Warszawa, 22-06-2022 r.

RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

VII.501.78.2022.MKS

Pan

Janusz Cieszyński

Sekretarz Stanu

Pełnomocnik Rządu do spraw Cyberbezpieczeństwa

ePUAP

Szanowny Panie Ministrze,

Ustawa z dnia 12 maja 2022 r. o zmianie ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa oraz ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. poz. 1087) rozpatrywana była przez Sejm RP w trybie pilnym. Z uwagi na pilny tryb uchwalenia ustawy Rzecznik nie miał możliwości przedstawienia swoich uwag w trakcie prac parlamentarnych, jednakże w ocenie Rzecznika ze względu na wysokie ryzyko jakie wiąże się z naruszeniem praw użytkowników projektowanego systemu – systemu, który dotyczy szczególnego rodzaju przetwarzania danych osobowych, związanego profilowaniem – a także z uwagi na pilotażowy charakter ustawy, która ma objąć w przyszłości również obywateli polskich (art. 2 ustawy), Rzecznik postanowił przedstawić Panu Ministrowi niniejsze uwagi, działając w tym zakresie na podstawie

Biuro Rzecznika Praw Obywatelskich
al. Solidarności 77
00-090 Warszawa

Tel. centr. (+48 22) 55 17 700
Infolinia obywatelska 800 676 676
biurorzecznika@brpo.gov.pl
bip.brpo.gov.pl

art. 16 ust. 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2020 r. poz. 627 ze zm.).

Będę wdzięczny za wzięcie pod uwagę przestawionego stanowiska również podczas projektowania przepisów wykonawczych do ustawy, czy projektowania samego systemu.

Ustawa przewiduje przygotowanie systemu teleinformatycznego (usługi online oraz mobilnej aplikacji) dla bezrobotnych obywateli Ukrainy, do którego dostęp mieliby pracodawcy. Ustawa opiera się na profilowaniu osób bezrobotnych i ma służyć ułatwienia nawiązywania kontaktów między pracodawcami a poszukującymi pracy. **Należy zatem na wstępie podkreślić, że idea stworzenia systemu, który ma służyć pomocą obywatelom Ukrainy w znalezieniu pracy zasługuje na aprobatę i uznanie, jednakże zdaniem Rzecznika Praw Obywatelskich istotne jest, aby prace nad tym systemem odbywały się z jednoczesnym należytym uwzględnieniem konstytucyjnego standardu ochrony prywatności i autonomii informacyjnej jednostki, a także były zgodne z wymogami rozporządzenia 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 (Dz. U. UE L. 119.1 ze sprost.; dalej; RODO).

1. W pierwszej kolejności pragnę zwrócić szczególną uwagę, że każdorazowo przy wprowadzaniu nowych technologii informatycznych istotna jest rola państwa w tworzeniu skutecznych mechanizmów ochrony danych osobowych. Kluczowym narzędziem wykazania, że wdrożono odpowiednie środki mające na celu wyeliminowanie czynników ryzyka związanego z przetwarzaniem danych, w tym związanego z zautomatyzowanym podejmowaniem decyzji, czy też profilowaniem, oraz wykazania zgodności z przepisami RODO, jest przeprowadzenie oceny skutków dla ochrony danych. **W uzasadnieniu ustawy brakuje natomiast informacji o przeprowadzonej ocenie skutków dla ochrony danych osobowych, do czego zobowiązuje wprost art. 35 ust. 3 RODO właśnie w odniesieniu do**

zautomatyzowanego przetwarzania, w tym profilowania, z którym mamy do czynienia w uchwalonej ustawie. Co natomiast istotne, wyniki oceny skutków dla ochrony danych mogą implikować konieczność przeprowadzenia uprzednich konsultacji z organem nadzorczym zgodnie z art. 36 ust. 1 RODO. Profilowanie jest bowiem szczególnym rodzajem przetwarzania danych osobowych, z którym mogą wiązać się zagrożenia dla praw i wolności osób, które są poddawane profilowaniu. Niezależnie jednak od powyższego, konieczność przeprowadzenia konsultacji z organem nadzorczym w przypadku projektowania przepisów dotyczących przetwarzania danych osobowych przewiduje również art. 36 ust. 4 RODO.

