Jaka branża, takie obowiązki

W ciągu minionego roku wiele branż stanęło przed problemami związanymi ze specyfiką ich działalności. Wątpliwości sprowadzały się najczęściej do podstawowych kwestii, takich jak dopuszczalność zbierania czy udostępniania danych i właściwego określenia podstawy ich przetwarzania. Jednak nie zawsze rozwiązania były jednoznaczne.

Na podstawie dotychczasowych doświadczeń wybraliśmy przykłady problemów z zakresu ochrony danych osobowych, które mają miejsce na co dzień, a mimo to wiążą się z dużymi wątpliwościami.

Imię i nazwisko podróżnego na bilecie internetowym

Spore wątpliwości budzi zasadność zbierania przez internet danych osobowych, których przewoźnicy nie zbierają na tradycyjnych biletach kupowanych w kasie lub w automatach. Dodatkowo w przypadku zakupu biletów dla kilku osób, dane zbierane są tylko od jednego podróżnego.

Z punktu widzenia ochrony danych osobowych zbieranie nadmiernych danych (które nie są konieczne do realizacji przejazdu) może stanowić naruszenie art. 5 ust. 1 lit. c RODO. Przewoźnicy jako powód zbierania danych wskazują konieczność zabezpieczenia biletów internetowych przed ich fałszowaniem. Jeżeli ten cel pozwala osiągnąć QR kod umieszczany na bilecie, to taka argumentacja może okazać się niewystarczająca.

Kontrola dokumentów tożsamości w pojazdach komunikacji

W teorii samo patrzenie na dane osobowe nie stanowi formy ich przetwarzania. Jednak aby stosować w tym przypadku wymogi dotyczące ochrony wynikające z RODO, dane powinny stanowić część zbioru. Kontroler, który weryfikuje dokument tożsamości potwierdzający uprawnienia do przejazdu lub zniżki od ceny biletu, nie zbiera tych danych – nie trafiają więc do żadnego zbioru. W związku z tym kontrola nie powinna budzić wątpliwości co do dopuszczalności na gruncie RODO.

Inaczej będzie w przypadku, kiedy kontroler wystawi kwit za przysłowiową jazdę na gapę. Taki obowiązek ciąży na przewoźnikach w transporcie publicznym zgodnie z prawem transportowym. GIODO w 2005 r. uznał takie działanie za przetwarzanie w celu realizacji obowiązku wynikającego z przepisu prawa. Stan prawny się zmienił, ale wnioski wciąż są aktualne także na gruncie RODO. Zatem podróżny powinien być o tym właściwie poinformowany.

Dane o stanie zdrowia w reklamacjach

Podstawy przetwarzania danych osobowych wrażliwych, m.in. o stanie zdrowia, są na dużą skalę ograniczone. Przedsiębiorcom najbardziej brakuje możliwości przetwarzania danych wrażliwych w związku z zawieraniem umów z osobami z niepełnosprawnościami.

Ten problem dobrze znają firmy z branży usług medycznych. Innym przedsiębiorcom ta kwestia często umyka, a jak się okazuje, nierzadko pojawia się konieczność przetwarzania takich danych. Dotyczy to również przewoźników, którzy otrzymują wnioski o przejazd osoby niepełnosprawnej czy reklamacje związane z jej prawem do ulgi. Administratorzy

mają niewielki wybór w zakresie podstaw przetwarzania takich danych – w zależności od specyfiki swojej działalności mogą próbować oprzeć przetwarzanie na względach związanych z ważnym interesem publicznym, co w przypadku transportu publicznego ma zastosowanie w obowiązkach dotyczących praw podróżnych. W przeciwnym razie pozostaje tylko i wyłącznie zbieranie zgody.

