywatności.

Jakkolwiek należy poprzeć ogólny kierunek obrany przez projektodawcę, to w opinii organu ochrony danych osobowych Strategia wymaga głębszej refleksji pod względem interakcji nowych technologii przede wszystkim z gwarancjami konstytucyjnymi, ale również zasadami określonymi w prawem międzynarodowym i prawem UE – w aktach takich, jak Konwencja o ochronie praw człowieka i podstawowych wolności, Karta Praw Podstawowych Unii Europejskiej, Traktat o Unii Europejskiej czy Traktat o funkcjonowaniu Unii Europejskiej. Taki właśnie kierunek wyznacza Trybunał Sprawiedliwości Unii Europejskiej w swoim orzecznictwie[2]. Wymóg ten stawia również samo rozporządzenie ogólne[3]. Szczególną uwagę do tych kwestii przywiązuje także Europejski Inspektor Ochrony Danych (EIOD)[4], podkreślając, że **ochrona prywatności i danych osobowych w perspektywie przyszłości cyfryzacji stanowi zagadnienie fundamentalne dla demokracji.** Takie stanowisko EIOD jest podzielane przez Prezesa Urzędu Ochrony Danych Osobowych, zwłaszcza w kontekście zjawisk takich jak cyberprzestępczość, szpiegostwo cyfrowe, czy wykorzystanie danych osobowych do ataków na instytucje demokratyczne (np. kampanie dezinformacyjne). To też wiąże się z hasłem przewodnim nadchodzącej polskiej prezydencji w Radzie UE – „Bezpieczeństwo Europo", gdzie jednym z wymiarów bezpieczeństwa jest bezpieczeństwo informacyjne. **W wymiarze strategicznym działań państwa hasło „bezpieczeństwo informacyjne" jest kluczowym filarem polityki ochrony danych osobowych i szerzej – bezpieczeństwa narodowego**. Wszelkie działania strategiczne państwa zmierzające do wzmocnienia tego aspektu bezpieczeństwa wiążą się z ochroną danych osobowych jako kluczowym elementem bezpieczeństwa informacyjnego, chociażby w aspektach związanych z bezpieczeństwem systemów IT, monitorowaniem zagrożeń czy utrzymaniem poufności danych, w szczególności w rejestrach państwowych.

[2] Zob. wyroki TSUE w sprawach o sygn. C-470/21, C-6/12, C-634/21, C-219/91, C-594/12, C-291/12.
[3] Zob. motyw 41 RODO.
[4] Zob. strategia EDSP „Shaping a Safer Digital Future".

Prawo do prywatności i prawo do ochrony danych osobowych w perspektywie zagrożeń ery cyfrowej, takich jak masowy nadzór czy dezinformacja powinny być zatem traktowane priorytetowo pod kątem formowania strategicznych rozwiązań i już na tym etapie stosowne środki ochrony powinny zostać zaplanowane. Strategia powinna przewidywać środki skutecznej kontroli danych osobowych z punktu widzenia osób, których dane dotyczą już na etapie projektowania przepisów prawa czy przedstawiania koncepcji rozwiązań. Wymóg ten wynika nie tylko z ogólnej zasady uwzględniania ochrony danych w fazie projektowania wywodzącej się z rozporządzenia ogólnego, ale również innych aktów europejskich dla Polski wiążących, wchodzących w życie lub planowanych, w sposób fundamentalny związanych również z ochroną danych osobowych, takich jak chociażby Akt w sprawie sztucznej inteligencji, rozporządzenie eIDAS2, dyrektywa NIS2, czy program EuroHPC.

Mając na uwadze powyższe – w trosce o poziom ochrony praw jednostki, w szczególności prawa do prywatności oraz prawa do ochrony danych osobowych – przedstawione zostają poniżej uwagi, które mogą wzbogacić planowany kierunek rozwoju państwa w obszarze cyfryzacji. Ich uwzględnienie powinno służyć zapewnieniu obywatelom pełnych gwarancji poszanowania ich praw – aby nie zostały one pominięte w rozwoju technologicznym, ale także by przyczyniały się do wzmocnienia bezpieczeństwa informacyjnego państwa, co jest spójne z ww. priorytetami.

II. Uwagi szczegółowe.

Opracowanie wieloletniego planu cyfryzacji państwa, który harmonizuje zrównoważony rozwój technologiczny z ochroną praw i wolności obywateli wymaga kompleksowego, wieloaspektowego podejścia, uwzględniającego również ochronę danych osobowych, która w obecnym kształcie projektu nie została w wystarczający sposób podniesiona.

Wprawdzie w dokumencie kierunkowym nie jest możliwe uwzględnienie wszystkich aspektów ochrony danych osobowych, jednak pod rozwagę należy poddać elementy kluczowe oraz takie, które przed przyjęciem dalszych działań powinny zostać objęte pogłębioną analizą.

