



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Jan Nowak

Warszawa, 26-09-2019

ZSPU.023.231.2019

Pan

Marek Zagórski

Minister Cyfryzacji

ul. Królewska 27

00-060 Warszawa

elektroniczna skrzynka podawcza ePUAP

/MAiC/SkrytkaESP

Szanowny Panie Ministrze,

w związku z trwającymi pracami nad projektem **rozporządzenia Ministra Cyfryzacji w sprawie aplikacji mobilnej służącej do rozliczania opłaty za przewóz osób**, dalej: projekt rozporządzenia, skierowanym do uzgodnień przez Ministra Cyfryzacji w dniu 12 września 2019 r., organ nadzorczy przedstawia opinię w sprawie projektu rozporządzenia z punktu widzenia przepisów 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 04.05.2016, str. 1, z późn. zm.¹⁾), dalej: RODO. Jednocześnie wskazuję, że projekt rozporządzenia nie został skierowany do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych.

Projektowane rozporządzenie jest wydawane na podstawie art. 13b ust. 4 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2019 r. poz. 58, z późn. zm.), zgodnie z którym minister właściwy do spraw informatyzacji w porozumieniu z ministrem właściwym do spraw transportu oraz ministrem właściwym do spraw finansów publicznych określi, w drodze rozporządzenia:

1) minimalne wymagania funkcjonalne dla aplikacji mobilnej oraz aplikacji mobilnej działającej przy udziale systemu teleinformatycznego,

¹⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

2) sposób zabezpieczenia danych gromadzonych przez aplikację mobilną oraz system teleinformatyczny

– mając na uwadze potrzebę prawidłowego naliczania opłat za przewóz osób oraz zabezpieczenia danych gromadzonych przez aplikację mobilną.

Biorąc pod uwagę tak ukształtowaną delegację ustawową wątpliwości organu nadzorczego budzi szereg zapisów rozporządzenia dot. przetwarzania danych osobowych.

W pierwszej kolejności należy wskazać na § 2 pkt 2 projektu rozporządzenia, który mówi ogólnie o funkcjonalności aplikacji mobilnej polegającej na gromadzeniu danych dotyczących usługi przewozowej, bez szczegółowego wskazania o jakie dane chodzi i czy w sformułowaniu tym mieszczą się także dane osobowe. Powyższy zapis narusza zasadę przejrzystości określoną w art. 5 ust. 1 lit. a RODO, zgodnie z którą dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

Zastrzeżenia budzi także § 3 pkt 2 lit. b projektu rozporządzenia, zgodnie z którym aplikacja mobilna w ramach funkcjonalności gromadzenia danych dotyczących usługi przewozowej zapewnia możliwość identyfikacji klienta. Nie jest wiadomym przy pomocy jakich danych identyfikacja ta miałaby być przeprowadzana. Czy byłoby to tylko imię i nazwisko, czy też także inne dane, takie jak adres IP osoby korzystającej z aplikacji mobilnej, numer karty bankowej czy też numer PESEL (podlegający szczególnej ochronie na gruncie art. 87 RODO)? Powyższy zapis również narusza wyżej wspomnianą zasadę przejrzystości.

Zasadę przejrzystości narusza także § 3 pkt 3 lit. e projektu rozporządzenia. Zgodnie z projektowanym przepisem, w ramach rejestracji danych o realizowanej usłudze przewozowej odbywać się będzie rejestracja incydentów uniemożliwiających realizację usługi przewozowej. Projektodawca, nie wskazał jakie dane oraz dotyczące jakich osób będą przetwarzane w ramach rejestracji tych incydentów.

Szczególne zaniepokojenie organu nadzorczego budzi § 3 pkt 4 projektu rozporządzenia, zgodnie z którym aplikacja mobilna zapewnia możliwość kontroli, przez uprawnione podmioty, w dowolnym czasie, zarejestrowanych danych dotyczących realizowanej usługi. Nie wiadomo jakie uprawnione podmioty projektodawca ma tutaj na myśli oraz z czego ich uprawnienie miałyby wynikać. Wskazać należy również na bardzo szeroki zakres danych, do których podmioty te miałyby dostęp – bo dotyczących zarówno identyfikacji przewoźnika, kierowcy i klienta, jak również pokonanej odległości, lokalizacji startowej i docelowej przewozu, czasu jego trwania, opłaty za przewóz oraz istotnych incydentów oraz wydarzeń, które miały miejsce w jego trakcie. Daje to nieokreślonej kategorii podmiotów (w tym służbom i inspekcjom) uprawnienie do dostępu do bardzo szczegółowych informacji o osobie korzystającej z usługi przewozowej. Zwrócić należy również uwagę, że przepis nie mówi czemu owa kontrola uprawnionych podmiotów miałaby służyć, tym samym dając w praktyce możliwość przeprowadzania kontroli operacyjnej, która będzie mogła być