Należy przy tym podkreślić, że „ocena skutków dla ochrony danych powinna rozpocząć się jak najwcześniej w fazie projektowania operacji przetwarzania, nawet jeżeli niektóre operacje przetwarzania nadal są nieznane. Aktualizacja oceny skutków dla ochrony danych przez cały cykl trwania projektu zapewni uwzględnienie ochrony danych i prywatności oraz zachęci do tworzenia rozwiązań promujących zgodność. W miarę postępów procesu rozwoju konieczne może być również powtórzenie poszczególnych etapów oceny, ponieważ wybór niektórych środków technicznych lub organizacyjnych może wpłynąć na prawdopodobieństwo wystąpienia zagrożenia wynikającego z przetwarzania lub jego wagę[1].

Trzeba również przypomnieć, że **dotychczas Rzecznik wielokrotnie wskazywał, że ścisła współpraca Urzędu Ochrony Danych Osobowych m.in. z Ministerstwem Cyfryzacji, w zakresie przeprowadzania oceny skutków dla ochrony danych, jest kluczowa**[2]. Rzecznik zwracał przy tym uwagę, zarówno na zagrożenia związane z wdrażaniem nowych technologii, jak i – mając na względzie różny poziom kompetencji cyfrowych obywateli – **konieczność dołożenia starań, by prawa i obowiązki związane z korzystaniem z aplikacji były przystępnie wyjaśnione i żeby stosowne komunikaty dotarły do wszystkich zainteresowanych**.

---

[1] Zob. wytyczne grupy roboczej w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE[1]; dalej; wytyczne grupy roboczej w sprawie zautomatyzowanego podejmowania decyzji

[2] Zob. wystąpienie RPO w sprawie aplikacji Kwarantanna domowa https://bip.brpo.gov.pl/sites/default/files/Wystapienie_PRM_Minister_Cyfryzacji_12.11.2020.pdf

Mając na uwadze ryzyko związane ze stosowaniem systemów sztucznej inteligencji, w szczególności Rzecznik powoływał[3] projektowane rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji[4]. Należy w tym miejscu wskazać, że w motywie 36 projektu tego rozporządzenia wskazuje się, że systemy sztucznej inteligencji wykorzystywane w obszarze zatrudnienia, w szczególności do rekrutacji i wyboru kandydatów, (...) należy (...) klasyfikować jako systemy wysokiego ryzyka, ponieważ systemy te mogą w znacznym stopniu wpływać na przyszłe perspektywy zawodowe i źródła utrzymania tych osób. (...) W całym procesie rekrutacji oraz w ramach oceny, awansu lub retencji osób pozostających w umownych stosunkach pracy systemy takie mogą utrwalać historyczne wzorce dyskryminacji, na przykład wobec kobiet, niektórych grup wiekowych, osób z niepełnosprawnościami lub osób o określonym pochodzeniu rasowym lub etnicznym bądź określonej orientacji seksualnej.

Mając powyższe na uwadze, w ocenie Rzecznika, brak przeprowadzenia oceny skutków dla ochrony danych osobowych, a także brak konsultacji z organem do spraw ochrony danych osobowych, przy wprowadzeniu tak istotnych rozwiązań z punktu widzenia praw jednostki w trybie pilnym, może podważać zaufanie do organów państwa, w tym w zakresie stworzenia właściwych mechanizmów zapobiegającym naruszeniom prywatności.

2. Należy również wskazać, że w ustawie brak jest szczegółowych regulacji, w tym odnoszących się do kwestii techniczno-organizacyjnych, dotyczących tego jak system będzie funkcjonował. Ustawa nie przewiduje również upoważnienia do wydania rozporządzenia w tym obszarze.

W ustawie oraz w uzasadnieniu ustawy wskazuje się, że system ma na celu stworzenie profilu pracownika, poprzez udostępnienie jego danych osobowych

[3] Zob. wystąpienie RPO w sprawie Zintegrowanej Platformy Analitycznej: https://bip.brpo.gov.pl/pl/content/rpo-rozporzadzenie-rzadu-dane-osobowe-zintegrowana-platforma-analityczna

[4] Wniosek Komisji Europejskiej z dnia 21 kwietnia 2021 r. Projekt w brzmieniu skierowanym do zaopiniowania udostępniony został na stronie internetowej https://eur-lex.europa.eu/legalcontent/PL/TXT/PDF/?uri=CELEX:52021PC0206&from=PL.