A. Przepisy dostosowane do ery cyfrowej.

Za kwestię priorytetową należy uznać wzmocnienie przepisów prawnych, poprzez dostosowanie ich do dynamicznych zmian technologicznych, oddając jednocześnie stopień ochrony prywatności gwarantowany przez rozporządzenie

ogólne. **Strategia powinna nie tylko uwzględniać zagrożenia wynikające z obecnie funkcjonujących już nowych technologii, takich jak sztuczna inteligencja czy gromadzenie danych przez IoT (tzw. internet rzeczy), ale – na ile to możliwe – antycypować zmiany technologiczne na przestrzeni lat.** Projektowanym przepisom nadać należy wymiar neutralności technologicznej, w znaczeniu zapewnienia im możliwie jak najdalej idącej odporności na zmiany technologii. Jednocześnie należy właściwie przypisywać odpowiedzialność – administratorowi, a nie narzędziu czy systemowi, w którym przetwarzane są dane.

Podstawowym zadaniem zarówno prawodawcy, jak i organów publicznych powinno być **wdrożenie środków kontroli usług cyfrowych**, np. poprzez mechanizmy certyfikacji i akredytacji oparte przede wszystkim o kryteria obligatoryjnego zapewnienia wymaganego, wysokiego stopnia poufności oraz transparentności. Kontrola usług cyfrowych powinna odbywać się nie tylko z poziomu państwa, ale również – w myśl zasady autonomii jednostki – poszczególnych obywateli, jako podmiotów praw. Powinno odbywać się to poprzez **zapewnienie obywatelom narzędzi umożliwiających i ułatwiających zarządzenie oraz realne dysponowanie swoimi danymi w sieci** (w tym skuteczne środki ich usuwania).

Powtarzającym się problemem dla ochrony danych osobowych jest obecnie brak stosowania podczas projektowania nowych regulacji normatywnych podejścia opartego na ryzyku[5] oraz uwzględniania ochrony danych w fazie projektowania[6]. W ocenie Prezesa UODO jest to problem kluczowy. Należy zatem zaproponować **wprowadzenie prawnego wymogu przeprowadzenia tzw. testu prywatności[7] już na etapie procesu legislacyjnego**, jako elementu oceny skutków regulacji (OSR). Tego rodzaju obowiązek jest szczególnie istotny w przypadku ekstensywnych systemów państwowych, rejestrów publicznych czy projektów integracji danych. Obecnie ocena skutków dla ochrony danych osobowych w praktyce jest często pomijana, z negatywnymi konsekwencjami dla wykonawców norm oraz osób, których dane dotyczą. Tego rodzaju luka pozwala na tworzenie systemów informatycznych realizowanych niekiedy z uchybieniem podstawowych zasad ochrony danych osobowych. Nałożenie obowiązku przeprowadzenia testu prywatności na etapie legislacyjnym pozwoliłoby twórcom na kreowanie systemów wyposażonych nie tylko w konkretne środki organizacyjno-techniczne zapewniające bezpieczeństwo danych już na poziomie normatywnym – nie przerzucając obowiązku ich wprowadzenia na administratorów lub użytkowników, ale i na przyjęcie rozwiązań optymalnych z punktu widzenia przysługujących podmiotom danych praw przewidzianych w rozdziale III rozporządzenia ogólnego.

[5] Zob. art. 24 RODO.
[6] Zob. art. 25 RODO.
[7] Zob. art. 35 RODO.

Analogicznie, postulowana jest także **zmiana wzoru opisu założeń projektu informatycznego**[8] Komitetu Rady Ministrów ds. Cyfryzacji (KRMC) o punkt, w którym beneficjent wskazuje informację w zakresie przetwarzania danych osobowych w projektowanym systemie informatycznym – co miałoby istotne prewencyjne znaczenie w zakresie tworzenia rozwiązań zgodnych z rozporządzeniem ogólnym.

Strategia kładzie nacisk na zwiększanie poziomu cyberbezpieczeństwa przy dalszym rozwoju cyfryzacji, nie zakłada natomiast żadnego przeglądu dotychczas obowiązujących przepisów i wprowadzenia zmian legislacyjnych, które od lat postuluje organ nadzorczy przy okazji konsultacji z Ministerstwem Cyfryzacji poszczególnych projekt aktów prawnych[9].

B. Edukacja i dostępność.

Strategia porusza temat dostępności cyfrowej dla wszystkich obywateli. Już na tym etapie zakładane jest dostosowanie podstawy programowej do postępu technologicznego czy ochrony przed dezinformacją. Obrany kierunek jest bezspornie słuszny, niemniej wymaga dalszego rozwinięcia. Cyfryzacja państwa – czy raczej całego społeczeństwa – powinna wiązać się z reformą edukacji. Wspierane powinny być przede wszystkim miękkie kompetencje przyszłości, takie jak empatia, współpraca, samodzielne myślenie. **Strategia powinna uwzględniać nie tylko edukację polegającą na zapoznaniu się z technologią i sposobami korzystania z niej, ale równorzędnie również ukierunkowaną na zwiększanie świadomości o bezpieczeństwie, prywatności i przysługujących środkach ochrony swoich danych osobowych (zarówno technicznych, organizacyjnych jak i prawnych).** Ucząc korzystania z technologii, szkoła powinna rozwijać rozsądny dystans do usług i aplikacji oferowanych przez firmy technologiczne oraz pokazywać ich szkodliwy wpływ na zdrowie psychiczne, jak również uczyć zdrowych nawyków cyfrowych i promować zachowania prozdrowotne (tzw. higienę cyfrową). Wziąć pod uwagę należy również wczesny etap edukacji, który realizowany powinien być zasadniczo bez żadnego kontaktu z urządzeniami elektronicznymi[10].

