PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 28 sierpnia 2024 r.

DOL.0623.10.2024

Pani
Agnieszka Bartol-Saurel
Sekretarz Stanu
Kancelaria Prezesa Rady Ministrów

Szanowna Pani Minister,

w odpowiedzi na pismo z 1 sierpnia br. dotyczące przedstawienia stanowiska w przedmiocie zasadności udziału Polski w postępowaniu w sprawie **C-422/24** *Storstockholms Lokaltrafik* (ochrona danych osobowych – prawo do informacji i dostępu do danych osobowych pozyskiwanych przy użyciu kamery nasobnej) informuję, że w ocenie Prezesa Urzędu Ochrony Danych Osobowych (dalej jako Prezes Urzędu), udział Polski w tym postępowaniu **jest zasadny**. Poniżej przedkładam uzasadnienie tego stanowiska.

We wniosku prejudycjalnym w sprawie C-422/24 *Storstockholms Lokaltrafik* (ochrona danych osobowych – prawo do informacji i dostępu do danych osobowych pozyskiwanych przy użyciu kamery nasobnej) przedstawiony został stan faktyczny, który polegał na wyposażeniu kontrolerów biletów w kamery nasobne i używaniu tych kamer podczas kontroli osób nie posiadających ważnego biletu, co wiązało się z uiszczeniem opłaty dodatkowej. Kamery były wykorzystywane w celu zapobiegania groźbom i aktom przemocy wobec kontrolerów biletów oraz dokumentowania takich sytuacji, a także w celu weryfikowania tożsamości pasażerów zobowiązanych do uiszczenia opłaty

dodatkowej. Ustalono, że kontrolerzy biletów nosili kamery nasobne przez całą zmianę roboczą. Kamery te w sposób ciągły nagrywały filmy zawierające obraz i dźwięk. Początkowo zarejestrowany materiał był przechowywany przez dwie minuty, ale w toku audytu nadzorczego czas ten skrócono do jednej minuty. Naciśnięcie przycisku przez kontrolera biletów wstrzymywało działanie funkcji automatycznego usuwania, co zapewniało, że nagranie nie zostanie skasowane. W takiej sytuacji w kamerze przechowywane były także informacje zapisane z wykorzystaniem funkcji wcześniejszego nagrywania, tj. materiał zarejestrowany w minucie poprzedzającej naciśnięcie przycisku przez kontrolera. Kontrolerom biletów polecono wstrzymywać działanie funkcji automatycznego usuwania zawsze, gdy nakładają opłatę dodatkową, a także w przypadku kierowania wobec nich gróźb.

W toku przeprowadzonego postępowania pojawiła się wątpliwość czy w przypadku, gdy dane osobowe są pozyskiwane przy użyciu kamery nasobnej, zastosowanie znajduje art. 13 czy też art. 14 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 (dalej: rozporządzenie 2016/679)[1]. Pytanie prejudycjalne zatem brzmi **czy w przypadku, gdy dane osobowe są pozyskiwane przy użyciu kamery nasobnej, zastosowanie znajduje art. 13 czy też art. 14 rozporządzenia 2016/679?**

Jednym z głównych obowiązków nałożonych na administratorów danych osobowych przez rozporządzenie 2016/679 jest obowiązek informacyjny, który w określonych sytuacjach musi być spełniony w stosunku do osoby, której dane dotyczą. Prawodawca unijny w znacznej mierze rozszerzył katalog informacji, jakie należy przekazać takiej osobie. Osoby, których dane dotyczą mają prawo do uzyskania szerokiego wachlarza informacji na temat samego administratora oraz przetwarzania ich danych osobowych przez tego administratora. W motywie 60 preambuły rozporządzenia 2016/679 zostało wskazane, że osoba, której dane dotyczą, musi być poinformowana o prowadzeniu operacji przetwarzania jej danych osobowych oraz o celach takiego przetwarzania. Ponadto, administrator powinien podać wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.