(wieku, płci, wykształcenia, kwalifikacji zawodowych i przebiegu zatrudnienia, a także po wyrażeniu dodatkowej zgody, imienia, nazwiska, daty urodzenia, adresu poczty elektronicznej, nr telefonu) pracodawcom przedstawiającym oferty pracy. Co ważne, ustawodawca określił zasady uaktualniania, usuwania (art. 22d ust. 2 ustawy) i czasu przetwarzania danych (art. 22g ust. 2 ustawy), a także przewidział możliwość korzystania z systemu na zasadzie dobrowolności (art. 22d ust. 1 ustawy).

Należy jednak zauważyć, że ustawodawca nie sprecyzował tych regulacji. Ustawa nie określa kształtu, czy procedury profilowania. Jedynie w uzasadnieniu projektu ustawy wskazano, że „dzięki wdrożeniu odpowiednich rozwiązań teleinformatycznych osoba zainteresowana będzie w stanie zmapować swoje kompetencje oraz potrzeby i uzyskać informację zwrotną dotyczącą ofert pracy i danych kontaktowych do potencjalnych pracodawców". Z tego punktu widzenia, **wątpliwości budzi więc np. zakres żądanych danych**, trudno bowiem ustalić jakie konkretne dane będą przez użytkowników udostępniane, chociażby w celu wykazania kwalifikacji zawodowych (np. znajomość języka obcego). W praktyce może więc okazać się, że bezrobotny uzyska konkretne informacje o zakresie oczekiwanych od niego informacji dopiero w trakcie przeprowadzania wobec użytkownika czynności profilowania, a źródłem tych informacji nie będą wówczas akty powszechnie obowiązującego prawa.

Trzeba przy tym mieć na uwadze, jak wskazywał Trybunał Konstytucyjny w wyroku z dnia 6 czerwca 2018 r., w sprawie o sygn. akt K 53/16, wydanym na wniosek Rzecznika Praw Obywatelskich, który dotyczył profilowania osób bezrobotnych, że „profilowanie niewątpliwie oznacza „gromadzenie informacji" o jednostkach w rozumieniu art. 51 ust. 1 i 5 Konstytucji RP. Obejmuje ono zbieranie (pozyskiwanie) danych, ich przetwarzanie przez system komputerowy i utrwalanie w tym systemie w celu wykorzystania na kolejnych etapach pracy z bezrobotnym (...). W sferze tej powinna więc obowiązywać zasada wyłączności ustawowej w ustalonym wyżej rozumieniu – bezwzględnie w ustawie powinny znaleźć się kompletne regulacje dotyczące „zasad" i „trybu" przeprowadzenia profilowania (por. art. 51 ust. 5 Konstytucji), a pozostałe aspekty tej czynności mogą być dzielone między ustawę i rozporządzenie na zasadach wynikających z art. 31 ust. 3 i art. 92 ust. 1 Konstytucji".

Ponadto pojawiają się wątpliwości, **czy analizowane regulacje dotyczą automatycznego przetwarzania danych, o którym mowa w art. 22 ust. 1 RODO**. Wówczas na administratorze danych osobowych, w tym na prawodawcy, ciążą dodatkowe obowiązki związane z wdrożeniem właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, czy też zagwarantowanie prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania decyzji (art. 22 ust. 2 i 3 RODO).

Z wytycznych grupy roboczej w sprawie zautomatyzowanego podejmowania decyzji wynika zaś, że wymagane środki ochronne w przypadku zautomatyzowanego podejmowania decyzji, o którym mowa w art. 22 ust. 1 RODO, obejmują określone w art. 13 i 14 RODO prawo do otrzymania informacji (zwłaszcza istotnych informacji o zasadach podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą) oraz zabezpieczenia, takie jak prawo do uzyskania interwencji ludzkiej oraz prawo do zakwestionowania tej decyzji (określone w art. 22 ust. 3 RODO).

O ile w art. 22h ustawy przewidziano zapewnienie obowiązku informacyjnego wobec użytkowników, to jednak brak jest jakichkolwiek regulacji odnoszących się do zapewnienia odpowiednich zabezpieczeń w przypadku, gdy podstawę przetwarzania stanowią art. 22 ust. 2 lit. a) lub c) RODO (zob. art. 22 ust. 3 RODO).

Należy również wskazać, że Trybunał Konstytucyjny w postanowieniu sygnalizacyjnym z dnia 6 czerwca 2018 r., o sygn. akt S 3/18, odnoszącym się do regulacji dotyczących profilowania bezrobotnych (dotyczącym wyroku TK w sprawie o sygn. akt K 53/16), uznał, że „jeżeli (...) ustalenie profilu miałoby być wynikiem zautomatyzowanego przetwarzania danych, konieczne byłoby wprowadzenie dodatkowych środków ochrony praw bezrobotnych. (...) W opinii Trybunału Konstytucyjnego, ten aspekt profilowania wymaga w sposób konieczny regulacji ustawowej”.