Edukacja cyfrowa w szkołach średnich powinna kształtować krytyczny zmysł wobec technologii – skupiać się nie tylko na kształtowaniu kompetencji cyfrowych (korzystanie z urządzeń), lecz przede wszystkim sprzyjać rozwojowi umiejętności rozumienia działania technologii w szerszym kontekście kulturowo-społecznym

[8] Uchwała Nr 6 Komitetu Rady Ministrów do spraw Cyfryzacji z dnia 6 kwietnia 2018 r. w sprawie określenia wzoru opisu założeń projektu informatycznego wydana na podstawie § 8 ust. 6 zarządzenia nr 48 Prezesa Rady Ministrów z dnia 12 kwietnia 2016 r. w sprawie Komitetu Rady Ministrów do spraw Cyfryzacji (M. P. poz. 379 z późn.zm.)

[9] Zob. opinia Prezesa UODO dot. projektu ustawy o zmianie ustawy o krajowy systemie bezpieczeństwa oraz niektórych innych ustaw z 4 czerwca 2024 r. (sygn.: DOL.401.155.2024.WL.RB, znak: P.MC.WL.0211.16.2024).

[10] Zob. petycja „Ratuj dzieci!" Instytutu Spraw Obywatelskich stanowiąca apel wielu specjalistów z zakresu także psychologii i psychiatrii dotyczący ograniczeń w korzystaniu z urządzeń elektronicznych (https://instytutsprawobywatelskich.pl/ratuj-dzieci/).

i ekologicznym. Rozważyć należy zastosowanie edukacji cyfrowej w szkole średniej realizowanej jako odrębny interdyscyplinarny przedmiot, zbierający wiedzę z zakresu antropologii, filozofii, etyki, teorii społecznej, nauk o mediach, nauk kognitywnych, ekonomii i prawa.

Dla skutecznej edukacji dzieci i młodzieży niezbędne jest **wsparcie kompetencji nauczycieli, nie tylko w kontekście rozwoju umiejętności cyfrowych (o czym mowa w Strategii), ale również świadomości zagrożeń oraz nabywania umiejętności obrony przed nimi.** Wymagane jest przewidzenie realnych środków w ramach reformy edukacji przeznaczonych na wspieranie nauczycieli, którzy pracują metodami projektowymi lub inspirują się pedagogiką projektową.

Problematyka edukacji nie powinna ograniczać się jedynie do nauczania w szkołach – **równie istotne jest wspieranie rodziców w edukacji cyfrowej ich dzieci,** poprzez integrację z systemem oświatowym, ale również kampanie społeczne i działalność szeroko rozumianych organów i organizacji zajmujących się pomocą rodzinom, tak aby zapewnić im wiedzę na temat korzyści, ale i możliwych negatywnych skutków korzystania z narzędzi cyfrowych.

Edukowanie dzieci i młodzieży jest kwestią niezaprzeczalnie istotną, **nie można jednak w ogólnym systemie edukacji pomijać osób narażonych na wykluczenie cyfrowe, w tym głównie osób starszych, nieporadnych lub z innego powodu bardziej narażonych na zagrożenia sieciowe.** Konieczne jest wprowadzenie usług społecznych mogących na bieżąco, wraz z rozwojem technologii, edukować osoby będące już poza systemem edukacji państwowej. Dotarcie do grupy senioralnej może odbywać się np. również poprzez system zdrowotny (lekarzy pierwszego kontaktu), w zakresie promowania zachowań prozdrowotnych związanych z używaniem technologii.

Strategia jedynie w niewielkim stopniu porusza problemy związane z niebezpieczeństwami wynikającymi z rozwoju cyfryzacji – przede wszystkim uzależnienia od stosowania technologii cyfrowych, zarówno pod względem psychospołecznym, jak i nadmiernego polegania w sensie mentalnym w codziennym funkcjonowaniu. Promowanie używania smarfonów niezbędnych do działania aplikacji oprócz oczywistych korzyści może mieć także niekorzystny wpływ szczególnie na mniej świadome zagrożeń dzieci i młodzież, do których przecież również kierowane są usługi państwowe takie jak np. mLegitymacja szkolna w aplikacji mObywatel[11]. Dlatego potrzebne jest położenie większego nacisku na te właśnie kwestie.

[11] Zob. ogólnopolski program edukacyjny Prezesa UODO „Twoje dane – twoja sprawa” (*https://uodo.gov.pl/pl/21/32*).