Rozporządzenie 2016/679 nakazuje spełnianie obowiązku informacyjnego w dwóch przypadkach: w momencie, gdy dane zbierane są bezpośrednio od osoby, której one dotyczą (art. 13 rozporządzenia 2016/679) oraz w sytuacji gromadzenia danych ze źródeł pośrednich, tj. nie od osoby, której one dotyczą (art. 14 rozporządzenia 2016/679). W przypadku zbierania danych od osoby, której dane dotyczą, rozporządzenie 2016/679 nie określa dokładnie sposobu ani formy za pomocą której takie informacje powinny być udzielone, jednak jasno określa, że za zastosowanie „właściwych środków" dotyczących spełnienia obowiązku informacyjnego odpowiada administrator danych (art.13 rozporządzenia 2016/679). Należy więc stwierdzić, że wymagane prawem informacje powinny zostać przekazane osobie, której dane dotyczą albo w momencie zbierania

[1] Dz. Urz. UE L 119 z 4.5.2016

danych osobowych (najpóźniej w chwili ich zebrania), albo bezpośrednio przed ich zebraniem. Dla spełnienia obowiązku informacyjnego nie ma znaczenia sposób w jaki te dane zostaną zebrane.

Zgodnie z art. 14 ust. 3 lit. a oraz motywem 61 preambuły rozporządzenia 2016/679, jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła należy poinformować ją o tym w rozsądnym terminie, jednak nie później niż w ciągu miesiąca. Natomiast jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą, obowiązek informacyjny powinien zostać spełniony najpóźniej przy pierwszej takiej komunikacji. Natomiast jeżeli administrator planuje ujawnić dane osobowe innemu odbiorcy, to będzie on zobowiązany poinformować o tym osobę, której dane dotyczą już w momencie pierwszego ujawnienia tych danych odbiorcy (art. 14 ust. 3 lit. c rozporządzenia 2016/679).

Obowiązek informacyjny należy spełnić w przypadku zbierania danych osobowych bezpośrednio lub pośrednio od osoby, której dane dotyczą (odpowiednio zgodnie ze wspomnianymi z art. 13 oraz 14 rozporządzenia 2016/679). Rozporządzenie 2016/679 nie wprowadziło definicji pojęcia zbierania danych osobowych. Można przyjąć, że jest to zestaw operacji składających się na przetwarzanie danych osobowych takich jak każde wejście w posiadanie tych danych wraz z zamiarem ich dalszego przetwarzania, bez względu na to, czy dane będą przetwarzane w zbiorze danych osobowych. Istotnym w tej sytuacji jest sam fakt pozyskania danych osobowych, drugorzędne znaczenie ma czy te dane zostały przekazane samodzielnie przez osobę, której dane dotyczą z jej własnej inicjatywy, czy też zostały pozyskane w inny sposób – obowiązek informacyjny w takich sytuacjach zawsze powinien zostać spełniony.

W przedmiotowej sprawie C-422/24 Storstockholms Lokaltrafik dotyczącej przetwarzania danych osobowych podczas używania kamer nasobnych przez kontrolerów biletów sąd apelacyjny odniósł się do wyroku w sprawie C-212/13 Ryneš[2], który dotyczył monitoringu wizyjnego prowadzonego przez osobę prywatną przy użyciu ustawionej w stałej pozycji kamery stacjonarnej. Trybunał orzekł, że mającym zastosowanie przepisem jest norma będąca dawnym odpowiednikiem art. 14 rozporządzenia 2016/679. Z brzmienia art. 13 rozporządzenia 2016/679 wynika, że aby można było przyjąć, że dane osobowe zostały zebrane od osoby, której dane dotyczą, konieczny jest jakiś rodzaj celowego działania ze strony tej osoby. Nie można uznać, że jest tak w przypadku, w którym dane osobowe są pozyskiwane przy użyciu przedmiotowych kamer nasobnych. Brzmienie tego przepisu w związku z wyrokiem Trybunału świadczy o tym, że art. 13 rozporządzenia 2016/679 nie znajduje zastosowania w takiej sytuacji. Szwedzki organ nadzorczy natomiast stwierdził, że przepisem, który znajduje zastosowanie w niniejszej sprawie jest właśnie art. 13 rozporządzenia 2016/679. Szwedzki organ nadzorczy, wskazał, że z czysto językowego punktu widzenia brzmienie tego artykułu wskazuje, że to administrator, a nie osoba, której dane dotyczą, ma być zaangażowany w zbieranie danych osobowych. Jego brzmienie nie stoi na przeszkodzie stosowaniu tego artykułu nawet w przypadku braku aktywnego uczestnictwa osoby, której dane dotyczą. Motyw 60 rozporządzenia 2016/679

