Minister
Cyfryzacji

BM.WBKN.053.35.2024
Warszawa, 03 sierpnia 2024

Fundacja Panoptykon
Fundacja "Internet. Czas Działać!"

Szanowni Państwo,

odpowiadając na Państwa petycję w sprawie wykorzystywania technologii śledzących na stronach internetowych prowadzonych przez organy administracji publicznej, w pierwszej kolejności chcę wyrazić wdzięczność za zwrócenie uwagi na wysoce istotny temat, jakim jest prawo do prywatności w Internecie, w tym zwłaszcza ochrona danych osobowych.

W temacie wykorzystywania technologii śledzących, bez wątpienia to instytucje administracji publicznej w pierwszej kolejności zobowiązane są kreować najlepszy wzór przestrzegania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej „RODO")[1] oraz ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[2], wdrażającej do polskiego porządku prawnego przepisy Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.

Odpowiadając na przedstawione w petycji wątpliwości dotyczące przekazywania danych do podmiotów trzecich mogących mieć siedzibę lub lokację serwerów, na których znajdą się dane, poza Europejskim Obszarem Gospodarczym, zwracam uwagę, że przywołane w piśmie porozumienie EU-US Data Privacy Framework wraz z decyzją wykonawczą Komisji Europejskiej stanowi obecnie podstawę do legalnego przekazywania danych do podmiotów ze Stanów Zjednoczonych. Niezależnie jednak od ww. porozumienia, przed przekazaniem danych osobowych konieczne jest przeprowadzenie szeregu działań przez każdego administratora danych, które umożliwią weryfikację legalności takiego transferu. Należy do tego m.in. zweryfikowanie podmiotu, do którego przekazywane są dane oraz określenie zasad i celów przetwarzania związanych z przekazywaniem tych danych. Jak wskazano w petycji, w przypadku technologii śledzących część polskich instytucji administracji publicznej w ramach oferowanych na stronach internetowych usług korzysta z narzędzi dostarczonych przez Google LLC. Spółka ta znajduje się na liście zweryfikowanych podmiotów zgodnie z założeniami porozumienia EU-US Data Privacy Framework.

W tym miejscu należy zwrócić uwagę na rolę polityk prywatności i polityk dotyczących plików cookies, które powinny być zgodne z wymogami RODO oraz w sposób transparentny i czytelny umożliwiać użytkownikowi rzeczywiste zapoznanie się z zasadami pozyskiwania i przetwarzania jego danych osobowych, potencjalnymi odbiorcami tych danych i przysługującymi mu prawami. Obowiązek przygotowaniem ww. polityk spoczywa na określonym administratorze danych, do którego należy konkretna strona internetowa. To w gestii administratora spoczywa przeprowadzenie analizy potrzeb związanych z zakresem pozyskiwanych danych, w tym zwłaszcza dążenie do minimalizacji danych

[1] rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej „RODO")
[2] ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2024 r. poz. 34).

telefon: +48 22 245 54 42
adres email: sekretariat.BM@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa

gromadzonych poprzez wykorzystanie narzędzi typu cookies. W tym kontekście trzeba wskazać przepis art. 37 ust. 1 RODO, zgodnie z którym administrator zobowiązany jest wyznaczyć inspektora ochrony danych, gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[3], w art. 9, wprost wymienia organy i podmioty publiczne obowiązane do wyznaczenia ww. inspektora. Są to jednostki sektora finansów publicznych (np. jednostki samorządu terytorialnego, uczelnie publiczne), instytuty badawcze oraz Narodowy Bank Polski. Wobec tego, każdy administrator w postaci instytucji publicznej powinien zapewnić sprawne funkcjonowanie powołanego inspektora i wykonać przy jego pomocy wszelkie konieczne analizy dotyczące pozyskiwanych danych, a także ustalić, które narzędzia typu cookies rzeczywiście są nieodzowne do prawidłowej realizacji usługi na stronie internetowej.

Jednocześnie, należy podkreślić, że w Polsce organem nadzorczym w sprawach ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (UODO). W przypadku występowania jakichkolwiek nieprawidłowości na stronie internetowej danego administratora, np. w zakresie kształtu polityk prywatności czy banneru zawierającego informacje o plikach cookies, każdy podmiot dostrzegający takie nieprawidłowości uprawniony jest zgłosić je do Prezesa UODO.

Podobnie w sytuacji, w której nieprzestrzegane są przepisy art. 173 ustawy Prawo telekomunikacyjne, tj. gdy informacje użytkownika lub abonenta przechowywane są bez jego zgody, uprawniony on jest do dochodzenia swoich praw przed Prezesem Urzędu Komunikacji Elektronicznej (UKE). Prezes Urzędu Komunikacji Elektronicznej może nałożyć karę pieniężną na podmiot, który nie wypełnia obowiązków uzyskania zgody abonenta lub użytkownika końcowego, o których mowa w art. 173 Prawo telekomunikacyjne.