C. Bezpieczeństwo cyfrowe i dobrostan obywatela.

Jak wspomniano już w części B. niniejszej opinii, edukacja nie powinna ograniczać się jedynie do osób młodszych, ale w szerokiej perspektywie obejmować ogół społeczeństwa, różne grupy społeczne, w tym seniorów przez zwiększanie nie tylko kompetencji cyfrowych, ale również świadomości co do środków zapewniających bezpieczeństwo i chroniących zdrowie. Promowane powinno być stosowanie narzędzi do ochrony prywatności (takich jak choćby szyfrowanie danych, czy usługi VPN) oraz sposoby minimalizacji szkodliwego oddziaływania technologii na stan psychiczny. Wpływ wdrażanych rozwiązań na zdrowie publiczne nie może być traktowany powierzchownie. Zagadnienia z tym związane, w tym plany minimalizacji czasu ekranowego w środowisku szkolnym, zostały niewystarczająco rozwinięte w Strategii i wymagają dalszego wzmocnienia, a przede wszystkim opracowania omówionych szerzej w dalszej części środków monitorowania.

Wdrożeniu Aktu o usługach cyfrowych[12] towarzyszyć powinny nie tylko zmiany prawne, ale również kampanie edukacyjne promujące nowe standardy wynikające z tego aktu, przestrzegające obywateli przed zagrożeniami związanymi z niebezpiecznymi modelami biznesowymi wielkich platform cyfrowych. Organy publiczne mogą oddziaływać w sposób pozytywny również metodami pośrednimi, takimi jak wprowadzenie standardu nieuzależniających praktyk w projektowaniu aplikacji, obowiązujących przedsiębiorców będących beneficjentami programów wspierania innowacji, czy też wymogów przestrzegania określonych standardów przez firmy mające świadczyć usługi dla szkół, administracji, spółek Skarbu Państwa itp. – za przykład takiego standardu niech posłuży system automatycznego wyłączenia programów szczególnie narażających na utratę kontroli nad czasem.

Wypracowanie państwowych standardów dla ochrony w produktach i usługach cyfrowych skupiać powinno się przede wszystkim na osobach małoletnich. Z tego powodu pozytywnie należy odnieść się do wprowadzenia mechanizmów weryfikacji wieku przy zachowaniu prywatności. Niemniej jednak zagadnienie dostępu osób małoletnich do treści cyfrowych wymaga zmian systemowych, które powinny być poczynione w drodze szerszej debaty publicznej. Należy zadać pytanie o ustalenie bezpiecznego wieku korzystania z produktów cyfrowych (zwłaszcza serwisów społecznościowych), w oparciu o wiedzę o wpływie technologii na stan psychospołeczny małoletnich. **Przyszłość nowych technologii cyfrowych skonfrontować należy z obecnym stanem prawnym określającym wiek zdolności do czynności prawnych oraz korzystania z usług społeczeństwa informacyjnego, wynikający z kodeksu cywilnego i rozporządzenia ogólnego**. Nie przesądzając na tym etapie kierunku, postulować należy jednak podjęcie dyskusji

[12] 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. U. UE. L. 2022 poz. 277.1.

nad tym, czy za wystarczające ocenić należy zastosowanie oddziaływań o charakterze miękkim, poprzez kampanie edukacyjne oraz promowanie zdrowych i bezpiecznych wzorców korzystania z produktów cyfrowych oparte na aktualnym stanie prawnym, czy raczej rozważyć należałoby rozwiązanie tej kwestii na drodze norm prawnych zakazujących osobom poniżej określonego wieku korzystanie z produktów cyfrowych takich jak media społecznościowe[13].

D. Technologia w służbie jednostki.

1. Tożsamość cyfrowa.

Strategia opisuje dalszy rozwój e-usług, takich jak cyfrowa tożsamość czy interoperacyjne rejestry, ale nie określa chociażby w sposób ogólny zasad ochrony danych osobowych, które systemy te respektują. Upowszechnianie różnych form podpisów elektronicznych powinno iść w parze z wprowadzeniem zmian systemowych w powszechnie obowiązującym prawie – szczególnie w perspektywie przewidzianej przez rozporządzenie eIDAS2 funkcji europejskiego portfela tożsamości cyfrowej oraz pojęcia certyfikatu podpisu elektronicznego. Szczególne zagrożenia dla prywatności obywateli związane są obecnie z coraz szerszym wykorzystywaniem (w tym ujawnianiem osobom postronnym) numeru PESEL w formie identyfikatora w podpisach elektronicznych, w tym wykorzystywania tego numeru przez pracownika reprezentującego pracodawcę jako podmiot zobowiązany – w sposób daleko odbiegający od pierwotnych celów numeru PESEL jako numeru referencyjnego do identyfikacji podatkowej, świadczeń z zakresu ubezpieczeń społecznych i ewidencji ludności. Bez podjęcia adekwatnych działań prawnych ze strony państwa problem ten będzie się jedynie pogłębiał[14].