dokonywana w dowolnym czasie i nie będzie w żaden sposób odnotowywana. Godzi to w art. 51 ust. 1 i 2 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którym nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby oraz stanowiącym, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Nieograniczony tryb dostępu podmiotów publicznych do danych gromadzonych przez aplikację mobilną narusza również motyw 31 RODO, mówiący, że ujawnianie danych podmiotom publicznym powinno mieć co do zasady charakter wnioskowy (odbywać się w formie pisemnej, być uzasadnione i mieć charakter wyjątkowy). Przepis w projektowanym kształcie jest również niezgodny z zasadą minimalizacji danych określoną w art. 5 ust. 1 lit. c RODO, zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Nie bez znaczenia jest również fakt, że pozyskiwanie tak szerokiego i specyficznego spektrum danych o osobach korzystających z aplikacji mobilnej (częstotliwość przejazdów, dane o geolokalizacji czy wysokość opłaty za przejazd) z łatwością może posłużyć do tworzenia profili osobowych jej użytkowników.

Należy również zwrócić uwagę, że zarówno ustawa z dnia 6 września 2001 r. o transporcie drogowym, jak i projektowane rozporządzenie, nie regulują kto miałby być administratorem danych gromadzonych przez aplikację mobilną oraz na jakim etapie i w jakim zakresie miałby za nie odpowiadać. Brak wskazania administratora danych, bądź kryterium jego wyznaczenia, uniemożliwia *de facto* zrealizowanie delegacji ustawowej z art. 13b pkt 2 ustawy z dnia 6 września 2001 r. o transporcie drogowym, gdyż nie wiadomo kto miałby odpowiadać za zabezpieczenie danych gromadzonych przez aplikację mobilną.

Wprowadzenie tak silnie ingerującego w prywatność rozwiązania cyfrowego, jak regulowana projektowanym rozporządzeniem aplikacja mobilna, powinno zostać poprzedzone oceną skutków dla ochrony danych, której projektodawca nie przeprowadził. Projektowane rozporządzenie związane jest z funkcjonowaniem systemów teleinformatycznych, więc projektodawca przy tworzeniu tego typu przepisów prawnych powinien pamiętać o uwzględnieniu ochrony danych w fazie projektowania oraz domyślnej ochrony danych (*Data protection by design and by default* – art. 25 RODO), a także oceny skutków dla ochrony danych (*Data protection impact assessment* – art. 35 RODO). W kontekście art. 35 ust. 10 RODO dokonanie oceny skutków dla ochrony danych powinno się odbyć już w ramach oceny skutków regulacji projektowanego rozporządzenia. Każdy system przetwarzania danych wykorzystujący mechanizmy teleinformatyczne wymaga analizy w zakresie oceny wpływu, która powinna uwzględniać nie tylko wpływ zastosowanej technologii na ochronę danych osobowych osób, których dane mają być przetwarzane ale również interesy zaangażowanych stron z punktu widzenia transparentności wykonywanych operacji. Zgodnie z art. 35 ust. 1 RODO, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia

praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Zgodnie z art. 35 ust. 7 RODO ocena skutków zawiera co najmniej: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania; ocenę, czy operacje są niezbędne oraz proporcjonalne w stosunku do celów; ocenę ryzyka naruszenia praw lub wolności podmiotów danych; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych.

Nieprzeprowadzenie wyżej wspomnianej oceny skutków dla ochrony danych narusza prawa i wolności osób, których dane będą przetwarzane przez regulowaną projektowanym rozporządzeniem aplikację mobilną.

Z wyrazami szacunku,
Prezes Urzędu Ochrony Danych Osobowych
Jan Nowak
/ - podpisano elektronicznie/