W związku z powyższym, podstawową rolę w zakresie budowania świadomości co do zgodnego z przepisami RODO i ustawy Prawo telekomunikacyjne korzystania z narzędzi typu cookies odgrywają Prezes UODO i Prezes UKE. Przeprowadzenie kontroli stosowania przepisów ochrony danych w instytucjach publicznych znajduje się w zakresie uprawnień Prezesa UODO.

W tym aspekcie zwracam uwagę również na wytyczne publikowane przez Prezesa UODO, jak i Europejską Radę Ochrony Danych (dalej: EROD), które stanowić powinny podstawę dla wszystkich administratorów przy opracowywaniu polityk prywatności czy polityk stosowania plików cookies. Wymienić można w tym kontekście między innymi wytyczne EROD nr 2/2023 z 14 listopada 2023, dotyczące zakresu technicznego art. 5 ust. 3, Dyrektywy 2002/58/WE oraz wytyczne Grupy Roboczej art. 29 (poprzednika EROD) dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia RODO.

Należy zauważyć, że EROD, dostrzegając wagę problemu, powołał grupę zadaniową ds. bannerów cookies, której prace poskutkowały wydaniem raportu wytyczającego minimalne wymogi, co do zgodnego z RODO, wykorzystywania plików cookies na stronach internetowych. Odnosząc się do technologii śledzących warto także kierować się publikacjami European Union Agency for Cybersecurity oraz orzecznictwem TSUE (np. w kontekście wyroku TSUE z 7 marca 2024. w sprawie C-604/22).

Ze względu na istotność tematu, zwróciłem się do Prezesa UODO oraz Prezesa UKE celem uzyskania informacji o problemie wskazanym w petycji oraz określenia odpowiedniego, zdaniem powyższych organów, kierunku działań. Skoordynowanie stanowisk ze wspomnianym organami jest niezbędne, gdyż to one w polskim porządku

[3] ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781).

prawnym nadzorują podniesione w petycji kwestie związane z wykorzystaniem technologii śledzących w Internecie.

Prezes UKE podkreślił istotność stosowania z najwyższą starannością przez organy administracji publicznej zasad ochrony prywatności, w tym ochrony danych osobowych użytkowników stron internetowych, w ramach własnych działań, co jest szczególnie istotne w dobie rozwoju usług e-administracji. Zwrócono uwagę, że organy administracji publicznej w sposób szczególny powinny dbać o bezpieczeństwo interesariuszy w ramach przyjętych polityk dotyczących plików cookies na stronach internetowych administracji publicznej. Mając powyższe na uwadze, Prezes UKE wskazał na potrzebę wypracowania pod auspicjami Ministerstwa Cyfryzacji i we współpracy z zainteresowanymi organami, wspólnych standardów, które pozwoliłyby na zabezpieczenie interesów użytkowników stron internetowych i ujednolicenie sposobu działania administracji publicznej w przedmiotowym obszarze.

W przedmiotowej sprawie stanowisko zajął również Prezes UODO, uwypuklając wagę kwestii zachowania prawa podmiotu danych do decydowania o swoich danych, zwłaszcza mając na uwadze ciągły rozwój technologiczny. Wskazał również, że wszystkie przyjmowane rozwiązania oparte o automatyczne przetwarzanie danych osobowych powinny być zgodne z zasadami ochrony danych osobowych i uwzględniać instrumenty przewidziane w RODO, w tym analizę ryzyka, ocenę skutków dla ochrony danych czy domyślną ochronę danych. Podniósł także, że stosowanie narzędzi informatycznych opartych na śledzeniu zachowania użytkownika może prowadzić do niekontrolowanego gromadzenia i przekazywania danych osobowych poza EOG z wykorzystaniem np. technologii plików cookies. Kluczowe znaczenie przypisano określeniu, czy informacja identyfikująca urządzenie końcowe użytkownika objęta jest zakresem definicji danych osobowych. Powołując się na motyw 30 RODO oraz pojęcie danych osobowych, a także wyrok TSUE z dnia 4 maja 2023 r. w sprawie C-487/21 stwierdzono, że administratorzy stron internetowych, którzy wykorzystują tzw. technologie śledzące, czy to w formie specjalnych skryptów, czy tzw. plików cookies, przetwarzają dane osobowe użytkowników odwiedzających ich strony. Działania podejmowane przez administratorów związane z prowadzeniem strony internetowej muszą spełniać wymogi wynikające z rozporządzenia RODO. Obowiązkiem podmiotu publicznego będącego administratorem będzie więc przeprowadzenie analizy ryzyka oraz zweryfikowanie podstawy prawnej każdego przetwarzania danych osobowych. Prezes UODO zaznaczył, iż identyfikuje problem podniesiony w petycji – i podejmuje w tym zakresie odpowiednie działania. Prowadzone są szkolenia dotyczące tematyki ochrony danych osobowych dla podmiotów publicznych, jak również akcje edukacyjne, zwłaszcza pod kątem ryzyk związanych z przetwarzaniem danych przez organy administracji publicznej oraz stanowienia prawa regulującego przetwarzanie danych. W przypadku skarg na nieprawidłowości w działaniu podmiotów publicznych jako administratorów, prowadzone są postępowania zmierzające do wyjaśnienia sprawy i wydania decyzji. Ponadto, przedstawiciele UODO aktywnie biorą udział w pracach podgrupy EROD ds. mediów społecznościowych (Social Media Expert Subgroup), która przygotowuje dokument dotyczący wykorzystywania mediów społecznościowych przez podmioty sektora publicznego.