Identyfikacja użytkowników nie powinna ograniczać się jedynie do podpisów elektronicznych. Konieczne jest wprowadzenie również w przestrzeni publicznej innych form potwierdzenia tożsamości, które – uwzględniając rozwój technologiczny – będą wiarygodne także w przyszłości. Z jednej strony konieczne jest opracowanie skutecznych i funkcjonalnych metod identyfikacji (szczególnie w kontekście weryfikacji wieku małoletnich dopuszczonych do usług cyfrowych), z drugiej zaś ustalenie granic ingerencji w sferę prywatności i autonomii informacyjnej jednostki. Strategia nie odnosi się do problemu identyfikacji z wykorzystaniem danych biometrycznych (w tym behawioralnych), chociaż takie mechanizmy są już stosowane (np. przez banki i inne instytucje finansowe). Tym samym, wymagane jest uregulowanie tej tematyki, w taki sposób, aby zapewnione

[13] Por.: przyjęta 28 listopada 2024 r. przez Senat Australii ustawa „Online Safety Amendment (Social Media Minimum Age) Bill 2024", wprowadzająca bezwzględny zakaz korzystania z mediów społecznościowych przez osoby poniżej 16 roku życia (*https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7284*).
[14] Zob. wystąpienie Prezesa UODO do Ministra Cyfryzacji z 12 września 2024 r. (sygn. DOL.413.3.2024.WL).

zostało ograniczenie przetwarzania danych biometrycznych do niezbędnego minimum, przy zachowaniu właściwych rygorów ochrony i poufności danych osobowych, tj. ze wskazaniem mechanizmów przewidujących odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą[15] oraz stworzeniem możliwych rozwiązań alternatywnych.

Zwiększenie wykorzystania internetu rzeczy (IoT) oraz sztucznej inteligencji (AI) w przestrzeni publicznej nieodłącznie związane jest ze wzmożonym zagrożeniem szerokiego wykorzystania technologii śledzących (często wręcz inwigilujących) osoby fizyczne. Strategia „inteligentne miasta" (smart cities) zakłada optymalizację zarządzania usługami publicznymi m.in. w oparciu o dane zbierane z coraz bardziej zawansowanych i rozbudowywanych systemów monitoringu. Ustalenie granic wykorzystania nowych technologii przez podmioty publiczne obowiązane do działania na podstawie i w granicach wyznaczonych im przepisami prawa (zasada legalizmu), w świetle potencjalnych negatywnych skutków dla suwerenności jednostki – w tym celem uniknięcia rozwiązań polegających na stosowaniu zautomatyzowanego podejmowania decyzji wywołującego wobec jednostki skutki prawne lub w sposób podobny istotnie na nią wpływającego – ma znaczenie kluczowe.

Strategia nie rozwija też mechanizmów zgód obywateli na przetwarzanie danych w systemach cyfrowych (opartych o kryteria świadomości, dobrowolności oraz braku ujemnych skutków w przypadku jej nieudzielenia lub odwołania), co stwarzać może pole do nadużyć w wykorzystywaniu danych.

2. Rejestry publiczne i aplikacja mObywatel.

Założony w Strategii rozwój rejestrów publicznych niesie ze sobą konieczność dokonania przeglądu dotychczasowego modelu ich funkcjonowania i wypracowania jednolitych standardów ich tworzenia. Założenia te już na etapie ich przyjmowania powinny być formułowane w oparciu o zasady przetwarzania danych ujęte w art. 5 rozporządzenia ogólnego i z zachowaniem warunków przewidzianych w art. 6 ust. 3, jak również art. 9 ust. 2-4 tego aktu, tak, aby stworzyć kompletne regulacje prawne, przyznające konkretne gwarancje prawne podmiotom danych w przypadku przetwarzania dokonywanego przez organy publiczne (administratorów) – z zachowaniem zasad: niezbędności, minimalizacji, ograniczenia przetwarzania, przejrzystości, rzetelności, rozliczalności oraz zapewnienia skutecznych środków bezpieczeństwa.

Szczególne obawy budzi zakładana interoperacyjność różnych baz, zasobów danych, systemów, stwarzająca znaczne ryzyko ich łączenia[16]. Przekazywanie

[15] Warunki dopuszczające przetwarzanie zostały określone w art. 9 ust. 2 rozporządzenia ogólnego w odniesieniu do wyjątków od zasady zakazu przetwarzania danych szczególnych kategorii
[16] Por. motyw 31 rozporządzenia ogólnego.

danych z zasobów coraz większych zbiorów danych potencjalnie utrudnia, czy wręcz czyni iluzoryczną możliwość sprawowania kontroli praw przez osoby, których dane dotyczą, a po stronie administratorów trudnym do spełnienia jest wymóg rozliczalności[17]. Problemy te nasila zakładany w Strategii model szerokiej współpracy z sektorem prywatnym przewidujący migrację danych z rejestrów państwowych do zasobów podmiotów rynkowych / prywatnych – na podstawie zawieranych porozumień, a nie przepisów prawnych rangi ustawowej. Wprowadzanie rozwiązań umożliwiających udostępnianie danych z poszczególnych rejestrów publicznych wymaga stosownego uprzedniego przeglądu obowiązujących regulacji i przyjęcia odpowiednich przepisów sektorowych, tak, aby zagwarantować w przepisach prawa rozwiązania spójne i zupełne oraz przewidujące mechanizmy zapewniające bezpieczeństwo przetwarzania danych oraz jasno określające status i odpowiedzialność wszystkich podmiotów biorących udział w procesach. **Wprowadzenie mechanizmu przepływu / wymiany danych / wspólnego przetwarzania danych pomiędzy bazami, czy rejestrami wymaga każdorazowej, wnikliwej analizy na poziomie legislacyjnym pod względem uczynienia zadość zasadom z art. 5 rozporządzenia ogólnego oraz zapewnienia realizacji praw podmiotów danych**[18].