Trzeba też podkreślić, że pomimo tego, że korzystanie z systemu jest dobrowolne, to jednak w przypadku profilowania istotny jest sposób realizacji obowiązku informacyjnego, tj. zapewnienie stosownych informacji na temat

planowanego wykorzystania danych oraz konsekwencji związanych z ich przetwarzaniem, tak, aby wyrażona **zgoda wynikała ze świadomej decyzji**. Informacje te można przekazać w połączeniu ze standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania (zob. motyw 60 RODO). Spełnienie tych wymogów jest istotne z punktu widzenia zasady przejrzystości (art. 5 ust. 1 pkt a RODO). Ponadto w doktrynie wskazuje się, że aby można było uznać, że został spełniony warunek wyrażenia wyraźnej zgody w związku z warunkami wskazanymi w art. 22 ust. 2 c RODO, w przypadku automatycznego podejmowania decyzji, niezbędna jest zgoda wyrażona poprzez oświadczenie woli podmiotu danych o odpowiedniej treści, z której wyraźnie wynika przyzwolenie na podjęcie decyzji w warunkach wyłącznie zautomatyzowanego przetwarzania danych osobowych, w tym profilowania (zob. komentarz do art. 22 RODO, red. M. Sakowska-Baryła, 2018, wydanie 1).

Należy przy tym zauważyć, że jak wynika z ustawy, system **przyznaje dostęp do danych szerokiemu kręgowi podmiotów** – tj. pracodawcom, podmiotom świadczącym usługi związane z udostępnieniem ofert pracy, a także podmiotom świadczącym usługi pośrednictwa między pracodawcami a osobami poszukującymi pracy (art. 22 f ustawy). Rodzi to dodatkowe zagrożenie dla prywatności związane z wyciekiem danych, a także dalszym przetwarzaniem/udostępnianiem danych w innym celu niż pierwotny.

Należy natomiast podkreślić, że w świetle art. 47 Konstytucji RP nie ulega wątpliwości, że ustawodawca ma konstytucyjny obowiązek zapewnić jednostce odpowiednią ochronę sfery prywatności nie tylko przed ingerencją ze strony podmiotów publicznych, ale również przed ingerencją ze strony innych jednostek i podmiotów prywatnych. Podkreślić również należy, że na podstawie norm zawartych w art. 47 i 51 Konstytucji RP można zrekonstruować po stronie jednostki publiczne prawo podmiotowe, do którego najważniejszych aspektów należy zaliczyć uzasadnione konstytucyjnie oczekiwanie jednostki w kwestii zgodnej z konstytucyjnym standardem regulacji przetwarzania informacji dotyczących jednostki przez państwo, pozwalającej jej na domaganie się ochrony w razie naruszenia jej sfery prywatnej, jak i bezpośredniej realizacji przez organy władzy publicznej prawa dostępu i korekty

zgromadzonych przez nie danych. Publiczne prawo podmiotowe ma również skutek horyzontalny, ponieważ w ramach jego realizacji powstają normy kształtujące relacje między jednostkami w dziedzinie przetwarzania danych osobowych. Oznacza to, że z prawem tym sprzężone jest prywatne prawo podmiotowe, związane z oczekiwaniami dotyczącymi ochrony prywatności informacyjnej w stosunkach prywatnoprawnych[5].

Istotna jest również okoliczność, że brak jest w ustawie regulacji dotyczących gwarancji zabezpieczenia gromadzonych danych osobowych (np. gwarancji, że dostęp do danych mają wyłącznie osoby zajmujące się kwestiami kadrowymi, czy rekrutacyjnymi), co rodzi dodatkowe zaniepokojenie Rzecznika z punktu widzenia poszanowania zasady integralności i poufności danych osobowych.

Należy przy tym zwrócić uwagę, że do konieczności uwzględnienia gwarancji proceduralnych i technicznych przetwarzania danych w regulacjach wprowadzających ograniczenia autonomii informacyjnej jednostki, Trybunał Konstytucyjny odniósł się w wyroku z dnia 20 stycznia 2015 r., sygn. akt K 39/12. Trybunał wskazał, że w wypadku ingerencji prawodawczej w autonomię informacyjną spełnienie wymogu proporcjonalności sensu stricto oznacza m. in.: a) istnienie ustawowo determinowanych gwarancji proceduralnych i technicznych bezpiecznego przetwarzania danych osobowych; b) ograniczenie katalogu podmiotów przetwarzających dane do minimum podyktowanego rodzajem danych i celem ich przetwarzania; c) określenie ram czasowych przetwarzania danych; d) wprowadzenie efektywnego mechanizmu anonimizacji; e) wprowadzenie przepisów umożliwiających stabilne finansowanie i konserwację baz danych celem zapewnienia ich niezakłóconego funkcjonowania w dobie dynamicznego rozwoju nowoczesnych technologii i różnego rodzaju ryzyka z tym związanego.

Mając powyższe na uwadze, należy podkreślić, że z perspektywy obowiązków nakładanych na podmioty tworzące, jak i wykorzystujące technologie oparte na sztucznej inteligencji, newralgiczne jest zapewnienie zgodności z podstawowymi zasadami przetwarzania danych, o których mowa w art. 5 RODO. Jak wskazuje się zaś w doktrynie, zasada legalności i rzetelności ma charakter nadrzędny i wymaga

[5] K. Łakomiec, Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia, WKP 2020.

wprowadzenia środków zapobiegających arbitralnemu, dyskryminującemu traktowaniu podmiotów danych. W konsekwencji wymaga implementacji rozwiązań i mechanizmów samouczących pozwalających wykluczyć z przetwarzania będącego podstawą decyzji dane niepoprawne, przetwarzane bezpodstawnie, czy w zakresie nieadekwatnym, a także takich, które zapewniają korektę czynników powodujących nieprawidłowości w danych osobowych i nakierowane będą na maksymalne zmniejszenie ryzyka błędów oraz zabezpieczenie danych osobowych w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą[6].

3. Ponadto Rzecznik zauważa, że **system teleinformatyczny, o którym mowa w ustawie, ma służyć osobom posiadającym nr PESEL**. Nr PESEL jest bowiem potrzebny do logowania i identyfikacji użytkownika, w ten sposób potwierdzenia się tożsamość osoby korzystającej z systemu. Weryfikacja tożsamości użytkownika, polega zaś na porównaniu danych wprowadzanych w procesie tworzenia profilu pracownika z danymi zawartymi w rejestrze PESEL (art. 22c ust. 2 i 3 ustawy). Aby móc skorzystać z usługi/aplikacji niezbędne jest więc posiadanie nr PESEL

Należy przy tym zwrócić uwagę, że zgodnie z art. 22 ust. 3 pkt 2 f ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa, przy rejestracji w Urzędzie Pracy, nr PESEL podaje bezrobotny obywatel Ukrainy, o ile go posiada. Natomiast zgodnie z art. 22 ust. 1 tej ustawy do wykonywania pracy na terytorium RP przez obywatela Ukrainy wymagane jest, aby: 1) jego pobyt na terytorium Rzeczypospolitej Polskiej uznany był za legalny na podstawie art. 2 ust. 1, lub aby 2) był obywatelem Ukrainy przebywającym legalnie na terytorium RP. Aktualnie nie ma więc obowiązku posiadania nr PESEL przy podejmowaniu legalnej pracy w Polsce wobec obywateli przybywających z Ukrainy w związku z wojną na terytorium ich kraju.

Wątpliwości budzi więc czy przyjęte rozwiązanie nie stanowi ograniczenia dla innych bezrobotnych obywateli Ukrainy, nieposiadających nr PESEL, w sytuacji gdy

[6] D. Lubasz, Zasady legalności, przejrzystości i minimalizacji danych w ogólnym rozporządzeniu o ochronie danych osobowych w kontekście sztucznej inteligencji [w:] Prawo sztucznej inteligencji, pod red. L. Lai, M. Świerczyńskiego, Warszawa 2020, s. 180 i n.

ustawa jest dedykowana właśnie obywatelom Ukrainy przebywającym na terytorium Polski w związku z konfliktem zbrojnym na ich terytorium kraju. Powstaje przy tym obawa, **czy system, który ma służyć rekrutacji pracowników (także przez organy państwowe, w tym przez Urząd Pracy) nie doprowadzi do wykluczenia (pozbawienia szans na znalezienie pracy) czy dyskryminacji pewnej grupy użytkowników**.

