PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

Warszawa, dnia 29 marca 2023 r.

Pan
Jacek Chlebny
Prezes
Naczelnego Sądu Administracyjnego
ul. Boduena 3/5
00-011 Warszawa

Szanowny Panie Prezesie,
w związku z wyrokiem Naczelnego Sądu Administracyjnego z dnia 9 lutego 2023 r. (sygn. akt III OSK 3945/21) Prezes Urzędu Ochrony Danych Osobowych, zwany dalej również Prezesem UODO, wyraża głębokie zaniepokojenie niebezpiecznym kierunkiem w jakim zmierza dokonana przez NSA interpretacja kompetencji i pozycji ustrojowej organu nadzorczego, niezgodna z treścią i celem przepisów prawa Unii Europejskiej, tj. Traktatu o funkcjonowaniu Unii Europejskiej (Dz.U.UE.C.2016.202.47), Karty praw podstawowych Unii Europejskiej (Dz. U. UE. C. z 2007 r. Nr 303, str. 1 ze zm.), 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35), zwanego dalej RODO, jak również wyrokami Trybunału Sprawiedliwości Unii Europejskiej.

Powołane orzeczenie w sposób niezaprzeczalny i precedensowy kwestionuje niezależność organu nadzorczego, jak i podważa jego kompetencje oraz kwalifikacje merytoryczne zatrudnionych w nim osób, niezbędne do wykonywania zadań, do których organ ten został powołany.

Z orzeczenia wynika wprost, iż przyczyną uchylenia decyzji Prezesa UODO było oddalenie przez organ wniosku o przeprowadzenie dowodu z opinii biegłego na okoliczność ustalenia standardów technicznych i organizacyjnych środków bezpieczeństwa oraz oceny czy środki techniczne i organizacyjne stosowane przez spółkę odpowiadały standardom środków bezpieczeństwa w działalności gospodarczej przedsiębiorców w obszarze e-commerce o skali i charakterze podobnym do skali i charakteru działalności tejże spółki.

W powołanym orzeczeniu NSA wyraża wątpliwość czy z uwagi na precedensowy charakter sprawy, związany ze skalą naruszenia poufności danych osobowych i rozmiarem działalności skarżącej kasacyjnie spółki, przetwarzającej dane osobowe ponad 2.200.000 użytkowników, Prezes UODO posiada „wiadomości specjalne" do samodzielnej oceny, czy stosowane przez nią środki techniczne i organizacyjne były odpowiednie. Jak wskazał cyt.: „(...) należy poddać w wątpliwość, czy organ - w dacie wydania zaskarżonej decyzji - posiadał własną wiedzę specjalistyczną, pozwalającą na ocenę odpowiedniości środków technicznych i organizacyjnych w działalności gospodarczej o tak dużej skali (...)", a także cyt.: „(...) wątpliwe wydaje się, czy organ w swojej dotychczasowej praktyce prowadził postępowania w zbliżonej kategorii spraw, co pozwalałoby na ustalenie odpowiedniego do charakteru, zakresu i kontekstu przetwarzania standardu środków bezpieczeństwa (...)", konkludując cyt.: „(...) Wskazane we wniosku dowodowym Morele.net okoliczności miały istotne znaczenie dla sprawy, a zatem wniosek o przeprowadzenie dowodu z opinii biegłego winien zostać przez Prezesa UODO uwzględniony (...)".

Twierdzeniami tymi NSA bezsprzecznie kwestionuje kompetencje i niezależność Prezesa UODO jako organu nadzorczego, podczas gdy niezależność ta ma swoje źródło w pierwotnym prawie Unii Europejskiej, tj. w art. 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.U.UE.C.2016.202.47) i art. 8 ust. 3 Karty praw podstawowych Unii Europejskiej (Dz. U. UE. C. z 2007 r. Nr 303, str. 1 ze zm.), gdzie wskazane zostało wprost, że przestrzeganie zasad przetwarzania danych osobowych podlega kontroli niezależnych organów.