Również rozwój aplikacji mObywatel i korzystania z kolejnych usług państwa z jej wykorzystaniem wymaga pogłębionych zmian systemowych w przepisach prawa. Dostosowania do zasad ochrony danych osobowych wymaga przede wszystkim sama ustawa o aplikacji mObywatel, która stwarza szereg problemów sygnalizowanych już przez Prezesa UODO, a które pozostają nadal aktualne[19]. Jedną z jej największych wad prawnych tej ustawy, wpływającą na kwestie bezpieczeństwa przetwarzania, jest niejasne określenie ról w procesach przetwarzania danych osobowych z użyciem aplikacji. Wątpliwości budzi status poszczególnych administratorów zawierających porozumienia z Ministrem Cyfryzacji. Ustawa zawiera również szereg rozwiązań blankietowych umożliwiających tworzenie nowych usług i „dokumentów elektronicznych" na podstawie uznaniowej decyzji Ministra Cyfryzacji. Dodatkowo pod rozwagę poddać należy z punktu widzenia zasady bezpieczeństwa przetwarzania danych, czy funkcje aplikacji mObywatel , które nie powinny być dostępne również z poziomu przeglądarki internetowej, bez konieczności instalacji aplikacji na urządzeniu. Sama aplikacja powinna być dostępna do pobrania ze stron rządowych w celu uniezależnienia od komercyjnych kanałów dystrybucji.

[17] Por. wyrok Naczelnego Sądu Administracyjnego z 3 grudnia 2021 r., sygn. III OSK 590/21.
[18] Zob. opinia Prezesa UODO z 5 maja 2022 r. dot. projekt ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji (sygn.: DOL.401.169.2022, znak: DRC.WL.0610.5.2021).
[19] Zob. opinia Prezesa UODO dot. projektu ustawy o aplikacji mObywatel z 17 lutego 2023 r. (sygn.: DOL.401.276.2022, znak: RCL.DPUE.550.21/2022) oraz dalsze (sygn. DOL.060.18.2024.WL.PM, DOL.060.31.2024.WL.EKR).

E. Mechanizmy ochrony praw jednostki.

W kontekście ochrony praw jednostki warto zwrócić uwagę, że poszerzonych regulacji wymagają zagadnienia związane z wykorzystaniem sztucznej inteligencji (AI). Punktem odniesienia dla wprowadzenia szczegółowych regulacji powinny być zasady: etycznego rozwoju, transparentności przyjmowanych rozwiązań, odpowiedzialności i przeciwdziałania różnym formom dyskryminacji. Zastosowanie tych zasad powinno przybrać wymiar uniwersalny, a więc odnosić się nie tylko do sektora prywatnego, ale w równym stopniu również do sektora publicznego.
W konkretnym wymiarze, przykładowo dostarczanie przez dany urząd państwowy treści (tekstowych, wideo, grafik) powinno być poprzedzone obowiązkiem informowania, że zostały wygenerowane przez AI wraz z publikacją w BIP informacji o użytym modelu i treści promptów. Wprowadzenia wymaga obowiązek informowania użytkowników o zastosowanych algorytmach oraz tego w jaki sposób dane są wykorzystywane i przetwarzane (w formule przystępnej i zrozumiałej dla odbiorcy).

Projektodawca powinien przewidzieć stosowanie środków kontroli przestrzegania zasad postępowania z technologią sztucznej inteligencji (AI) oraz wykrywania błędów systemów, poprzez stałe i obowiązkowe audyty i przeglądy. Ponadto, wymagane jest wprowadzenie zabezpieczeń przeciwko niejawnemu i bezprawnemu nadzorowi (np. z wykorzystaniem biometrii). Rozszerzonej analizy wymaga zagadnienie tzw. agentów sztucznej inteligencji, a więc tego, jak uregulowane powinno zostać reprezentowanie osób i podmiotów za pomocą oprogramowania, które może wykonywać w imieniu użytkownika zadania, podejmując decyzje i wchodzić w interakcję z innymi podmiotami czy osobami. Z punktu widzenia ochrony praw podmiotów danych kwestią kluczową jest też uregulowanie materii zautomatyzowanego podejmowania decyzji i profilowania z wykorzystaniem sztucznej inteligencji, szczególnie w kontekście podstaw prawnych na tego rodzaju operacje przetwarzania, udzielania zgody, spełniania obowiązku informacyjnego, realizowania prawa do interwencji ludzkiej, czy wdrażania właściwych środków ochrony interesów osób, których dane dotyczą. Szczególna uwaga powinna zostać poświęcona operacjom przetwarzania danych szczególnych kategorii (np. wymiana dokumentacji medycznej między placówkami[20]).