Ponadto Rzecznik dostrzega również zagrożenie w posługiwaniu się nr PESEL, który służący identyfikacji użytkownika w systemie. Należy bowiem zauważyć, że aktualnie nr PESEL, jest co raz bardziej powszechnie dostępny w różnych systemach/bazach publicznych, takich jak np. Krajowy Rejestr Sądowy, Krajowy Rejestr Zadłużonych, Elektroniczne Księgi Wieczyste, czy np. w certyfikacie podpisu elektronicznego. **Wykorzystywanie go zatem coraz częściej przez prawodawcę w celach identyfikacji osób fizycznych (a nie jedynie w celach ewidencyjnych, do jakich został on stworzony) w istocie rodzi ryzyko kradzieży tożsamości**, na co Rzecznik zwracał już wielokrotnie uwagę w korespondencji z PUODO[7].

Jednocześnie należy zauważyć, że art. 22b ust. 4 projektu ustawy przewiduje, że przedmiotowy system teleinformatyczny przyłączony jest do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 1 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2021 r. poz. 1797). W uzasadnieniu projektu ustawy wskazuje się przy tym, że „w celu zapewnienia realizacji ww. metody uwierzytelniania (logowania) użytkowników system zostanie przyłączony do węzła krajowego identyfikacji elektronicznej na podstawie przepisów ustawy, bez konieczności składania wniosku o przyłączenie w trybie określonym w ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej". Wydaje się zatem, że przedmiotowy system ma zostać przyłączony do węzła krajowego jedynie w celu potwierdzenia tożsamości użytkownika. W przypadku jednak, gdyby doszło do udostępnienia przetwarzanych danych do węzła krajowego

[7] Zob. np. https://bip.brpo.gov.pl/pl/content/rzecznik-wystapil-w-sprawie-ochrony-danych-osobowych-pracownikow-sadow;
https://bip.brpo.gov.pl/pl/content/rpo-kazdy-moze-w-sieci-poznac-dane-osobowe-z-ksiag-wieczystych
https://bip.brpo.gov.pl/pl/content/pracownicy-sanepidu-musza-miec-profil-zaufany-do-celow-sluzbowych-interwencja-rpo-u-puodo

pojawiają się dodatkowe wątpliwości z związane z kręgiem podmiotów, któremu miałoby nastąpi udostępnienie danych osobowych oraz i celem w jakim miałyby być one być dalej przetwarzane.

Co ważne, powielanie w innym miejscu zebranych uprzednio danych i zestawianie ich z innymi zestawami danych, które także uprzednio zebrane zostały w innym celu jest niezgodne z zasadą minimalizacji danych oraz zasadą ograniczenia celu[8]. Należy również podkreślić, że zgodnie z motywem 31 RODO, **żądanie ujawnienia danych osobowych, z którym występują organy publiczne** (...) **nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych**. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

4. Na marginesie powyższych uwag, należy zwrócić uwagę, że motyw 41 RODO wskazuje, że wybór formy i sposobu uchwalenia przepisów dotyczących przetwarzania danych osobowych zależy od konstytucyjnych zasad tworzenia prawa danego państwa, a ponadto, przewiduje, że przepisy powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających. Należy zaś wskazać, że ustawa została uchwalona w trybie pilnym, bez koniecznych konsultacji, a w wielu kwestiach budzi wątpliwości. Co również istotne, art. 3 i 4 ustawy przewiduje zaś, że ustawa wchodzi w życie po ogłoszeniu, jednak w praktyce dopiero z chwilą ogłoszenia komunikatu o uruchomieniu usługi – który nie został ustawowo określony. Na komisji senackiej zgłoszono zaś uwagę, że „żaden z przepisów ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych nie daje możliwości publikowania komunikatów w Dzienniku Ustaw. Takiej możliwości nie dopuszcza się nawet fakultatywnie[9]".

Mając powyższe na uwadze, działając na podstawie art. 16 ust. 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich, przedstawiam niniejsze uwagi Panu

[8] Zob. powołane już powyżej wystąpienie RPO dot. zintegrowanej platformy analitycznej.
[9] Zob. art. 9 tej ustawy; https://www.senat.gov.pl/prace/posiedzenia/tematy,576,1.html

Ministrowie, jednocześnie prosząc o przedstawienie wyjaśnień w niniejszej sprawie i odniesienie się do przedstawionych uwag.

Z wyrazami poważania,

Marcin Wiącek
Rzecznik Praw Obywatelskich
/-podpisano elektronicznie/

Do wiadomości:

Pan Jan Nowak

Prezes

Urzędu Ochrony Danych Osobowych

ePUAP