Jak wskazuje się w piśmiennictwie cyt.: „(...) Wymóg niezależności organu nadzorczego wywodzi się z art. 28 ust. 1 dyrektywy 95/46/WE, ma również oparcie w przepisach traktatowych, stąd należy przyjąć, że regulacja prawna zawarta w art. 52 RODO stanowi kontynuację regulacji ją poprzedzającej. Prawodawca unijny uznał wymóg niezależności organu nadzorczego za niezwykle istotny, dlatego znacznie bardziej szczegółowo uregulował te kwestie w komentowanym przepisie (...)" (por. P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 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] [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II, Warszawa 2022, art. 52, Opublikowano: WKP 2022).

Niezależność ta jest zagwarantowana art. 52 ust. 1 RODO, zgodnie z którym każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem działa w sposób w pełni niezależny, która to całkowita niezależność do wypełniania zadań i wykonywania uprawnień jest zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (por. motyw 117 RODO). Owa niezależność przejawia się również w dysponowaniu przez organ nadzorczy własnym personelem, który jest dobierany przez ten organ nadzorczy (por. motyw 121 RODO, art. 52 ust. 4 i 5 RODO).

Prawodawca unijny wyszedł bowiem z założenia, że organ nadzorczy może prawidłowo realizować swoje zadania jedynie wówczas, gdy będzie miał

zagwarantowaną niezależność. Wymóg niezależności odnosi się do wypełniania zadań i wykonywania uprawnień organu nadzorczego. Osoby pełniące funkcje organu powinny mieć możliwość samodzielnego decydowania o działaniach, które są podejmowane w ramach pełnionej funkcji. Niezależność powinna oznaczać brak podległości organizacyjnej, ochronę przed uleganiem wpływom czy naciskom ze strony innych organów oraz swobodę w podejmowaniu rozstrzygnięć nadzorczych (por. op. cyt. powyżej).

Jak wynika z art. 52 ust. 2 RODO, jednym z wymogów, jakie stanowić mają gwarancję niezależności organu nadzorczego, jest niepodleganie wpływom zewnętrznym, a także zakaz zwracania się o instrukcje oraz zakaz przyjmowania instrukcji od innych podmiotów. Z kolei, jak wynika z art. 52 ust. 4 RODO, istotnym elementem, mającym wpływ na niezależność organu nadzorczego, jest dysponowanie zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędnymi do skutecznego wypełniania swoich zadań i wykonywania swoich uprawnień umożliwiającymi organowi realizację jego zadań.

Dodatkowe wymogi odnoszą się do personelu zatrudnionego w urzędzie obsługującym organ nadzorczy. Zgodnie z przepisem ust. 5 komentowanego artykułu, państwo członkowskie powinno zapewnić, by każdy organ nadzorczy wybierał i posiadał własny personel, działający pod wyłącznym kierownictwem członka lub członków danego organu nadzorczego. Wymóg ten ma stanowić kolejną gwarancję niezależności organu, gdyż korzystanie z „cudzych zasobów kadrowych" może pociągać za sobą wątpliwości co do niezależności organu (por. op. cyt. powyżej).

Ponadto Trybunał Sprawiedliwości Unii Europejskiej, zwany dalej TSUE, wielokrotnie podkreślał wagę niezależności organu ds. ochrony danych osobowych wskazując, iż ta niezależność wyklucza nie tylko jakikolwiek wpływ ze strony instytucji kontrolujących, lecz również jakiekolwiek nakazy i jakikolwiek inny wpływ z zewnątrz, bez względu na to, czy bezpośredni, czy pośredni, który mógłby podważyć wykonywanie przez te organy ich zadań polegających na ustaleniu słusznej równowagi pomiędzy ochroną prawa do poszanowania życia prywatnego a swobodą przepływu danych osobowych. Jak wskazywał TSUE, rola strażników prawa do poszanowania życia prywatnego, jaką wypełniają organy nadzorcze, wymaga, by ich decyzje, a tym samym one same, pozostawały poza jakimkolwiek podejrzeniem stronniczości. Określenie „niezależny" oznacza zwykle status, który zapewnia danemu organowi możliwość w pełni swobodnego działania, z wyłączeniem jakichkolwiek instrukcji czy nacisków. Pojęcie „niezależny" zostało wzmocnione przysłówkiem „całkowicie", co oznacza, że uprawnienia decyzyjne wyłączone są spod jakiegokolwiek wpływu spoza organu kontroli, bez względu na to, czy pośredniego, czy bezpośredniego. Natomiast niezależność funkcjonalna organów nadzorczych, w tym znaczeniu, że ich członkowie nie są związani żadnymi instrukcjami w zakresie wykonywanych przez siebie funkcji, stanowi warunek konieczny (por. wyrok Trybunału z 6 października 2015 r. w sprawie C-362/14, MAXIMILLIAN SCHREMS v. DATA PROTECTION COMMISSIONER, ZOTSiS 2015, nr 10, poz. I-650;