Nie tylko w kontekście bezpieczeństwa, ale również zgodności z normami etycznymi oraz poszanowaniem godności ludzkiej, zagadnienia związane z wykorzystaniem sztucznej inteligencji wymagają dalszej pogłębionej debaty, zwłaszcza w kontekście przyjmowania rozwiązań opieranych wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, wywołującemu skutki prawne lub w inny sposób znacząco wpływającemu na jednostkę (podmiot danych). Potrzebne jest wytyczenie jasnych granic sfer, w których użycie takich technologii

[20] Zob. bezpieczne standardy wymiany danych medycznych wdrażane na gruncie Europejskiej przestrzeni danych dotyczących zdrowia (EHDS).

jest dopuszczalne, a które powinny zostać od niej (przy użyciu stosownych środków gwarancyjnych) skutecznie odseparowane – w szczególności mowa tu o szeroko rozumianej opiece zdrowotnej, czy wymiarze sprawiedliwości.

Bardzo dobrym rozwiązaniem, docenianym i wspieranym przez organ nadzorczy, jest sformułowanie modelu przejrzystego dostępu obywatela do informacji o tym jaki organ i w jakiej sprawie miał dostęp do określonych dotyczących go danych osobowych. Udostępnienie obywatelowi – działającej niezależnie od służb publicznych i administracji rządowej – ścieżki kontroli oraz zgłaszania naruszeń wyznacza słuszny kierunek rozwoju, sprzyjającego gwarancjom konstytucyjnym i z tych powodów wart jest dalszego rozwoju i przeniesienia również na inne aspekty Strategii.

Cyfryzacja jest szansą, aby administracja publiczna przeniesiona została na alternatywne, działające w interesie publicznym kanały bieżącej komunikacji z obywatelem, odchodząc od zamkniętych platform. **Ze stron administracji publicznej zniknąć powinny zbędne skrypty śledzące.**

Rekomendowanym przez organ nadzorczy rozwiązaniem jest stworzenie sprawnej, darmowej, bezpiecznej, posiadającej otwarte API i dostosowanej do polskiego systemu edukacji platformy do komunikacji szkół z rodzicami (e-dziennik).

Są to przykłady rozwiązań sprzyjających budowaniu zaufania osób fizycznych do proponowanych przez państwo technologii, bez pośrednictwa podmiotów prywatnych oferujących przy tej okazji rozszerzenie zakresu usług za opłatą.

F. Suwerenność cyfrowa państwa i odpowiedzialność korporacji technologicznych.

Projektodawca słusznie spostrzegł, że uzależnienie od rozwiązań dostarczanych przez zewnętrznych dostawców jest potencjalną słabością cyfrowego państwa. **Stanowi to niebezpieczeństwo dla suwerenności cyfrowej, prywatności obywateli oraz cyberbezpieczeństwa, ale również jest wątpliwe z punktu widzenia gospodarności.** Zbudowanie publicznej infrastruktury może być w dalszej perspektywie zabiegiem gwarantującym niezależność funkcjonowania systemów państwa, jak i rozwiązaniem tańszym z punktu widzenia przeznaczanych środków publicznych. Suwerenność nie powinna być przy tym rozpatrywana jedynie w aspekcie cyfrowym. Suwerenność danych (rozumiana jako dostęp do danych) oraz związana z nią także ściśle niezależność energetyczna państwa są równie istotne i powinny zostać poparte konkretnymi rozwiązaniami.

Z punktu widzenia standardów przetwarzania danych osobowych niepokojącym zjawiskiem, z którym należy się zmierzyć, jest tworzenie rozwiązań w oparciu o infrastrukturę dużych korporacji technologicznych, których siedziby

znajdują się poza Europejskim Obszarem Gospodarczym. W tym aspekcie niezwykle istotne jest zapewnienie poszanowania europejskich regulacji prawnych. **Obywatelom powinien zostać zapewniony dostęp do usług publicznych poprzez aplikacje gwarantowane przez własne państwo, a nie podmioty czy *de facto* państwa trzecie, bez względu na producenta urządzeń i oprogramowania, z których korzystają.**

Strategia zakłada rozwój chmury obliczeniowej, ale nie przedstawia konkretnych warunków dotyczących przechowywania danych obywateli, ani mechanizmów weryfikacji bezpieczeństwa usług. Zauważalny jest bardzo duży nacisk na współpracę z sektorem prywatnym przy tworzeniu poszczególnych rozwiązań informatycznych. Nie należy kwestionować samego zamysłu zaangażowania podmiotów prywatnych w tworzenie infrastruktury cyfrowej, jednak taki model powinien być oparty na konkretnych gwarancjach, kryteriach weryfikacji takich partnerów oraz w sposób wykluczający monopolizację ze strony podmiotów prywatnych. Szczególnie niepokojące byłoby wdrażanie takich rozwiązań jak publiczna chmura obliczeniowa w oparciu wyłącznie o infrastrukturę wielkich korporacji technologicznych operujących poza reżimem prawnym UE. Takie rozwiązanie pod znakiem zapytania stawiałoby możliwość sprawowania realnego nadzoru i zapewnienia standardów poufności przetwarzanych informacji.