[2] Wyrok Trybunału z dnia 11 grudnia 2014 r. w sprawie C-212/13, František Ryneš, EU:C:2014:2428.

przewiduje, że jeżeli gromadzi się dane osobowe od osoby, której dane dotyczą, należy ją też poinformować, czy ma ona obowiązek je podać oraz o konsekwencjach ich niepodania. Taką informację podaje się jednak wyłącznie wówczas, gdy jest to wymagane w konkretnym przypadku, w związku z czym brzmienia motywu 60 rozporządzenia 2016/679 nie należy interpretować w ten sposób, iż wprowadza on wymóg, zgodnie z którym dla zastosowania art. 13 rozporządzenia 2016/679 niezbędne jest, we wszystkich przypadkach, rzeczywiste działanie ze strony osoby, której dane dotyczą. Ponadto, szwedzki organ nadzorczy zaznaczył, że w niniejszej sprawie nie jest tak, że osoba, której dane dotyczą, nie podejmuje żadnego świadomego działania. Ponieważ w przypadku korzystania z monitoringu wizyjnego informacje muszą być podane przed rozpoczęciem przetwarzania danych osobowych, tym, kto umożliwia zbieranie danych osobowych, jest osoba, której dane dotyczą, ponieważ świadomie wchodzi ona na teren objęty monitoringiem. Artykuł 14 rozporządzenia 2016/679 odnosi się do sytuacji, w których dane osobowe są pozyskiwane w sposób inny niż od osoby, której dane dotyczą. W motywie 61 rozporządzenia 2016/679 wskazano, że oznacza to pozyskiwanie danych osobowych bezpośrednio z innego źródła. Ponadto art. 14 ust. 2 rozporządzenia 2016/679 stanowi, że należy podać informacje o źródle pochodzenia danych osobowych. Wszystko to sugeruje, że ów artykuł ma zastosowanie w sytuacjach, w których dane osobowe są pozyskiwane od podmiotu zewnętrznego lub ze źródła zewnętrznego. Nie można uznać, że jest tak w przypadku monitoringu wizyjnego prowadzonego przez samego administratora. Inne istotne różnice między art. 13 a art. 14 rozporządzenia 2016/679 dotyczą momentu, w którym należy podać informacje, jak również możliwości zwolnienia z obowiązku podawania informacji. W razie przyjęcia, że art. 14 rozporządzenia 2016/679 ma zastosowanie do monitoringu wizyjnego istnieje ryzyko, iż administratorzy będą interpretować przepisy rozporządzenia 2016/679 w ten sposób, że informacje nie muszą być podawane ani w obrębie terenu objętego monitoringiem, ani po jego opuszczeniu. Monitoring wizyjny stanowi, co do zasady, przetwarzanie danych osobowych o charakterze istotnym z punktu widzenia życia prywatnego, w przypadku którego zasadniczo istnieje szczególny interes w tym, aby osoby, których dane dotyczą, otrzymywały informacje, co świadczy o tym, że art. 14 rozporządzenia 2016/679 nie został pomyślany jako przepis mający ogólne zastosowanie do monitoringu wizyjnego.