wyrok Trybunału z 9 marca 2010 r. w sprawie C-518/07 - Komisja/Niemcy, http://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=PL&mode=doc&dir=&occ=first&part=1&cid=745626;
wyrok Trybunału (wielka izba) z dnia 8 kwietnia 2014 r. w sprawie C-288/12 - Komisja/Węgry, https://curia.europa.eu/juris/document/document.jsf?text=&docid=150641&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=8062595;
wyrok Trybunału (wielka izba) z dnia 16 października 2012 r. w sprawie C-614/10 Komisja/Austria, https://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=8062539).

Tymczasem NSA w ww. wyroku z dnia 9 lutego 2023 r. (sygn. akt III OSK 3945/21) kategorycznie przesądzając, że w sprawie cyt.: „(...) Zarzuty {kasacyjne} (...) zasługują na uwzględnienie w części dotyczącej arbitralnej oceny materiału dowodowego na skutek samodzielnego, tj. bez przeprowadzenia dowodu z opinii biegłego, określenia przez Prezesa UODO, iż stosowane przez skarżącą środki techniczne nie były odpowiednie (...)", a co za tym idzie cyt.: „(...) wniosek o przeprowadzenie dowodu z opinii biegłego winien zostać przez Prezesa UODO uwzględniony (...)", całkowicie pomija istnienie powyższych norm unijnych i ugruntowanego stanowiska TSUE, co do niezależności Prezesa UODO jako organu właściwego w sprawie ochrony danych osobowych (art. 34 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. z 2019 r. poz. 1781) i organu nadzorczego (art. 51 ust. 1 RODO), podważając jego kompetencje i posiadanie wiedzy specjalistycznej do oceny środków technicznych i organizacyjnych stosowanych w systemach informatycznych.

Wysoce dotkliwe, a jednocześnie jaskrawo sprzeczne z zasadami racjonalnego rozumowania są twierdzenia NSA, że cyt.: „(...) Prezes UODO rozstrzygał sprawę w oparciu o nowy stan prawny. Organ nie mógł skutecznie powołać się na wiedzę specjalistyczną pracowników urzędu, skoro odnosiła się ona do poprzedniego stanu prawnego, w ramach którego nie stosowano rozwiązania takiego jak w art. 32 RODO (...)", a w związku z tym zdaniem NSA organ powinien skorzystać z opinii biegłego posiadającego taką wiedzę specjalistyczną. Idąc tokiem myślenia zaprezentowanym przez NSA, stosując zasady racjonalnego rozumowania, należałoby dojść do wniosku, że skoro wiedza specjalistyczna w zakresie środków bezpieczeństwa systemów informatycznych pozyskana przed rozpoczęciem stosowania RODO jest nieprzydatna do oceny tych środków na gruncie art. 32 RODO, to zasada ta dotyczy nie tylko pracowników urzędu, ale także jakichkolwiek ekspertów w tej dziedzinie, spośród których organ mógłby powołać biegłego, a tym samym nie sposób, w dacie wydania decyzji, byłoby wskazać w Polsce jakiegokolwiek eksperta, który ze względu na krótki okres stosowania RODO posiadałby wystarczającą wiedzę specjalistyczną pozwalającą na występowanie w charakterze biegłego w niniejszej sprawie.