Dodatkową analizę poświęcić należy kwestii suwerenności energetycznej i ekonomicznej. Strategia powinna przewidywać zasób energetyczny potrzebny do utrzymywania planowanych systemów, jak również plany kryzysowe, zachowanie ciągłości i dostępu do danych w przypadku awarii i dłuższej utraty energii. Przeanalizować należy funkcjonowanie systemu w warunkach ograniczonych zasobów energetycznych oraz ich zupełnego braku w sytuacjach nadzwyczajnych. Nie można pomijać aspektu związanego z obronnością, a więc w jakim stopniu infrastruktura krytyczna dla funkcjonowania państwa odporna jest na zintensyfikowane działania hybrydowe o charakterze zorganizowanych, masowych cyberataków.

Osobnym problemem, który również nie może być bagatelizowany jest zapewnienie środków do wspierania zarówno organizacyjnego, technicznego jak i finansowego, by umożliwić wdrożenie i efektywne działanie powołanym instytucjom władzy publicznej.

G. Monitorowanie i adaptacja Strategii.

Strategia stanowi wizję cyfryzacji Polski na rok 2035, jednak nie została uzupełniona o cele cząstkowe. Już tylko cyberbezpieczeństwo jest wyzwaniem w tym samym stopniu perspektywicznym, co bieżącym. Wdrażanie konkretnych rozwiązań powinno odbywać się zatem już obecnie, a w dalszej perspektywie etapowo, **według określonego planu działania (realizacji celów cząstkowych).**

Takiemu planowi towarzyszyć powinny regularne konsultacje społeczne umożliwiające obywatelom wypowiedzenie się na temat działania systemów cyfrowych państwa, w tym również w kontekście zagrożenia praw podmiotów danych. Strategia powinna przewidywać w tym zakresie elastyczność i możliwość modyfikacji w perspektywie nowych informacji zwrotnych lub pojawiających się problemów. Elementem podstawowym Strategii powinno być zarządzenie dynamiczne, polegające na monitorowaniu postępów, reagowaniu na bieżące wyzwania i modyfikacji założeń. Przede wszystkim monitorowaniem objęte powinny zostać relacja implementowanych technologii na stan zdrowia publicznego oraz jaki wywierają one wpływ społeczny – ale także klimatyczny, a więc jaki wpływ technologia ma na środowisko, czy procesy są, albo mogą zostać uczynione bardziej energooszczędnymi. Nie tylko planowanie, ale dobrze przeprowadzona analiza użycia nowych rozwiązań jest podstawą do ewolucyjnego wypracowywania rozwiązań optymalnych.

Możliwość dostosowania założeń Strategii do nowych okoliczności jest szczególnie istotna z punktu widzenia dopiero rozwijających się nowych systemów elektronicznych – komputerów kwantowych. Postkwantowa ochrona prywatności i metody zabezpieczenia danych przed łamaniem zabezpieczeń komputerami kwantowymi wymagają stałego śledzenia rozwoju tej technologii, zarówno rozwiązań już funkcjonujących, jak i perspektywicznego budowania zaplecza naukowego, specjalistycznego i technicznego potrzebnego w przyszłości.

Możliwość elastycznego implementowania do strategii informatyzacji państwa rozwoju nowych technologii i potrzebnych środków zaradczych jest kluczowa. Projektodawca słusznie diagnozuje niebezpieczeństwa ery cyfrowej takie jak modele biznesowe oparte na uzależnianiu użytkowników od ich treści, algorytmy śledzące, upowszechnianie nierealistycznych standardów urody, dostęp nieletnich do szkodliwych treści, wykluczenie społeczne, dezinformacja, które mają negatywny wpływ na zdrowie psychiczne zarówno dzieci i dorosłych oraz osłabienie więzi społecznych. W tym kontekście Strategia powinna poruszyć zagadnienie monitorowania postępów jej wdrażania oraz skutków przyjmowanych rozwiązań dla różnych grup wiekowych. Pod rozwagę należy wziąć również wygospodarowanie środków publicznych na badanie wpływu mediów społecznościowych na stan psychiczny obywateli oraz oddziaływanie na kondycję debaty publicznej i funkcjonowanie zasad demokratycznego państwa. Właściwa reakcja organów państwowych, poprzez odpowiednie ustawodawstwo czy oddziaływanie pośrednie, może być podjęta po zbadaniu aktualnych skutków zidentyfikowanych zagrożeń.

III. Uwagi końcowe.

Rozwój cyfrowy jest zjawiskiem doniosłym i złożonym, mającym wymiar zarówno prawny, społeczny, kulturowy, polityczny, naukowy, ekonomiczny wychowawczy, związany z obronnością, jak i odnoszący się do elementarnych praw i wolności jednostki. Zdaniem organu ochrony danych osobowych budowanie strategicznego planu rozwoju państwa cyfrowego powinno stanowić emanację wspólnej inicjatywy różnych resortów, służb, organów administracji i organizacji pozarządowych.

Ufam, że niniejsze pismo stanie się pozytywnym impulsem do dalszego rozwoju Strategii również pod względem materii związanej z ochroną danych osobowych i prywatności, mając na celu pogodzenie rozwoju technologicznego z ochroną praw podstawowych. Deklaruję niezmiennie wsparcie eksperckie Urzędu Ochrony Danych Osobowych i liczę na zaangażowanie nad wdrażaniem Strategii oraz konkretnych rozwiązań prawnych z niej wynikających.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu
Ochrony Danych Osobowych