W ocenie Prezesa Urzędu uznanie, że w przypadku korzystania z kamery nasobnej pozyskuje się dane osobowe osoby, której dane dotyczą z innego źródła niż ona sama, nie jest w żaden sposób uzasadnione. Co więcej, prowadziłoby do wniosku, że podczas pozyskiwania danych osobowych z monitoringu wizyjnego można zrezygnować z informacji o tym monitoringu na rzecz informowania osób, których dane dotyczą w późniejszym terminie. Takie rozwiązanie wydaje się niedopuszczalne.

W związku z powyższym, Prezes Urzędu stoi na stanowisku, że w przypadku przetwarzania danych osobowych pozyskiwanych przy użyciu monitoringu wizyjnego, w tym kamery nasobnej, zastosowanie będzie miał art. 13 rozporządzenia 2016/679.

W tym miejscu należy wspomnieć o Wytycznych Europejskiej Rady Ochrony Danych (dalej: EROD) 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo z dnia 29 stycznia 2020 r.[3] (dalej: Wytyczne). Zgodnie z pkt. 110 Wytycznych, osoby, których dane dotyczą należy poinformować w sposób szczegółowy o miejscach objętych monitoringiem. Zgodnie z RODO ogólne obowiązki w zakresie przejrzystości i obowiązki informacyjne określono w art. 12 RODO i nn. Wytyczne Grupy Roboczej art. 29 w sprawie przejrzystości na mocy rozporządzenia 2016/679 (WP260)[4], które zostały zatwierdzone przez EROD w dniu 25 maja 2018 r., dostarczają dalszych szczegółów. Zgodnie z WP260 pkt 26 art. 13 RODO ma zastosowanie, w przypadku gdy dane osobowe pozyskiwane są „[...] od osoby, której one dotyczą, poprzez obserwację (np. wykorzystując urządzenia zautomatyzowanego przechwytywania danych lub oprogramowania do przechwytywania danych, takich jak kamery [...]".

W polskim prawie krajowym nie ma przepisów, które wprost regulowałyby używanie kamer nasobnych przez kontrolerów biletów. Takie użycie nie jest również zakazane. W tym miejscu należy również wskazać na przepisy potwierdzające, że monitoring wizyjny (w tym używanie kamer nasobnych) dotyczy zbierania danych osobowych od osoby, której dane dotyczą. Zgodnie z art. 22^2 Kodeksu pracy[5], jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring), a pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem. W przypadku wprowadzenia monitoringu pracodawca oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem. Ustawodawca wprost wskazuje, że postanowienie dotyczące oznaczenia miejsca monitorowanego nie narusza przepisu art. 13 rozporządzenia 2016/679. Odnosząc się już bezpośrednio do użycia kamer nasobnych, które mogą być stosowane przez służby państwowe, zgodnie z art. 15c ustawy z dnia 6 kwietnia 1990r. o Policji[6], w określonych przypadkach zastosowania rejestrowania obrazu i dźwięku, z wyłączeniem działań kontrterrorystycznych oraz wspierania działań jednostek organizacyjnych Policji przez służbę kontrterrorystyczną w warunkach szczególnego zagrożenia lub wymagających użycia specjalistycznych sił i środków oraz specjalistycznej taktyki działań, funkcjonariusz Policji w miarę możliwości uprzedza osobę, wobec której podejmuje czynności, o rejestrowaniu obrazu lub dźwięku. Podobnie w przypadku Służby Granicznej – zgodnie z art. 11 ust. 2f ustawy z dnia 12 października

[3] Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo, 29 stycznia 2020 r. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pl.pdf
[4] Wytyczne Grupy Roboczej art. 29 w sprawie przejrzystości na mocy rozporządzenia 2016/679 (WP260), w wersji polskiej: https://archiwum.uodo.gov.pl/pl/3/1343
[5] Dz. U. z 2023 r. poz. 1365.
[6] Dz. U. z 2024 r. poz. 145.

1990r. o Straży Granicznej[7] w określonych przypadkach, funkcjonariusz Straży Granicznej w miarę możliwości uprzedza osobę, wobec której podejmuje czynności, o rejestrowaniu obrazu lub dźwięku. Ponadto, zgodnie z art. 11 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych związku z realizowanymi zadaniami straży przysługuje prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych w przypadku, gdy czynności te są niezbędne do wykonywania zadań oraz w określonych celach[8]. Rozporządzeniem Rady Ministrów z dnia 16 grudnia 2009 r.[9] wskazano sposób wykonywania powyższych czynności, uwzględniając potrzebę zapewnienia skuteczności obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, a także potrzebę respektowania godności ludzkiej oraz przestrzegania i ochrony praw człowieka.

Nie ma wątpliwości, że użycie kamer nasobnych stanowi formę monitoringu wizyjnego. Ze względu na fakt, że monitoring wizyjny jest inwazyjną formą przetwarzania danych osobowych i jako taki powinien podlegać szczególnej weryfikacji przez administratora, Prezes Urzędu wydał Wskazówki dotyczące monitoringu wizyjnego[10]. We wspomnianym dokumencie wskazane zostało, że jednym z istotnych zadań administratora danych, który wprowadził przetwarzanie danych osobowych z użyciem monitoringu wizyjnego, jest realizacja wobec osoby obserwowanej obowiązku informacyjnego ujętego w art. 13 rozporządzenia 2016/679. Musi on być, zgodnie z art. 12 rozporządzenia 2016/679, realizowany w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część z wymienianych powyżej przepisów szczególnych wskazuje dodatkowo znaki lub ogłoszenia dźwiękowe, którymi należy oznaczyć pomieszczenia i teren monitorowany (w/w przepisy Kodeksu pracy i Prawa oświatowego). Pełna informacja o monitoringu, obejmująca wszystkie wymogi z art. 13 rozporządzenia 2016/679, powinna być dostępna w miejscu monitorowanym, np. na tablicach albo w formie dokumentu dostępnego na recepcji czy też u przedstawiciela administratora. **Możliwa jest zatem realizacja obowiązku informacyjnego poprzez podanie informacji podstawowych i uzupełnienie ich w kolejnych warstwach informacyjnych**. **Obowiązek informacyjny w przypadku przetwarzania danych za pomocą kamery nasobnej może zostać spełniony, np. poprzez odpowiednie oznakowanie.**

Należałoby również rozważyć argumenty i stanowisko drugiej strony, a więc Spółki AB Storstockholms Lokaltrafik, a następnie szwedzkiego sądu apelacyjnego. Zgodnie z tym stanowiskiem warunkiem zastosowania art. 13 rozporządzenia 2016/679 jest intencjonalne, celowe działanie podmiotu danych co do podania informacji na swój temat. Przy zbieraniu informacji za pomocą kamery nasobnej (i innych podobnych urządzeń) mamy do czynienia z sytuacją, w której inicjatywa zebrania danych osobowych od osoby, której dane dotyczą, leży po stronie administratora. Dodatkowo, w przedstawionym w pytaniu prejudycjalnym stanie faktycznym nie wskazano na czym się oparto przyjmując,

[7] Dz. U. z 2024 r. poz. 915.
[8] Dz. U. z 2021 r. poz. 1763.
[9] Dz. U. Nr 220 poz. 1720.
[10] Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego, czerwiec 2018, https://uodo.gov.pl/data/filemanager_pl/1200.pdf

że osoby nagrywane przez kontrolerów biletów za pomocą kamer nasobnych wiedziały, że wchodzą w obszar monitorowany za ich pomocą, czyli świadomie podejmują decyzje o udostępnieniu swoich danych.

Mając na względzie powyższe, w ocenie Prezesa Urzędu, **udział Polski w przedmiotowym postępowaniu jest zasadny, ponieważ orzeczenie Trybunału może mieć wpływ na stosowanie prawa krajowego.**

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym-/