Podkreślenia wymaga, iż personel zatrudniany przez Prezesa UODO, a wcześniej przez Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej GIODO, ma bowiem blisko dwudziestopięcioletnie doświadczenie w kontroli

i prowadzeniu postępowań wobec podmiotów przetwarzających dane osobowe w systemach informatycznych, które to doświadczenie jest systematycznie wzbogacane, w szczególności poprzez odbywanie przez pracowników organu specjalistycznych kursów, szkoleń, potwierdzanych stosownymi certyfikatami. W tym właśnie okresie wytworzona została unikalna wiedza instytucjonalna organu, na której bazują wszyscy jego pracownicy, a która daje gwarancję posiadania wiedzy specjalistycznej pozwalającej na samodzielną ocenę stosowania środków technicznych i organizacyjnych w systemach informatycznych bez konieczności korzystania z pomocy biegłego. Ponadto, wbrew twierdzeniom NSA, dokonywana przez Prezesa UODO ocena stosowania środków technicznych i organizacyjnych na gruncie RODO nie jest żadnym novum w stosunku do oceny dokonywanej na gruncie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 ze zm.) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024), które to oceny w związku z kontrolami wielokrotnie były przeprowadzane. Przepisy ustawy o ochronie danych osobowych z 1997 r. stanowiły bowiem implementację dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, str. 31, ze zm.), której art. 28 przewidywał wprowadzenie przez administratora danych odpowiednich środków technicznych i organizacyjnych zwłaszcza w celu ochrony danych osobowych przed niedozwolonym ujawnieniem lub dostępem, szczególnie wówczas gdy przetwarzanie danych obejmowało transmisję danych w sieci, natomiast przepisy RODO w tym zakresie stanowią wyłącznie kontynuację przyjętych w dyrektywie 95/46/WE rozwiązań, kontrolowanych już przez Prezesa UODO. Co więcej, przepisy RODO, jakkolwiek mają zastosowanie od dnia 25 maja 2018 r., to jednak weszły w życie z dniem 24 maja 2016 r. (por. art. 99 RODO), co dało organom nadzorczym dwuletni okres czasu na przygotowanie do jego stosowania, a zwłaszcza na weryfikację dotychczasowych uregulowań prawnych i praktyki pod kątem jego rozwiązań. Z powyższych względów stwierdzenia NSA zawarte w ww. wyroku jakoby cyt.: „(...) Prowadząc postępowanie administracyjne i wydając we wrześniu 2019 r. decyzję o nałożeniu kary pieniężnej. Prezes UODO rozstrzygał sprawę w oparciu o nowy stan prawny (...)" są zatem błędne. Podkreślenia przy tym wymaga, że mimo iż wskazana argumentacja organu była NSA znana, spotkała się wyłącznie z jego lakonicznym stwierdzeniem cyt.: „(...) Okoliczności te pozostają bez znaczenia dla sprawy, zważywszy na skalę działalności Morele.net i związaną z nią specyfikę stosowanych środków zabezpieczenia danych osobowych ponad dwóch milionów klientów (...)".

Co istotne, NSA przed wejściem w życie RODO nie kwestionował kompetencji pracowników Biura GIODO do kontroli i prowadzenia postępowania wobec podmiotów przetwarzających dane w systemach informatycznych, w tym w strategicznych z punktu widzenia interesów państwa systemach np. rejestru PESEL. Przykładowo, NSA w wyroku z dnia 3 grudnia 2021 r. (sygn. akt III OSK 590/21) oddalił skargę Ministra

Cyfryzacji na decyzję GIODO, w której organ nakazał m. in. zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, o których była mowa w art. 36 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. NSA nie miał też wątpliwości, że GIODO posiadał kompetencje do badania wymiany danych pomiędzy systemami Ministra Finansów i Prezydenta Miasta Stołecznego Warszawy, oddalając skargę Ministra Finansów wyrokiem z dnia 27 października 2017 r. (sygn. akt I OSK 3192/15). Ponadto, należy zauważyć, że ustawodawca wprost nakłada na organ ochrony danych obowiązek przeprowadzania kontroli w zakresie działania systemów, w których przetwarzane są dane osobowe takich jak np. System Informacyjny Schengen, Wizowy System Informatyczny, Krajowy System Informatyczny PNR, które to kontrole były przeprowadzane.