Jednocześnie pragnę wspomnieć, że także Zespół do spraw wdrożenia i utrzymania Portalu RP w Ministerstwie Cyfryzacji korzysta z dobrych praktyk rekomendowanych przez odpowiednie podmioty zewnętrzne oraz ekspertów wewnętrznych w zakresie ochrony danych osobowych oraz bezpieczeństwa informacji. Portal RP nie tylko nie gromadzi żadnych danych wrażliwych osób go odwiedzających, ale również dba o anonimizację sesji otwieranych w przeglądarkach internetowych użytkowników sieci Internet podczas wizyt na stronach informacyjnych jednostek administracji publicznej alokowanych pod adresami www.gov.pl oraz samorzad.gov.pl.

Większość witryn internetowych wykorzystuje narzędzia analityczne do wyciągania wniosków na temat zachowania użytkowników. Najpopularniejszym z nich jest Google Analytics i z tego narzędzia w pierwszym okresie swojego funkcjonowania również korzystał Portal RP. Przeprowadzone przez Ministerstwo Cyfryzacji konsultacje w tym zakresie potwierdziły, że operator serwisu gov.pl / samorzad.gov.pl nie ma wpływu na przetwarzanie przez Google danych (np. do celów profilowania), stąd podjęto decyzję o zmianie narzędzia analitycznego. Należy podkreślić, że przyjęcie wcześniej wspomnianego EU-US Data Privacy Framework na nowo uregulowało wymianę danych pomiędzy podmiotami mającymi siedzibę w państwach członkowskich UE a podmiotami ze Stanów Zjednoczonych. W świetle przywołanego dokumentu należy uznać, że wykorzystywanie Google Analytics jest dozwolone, niemniej jednak, niezależnie od treści EU-US Data Privacy Framework, spełnione muszą być jednocześnie wszystkie warunki przekazywania danych, które określone są w RODO. Mając to na uwadze, korzystanie z Google Analytics poprzedzone musi być odpowiednią pogłębioną analizą, zwłaszcza w przypadku stron administracji publicznej.

Aby zachować zgodność z RODO, konieczne jest m.in. korzystanie z usług pomiaru i analizy oglądalności, które służą wyłącznie do tworzenia anonimowych danych statystycznych. Wobec powyższego Ministerstwo Cyfryzacji zdecydowało się na korzystanie z oprogramowania Matomo. Platforma ta korzysta z opcji anonimizacji danych, dzięki czemu mamy dostęp do informacji nie tylko o tych osobach, które wyraziły na to zgodę. Aktualnie, na stronach gov.pl i samorzad.gov.pl, nie widnieje widget, który pozwala na zarządzanie danymi osobowymi. Prace nad tym rozwiązaniem zostały rozpoczęte w ubiegłym roku. W najbliższym czasie narzędzie zostanie zaimplementowane na wyżej wymienionych portalach zgodnie z art. 6 RODO i wytycznymi dotyczącymi dostępności treści internetowych - WCAG.

Podsumowując, chcę podkreślić, że doceniamy wszelkie działania ze strony organizacji pozarządowych, które wzmacniają możliwości użytkowników Internetu w realizacji swoich praw. Celem wzmocnienia ochrony danych osobowych konieczna jest współpraca organów nadzorczych z sektorem prywatnym i pozarządowym, a wszelkie przedsięwzięcia, takie jak wskazana w petycji wtyczka Fundacji „Internet. Czas Działać!" o nazwie Rentgen czy opracowywana przez Fundację aplikacja Rentgendroid ułatwiają zagwarantowanie egzekwowalności przepisów RODO. Mając na uwadze powyższe, zorganizujemy robocze spotkanie konsultacyjne, podczas którego podsumujemy zgłoszone dotychczas stanowiska. Przekażemy informację i zaproszenie w odrębnej korespondencji oraz komunikacie.

Z wyrazami szacunku
wz. Dariusz Standerski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:

1. Prezes Urzędu Komunikacji Elektronicznej.
2. Prezes Urzędu Ochrony Danych Osobowych.

telefon: +48 22 245 54 42
adres email: sekretariat.BM@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa