Systemy biletowe muszą lepiej chronić dane pasażerów

4 czerwca 2024

Kolejne miasta wdrażają lub opracowują nowe systemy płatności za komunikację miejską. Mają one przede wszystkim być proste i wygodne w obsłudze, ale przy pełnym bezpieczeństwie danych pasażerów. „Systemy biletowe muszą być skonstruowane w taki sposób, by nie naruszały prywatności pasażerów i właściwie chroniły ich dane osobowe. Mogą one być cennym łupem dla przestępców" – podkreśla Konrad Komornicki, zastępca prezesa Urzędu Ochrony Danych Osobowych. To istotne zwłaszcza w kontekście wchodzącej w życie w październiku dyrektywy NIS2, która zaostrza unijne przepisy dotyczące cyberbezpieczeństwa.

W lutym 2023 roku z poważnym atakiem mierzył się system Śląskiej Karty Usług Publicznych, która była wówczas głównym nośnikiem biletów komunikacji miejskiej w Górnośląsko-Zagłębiowskiej Metropolii. Z kolei pod koniec czerwca ubiegłego roku atak hakerski sparaliżował działanie systemu w Olsztynie, przez co miasto uruchomiło czasową sprzedaż specjalnych biletów papierowych, również okresowych. Utrudnienia trwały kilka miesięcy.

„Mieliśmy w kraju przypadki dużych awarii systemów biletowych. Jedno z miast wojewódzkich prawie miesiąc podnosiło się po awarii, poniosło przy tym bardzo duże koszty nie tylko finansowe, ale i wizerunkowe" – mówi agencji Newseria Konrad Komornicki. „Do tej pory w mojej ocenie systemy biletowe w komunikacji miejskiej działają sprawnie. Nie mamy zgłoszeń co do wycieku danych, awaryjności, bardziej jest to jakiś błąd ludzki, polegający na tym, że te dane nie tam zostały przesłane, gdzie trzeba, ale nie chodzi o cały system biletowy".

Nad nowym systemem biletowym pracuje m.in. Warszawa. Zgodnie z

zapowiedziami władz miasta ma być gotowy za dwa–trzy lata. Umożliwi opłatę za przejazd za pomocą karty płatniczej, telefonu, smartwatcha i karty miejskiej, ale także zaplanowanie podróży. Nowy system biletowy jest wdrażany także na Pomorzu, z kolei mieszkańcy Wrocławia już płacą za przejazdy w nowoczesny sposób. Operatorzy systemów podkreślają, że bez względu na zastosowane w nich technologie muszą one być przede wszystkim wygodne i łatwe w obsłudze. Ważne jest jednak, by nie naruszały prywatności użytkowników i zapewniały skuteczną ochronę danych osobowych.

Ważne jest też prawidłowe przeprowadzenie oceny skutków dla ochrony danych przy wdrażaniu w komunikacji nowoczesnych rozwiązań, w których mają być przetwarzane dane pasażerów. „Jest bardzo duża pokusa i to widać przy zastosowaniu nowych technologii, w dobie rozwijającej się sztucznej inteligencji, jak również w dobie dużej pokusy w przetwarzaniu naszych danych biometrycznych. Musimy reagować na bieżąco, prowadzić działalność edukacyjną, działalność wskazującą pewne ryzyka, jeśli chodzi o przetwarzanie danych. To administrator decyduje, jakie środki techniczno-organizacyjne i regulacyjne wprowadzi u siebie" – przypomina ekspert UODO.

Podmioty projektujące i wdrażające nowoczesne systemy biletowe muszą się stosować do wskazanych w RODO zasad privacy by design i privacy by default. Dzięki temu już na etapie planowania zostanie uwzględniona ochrona danych przetwarzanych w ramach takich rozwiązań, co znacznie ułatwi zapewnienie odpowiedniego poziomu bezpieczeństwa.

„Administrator takiego systemu nie może przetwarzać danych bez wyraźnej zgody osoby, której te dane dotyczą. Innymi słowy, nie może podejmować operacji na tych danych, jeśli nie było wyraźnej zgody osoby, której te dane dotyczą" – zauważa Konrad Komornicki. „Jeszcze 16 lat temu w jednym z dużych miast była funkcjonalność zbierania danych z kasownika, jeśli chodzi o wejścia, wyjścia, gdzie było to spersonalizowane. Ta funkcja decyzją Generalnego Inspektora Ochrony Danych Osobowych

została wyłączona”.

Przedstawiciel UODO przypomina, że wszyscy organizatorzy i operatorzy systemów biletowych muszą brać pod uwagę kwestie związane z ochroną danych osobowych. Administrator musi przeprowadzić ocenę skutków nowego systemu dla prywatności użytkowników, stwierdzić, czy pobierane dane są adekwatne, jakie są systemy zabezpieczeń, jak szacować ryzyka. Administratorzy muszą również uwzględnić, jakie prawa mają osoby, których dane będą przetwarzane. Jakakolwiek zmiana i operacja zmiany danych wymaga zgody użytkownika.

„Wszelkie regulaminy i instrukcje powinny być rzetelne, czyli powinny być pisane językiem zrozumiałym dla każdego pasażera, powinny być prawdziwe i aktualne. Dzięki temu odbiorca takiego systemu, pasażer, będzie miał łatwość i przyswajalność pewnych regulacji i jego praw, które wynikają z przetwarzania jego danych osobowych” – ocenia zastępca prezesa UODO.

Przestrzeganie bezpieczeństwa danych jest istotne zwłaszcza w kontekście dyrektywy NIS2, która zaostrza unijne przepisy dotyczące cyberbezpieczeństwa. Wprowadza większe wymagania w zakresie zarządzania, ujawniania luk w zabezpieczeniach, testowania poziomu cyberbezpieczeństwa oraz wykorzystania szyfrowania. Dyrektywa weszła w życie w 2023 roku, a do 18 października 2024 roku wszystkie podmioty muszą się do niej dostosować.

„Jeśli chcesz mieć pokój, szykuj się do wojny, w tym przypadku, jak chcesz mieć bezpieczny system biletowy, szykuj się na atak hakerów. Dane przetwarzane przez jednostki samorządu terytorialnego, w tym przypadku mówimy o operatorze transportu, to dane, w których pozyskiwany jest PESEL do wyrobienia spersonalizowanej karty miejskiej, ale również inne dane wrażliwe. To bardzo cenny łup dla cyberprzestępców” – podkreśla Komornicki.

Z jednej strony potrzebna jest taka budowa systemu, która

będzie minimalizować ryzyka. Z drugiej strony – konieczna jest odpowiednia świadomość konsumentów. Jak wynika z badania „Wiedza na temat bezpieczeństwa ochrony danych osobowych w Polsce" przeprowadzonego na zlecenie ChronPESEL.pl i Krajowego Rejestru Długów, o tym, jakie działania należy podjąć w przypadku kradzieży danych osobowych, wie niespełna 56 proc. respondentów. W przypadku wycieku danych z serwisu lub aplikacji, w której ma się konto, tylko 45 proc. ich posiadaczy wiedziałoby, jak się zachować.

„Mieliśmy przykład dużej akcji w internecie, szczególnie na portalach społecznościowych, cyberprzestępców podszywających się między innymi przez jednego z operatorów transportu w celu wyłudzenia środków finansowych. Sprawna akcja samego operatora, jak również świadomość odbiorców aplikacji pokazała, że ta akcja na szczęście nie okazała się sukcesem cyberprzestępcy" – mówi ekspert UODO.

Źródło: Newseria.pl