W świetle powyższego wysoce krzywdzące są zatem wątpliwości NSA wyrażone w ww. wyroku z dnia 9 lutego 2023 r. (sygn. akt III OSK 3945/21) dotyczące tego cyt.: „(...) czy organ - w dacie wydania zaskarżonej decyzji - posiadał własną wiedzę specjalistyczną, pozwalającą na ocenę odpowiedniości środków technicznych i organizacyjnych w działalności gospodarczej o tak dużej skali (...)", a także cyt.: „(...) czy organ w swojej dotychczasowej praktyce prowadził postępowania w zbliżonej kategorii spraw, co pozwalałoby na ustalenie odpowiedniego do charakteru, zakresu i kontekstu przetwarzania standardu środków bezpieczeństwa (...)". Prezes UODO ma bowiem „wiadomości specjalne" wymagane do oceny czy środki techniczne i organizacyjne stosowane przez spółkę odpowiadały standardom środków bezpieczeństwa w działalności gospodarczej przedsiębiorców w obszarze e-commerce o skali i charakterze podobnym do skali i charakteru działalności tejże spółki, potwierdzone dotychczasową praktyką. W sprawie będącej przedmiotem rozstrzygnięcia NSA, owe „wiadomości specjalne" niewątpliwie zostały wykorzystane, co znalazło swój wyraz w szczególności w dokumentacji z przeprowadzonej w spółce kontroli, jak np. w protokołach kontroli wskazujących na dokładne zbadanie przez specjalistów organu stosowanych przez spółkę środków technicznych i organizacyjnych w jej systemach informatycznych.

Niezależnie od powyższego, należy zwrócić uwagę, iż NSA ww. orzeczeniem całkowicie pominął prawa ponad 2.200.000 użytkowników, których dane osobowe zostały naruszone wskutek działalności spółki, a którzy ponosić mogą również i dotkliwe konsekwencje związane z uzyskaniem nieuprawnionego dostępu do ich danych. Nie budzi wątpliwości, że wyciek danych osobowych może wiązać się z utratą haseł dostępu do rozmaitych serwisów internetowych, np. e-bankowości, profilu zaufanego czy portali społecznościowych. Kradzież wirtualnej tożsamości stwarza sprawcom dogodne warunki, aby wykorzystać uzyskane dane do własnych celów, jak np. wyczyszczenie konta internetowego z prywatnych oszczędności, wykupienie usługi na koszt poszkodowanego czy zaciągnięcie pożyczki w aplikacji mobilnej banku. Konsekwencje powyższe najwyraźniej umknęły NSA, podczas gdy prawa osób, których dane dotyczą, winny być istotną wartością w rozpatrywanej sprawie, zwłaszcza, że organ podkreślił, iż w stanie faktycznym przedmiotowej sprawy ryzyko dotyczyło zagrożenia polegającego na zastosowaniu metody zwanej phishingiem, mającej na celu

wyłudzenie danych, m.in. uwierzytelniających do konta bankowego poprzez podszycie się pod spółkę w wiadomościach SMS i wykorzystanie faktu dokonania zamówienia przez klienta.

Reasumując, Prezes UODO, w związku z wyrokiem Naczelnego Sądu Administracyjnego z dnia 9 lutego 2023 r. (sygn. akt III OSK 3945/21), zwracając uwagę na aspekty tej sprawy budzące jego poważne zaniepokojenie, jednocześnie wyraża głębokie przekonanie, że wskazane w niniejszym piśmie kwestie zostaną uwzględnione w praktyce orzeczniczej. Jest to o tyle istotne, że funkcjonowanie w obrocie prawnym ww. prawomocnego orzeczenia rodzi niebezpieczeństwo powielania zaprezentowanego w nim wadliwego stanowiska, a co za tym idzie, powstania szkodliwej dla osób, których dane dotyczą, linii orzeczniczej. Przyjęcie bowiem stanowiska NSA wyrażonego w ww. wyroku, kwestionującego kompetencje Prezesa UODO i podważającego jego niezależność, za słuszne, w praktyce oznaczałoby uniemożliwienie organowi samodzielnego funkcjonowania i rozstrzygania spraw z zakresu ochrony danych osobowych w systemach informatycznych służących do przetwarzania danych i prowadziłoby do pozbawienia skutecznej ochrony praw osób, których dane są przetwarzane, zagwarantowanej przepisami Traktatu o funkcjonowaniu Unii Europejskiej, Karty praw podstawowych Unii Europejskiej i RODO.

Z wyrazami szacunku,

Prezes Urzędu Ochrony Danych Osobowych
Jan Nowak