Udostępnianie danych pomiarowych

Przedsiębiorstwa energetyczne prowadzą działalność w oparciu o szereg danych, w tym danych pomiarowych. Warto pamiętać, że numer licznika czy też wielkość zużycia energii mogą stanowić dla nich dane osobowe, ponieważ na ich podstawie można ustalić, kogo dotyczą. Dane te są zbierane przede wszystkim na potrzeby wykonania zawartej umowy. Nie można zapominać, że ich wymiana między dystrybutorem a sprzedawcą może opierać się na dodatkowych podstawach prawnych, ponieważ są przetwarzane także w celu zapewnienia dystrybucji na potrzeby umowy kompleksowej, zawarcia umowy sprzedaży rezerwowej czy przeciwdziałania nielegalnemu poborowi energii. Jedno jest pewne – nie ma potrzeby zbierania dodatkowych oświadczeń odbiorcy o zgodzie dla podanego zakresu przetwarzania. Przedsiębiorstwa energetyczne nadal często posługują się pojęciem zgody. Poszczególne podstawy przetwarzania powinny być jasno określone w obowiązku informacyjnym – co w dalszym ciągu nie zawsze ma miejsce.

Dane pomiarowe a inteligentne liczniki

Firmy z branży energetycznej skierowały swoje działania ku wdrażaniu tzw. inteligentnych liczników, które stanowią kopalnię danych osobowych. Do końca 2026 r. mają one stanowić 80 proc. wszystkich urządzeń pomiarowych. Urządzenia te zbierają dane o zużyciu z dużo większą częstotliwością niż standardowe liczniki. Pozwalają nie tylko ustalić profil zużycia, ale również zbierać informacje o działającym w domu sprzęcie.

Przetwarzanie danych przez inteligentne liczniki wymaga szczególnie wnikliwej oceny bezpieczeństwa. Firmy energetyczne muszą obowiązkowo sporządzić i udokumentować ocenę skutków dla ochrony danych przetwarzanych w tych urządzeniach.

Monitoring infrastruktury bez informacji o przetwarzaniu

W obszarze monitoringu, RODO nakłada obowiązek informowania osób, których dane dotyczą, o zasadach przetwarzania ich danych. Dotyczy to również wizerunku nagranego kamerą.

Przedsiębiorcy mogą monitorować swój teren ze względów bezpieczeństwa, co jest ich uzasadnionym interesem prawnym. Mają jednak obowiązek umieścić piktogramy i informacje o zasadach przebiegu monitorowania.

Co w sytuacji, gdy kamera ma nagrać z ukrycia złodzieja? Incognito nagrywać mogą nie tylko organy ścigania. Nowe krajowe przepisy wprowadzające RODO taką możliwość, bez konieczności informowania nagrywanych osób, stworzyły dla podmiotów świadczących usługi detektywistyczne. Firmy, które planują same wykrywać nieprawidłowości, muszą właściwie oznaczyć każde monitorowane miejsce.

Formalne wymogi przetwarzania w chmurze

Firmy, które przechowują swoje dane w chmurze, muszą pamiętać, że w takiej sytuacji zazwyczaj dochodzi do powierzenia przetwarzania danych osobowych firmie, która udostępnia serwery. Część dostawców usług stosuje ustandaryzowane wzory postanowień, które są narzucane użytkownikom. Dlatego niezbędne jest zweryfikowanie, czy zapisy umowy są akceptowalne.

Dodatkowo chmura, w której następuje przepływ danych, może dopuszczać przetwarzanie danych w państwie trzecim. O takim przetwarzaniu muszą być poinformowane osoby, których dane dotyczą. Dodatkowo, jeżeli serwer jest zlokalizowany poza Europejskim Obszarem Gospodarczym (EOG), należy sprawdzić, czy Komisja Europejska uznała taki kraj za bezpieczny (np. Kanada czy Japonia), czy trzeba zastosować dodatkowe zabezpieczenia.

Wyjście Wielkiej Brytanii z Unii Europejskiej

Przedsiębiorcy współpracujący z firmami z Wielkiej Brytanii muszą wziąć pod uwagę, że z momentem bezumownego Brexitu kraj ten stanie się państwem trzecim, który nie należy do Europejskiego Obszaru Gospodarczego. Oznacza to, że udostępnianie danych osobowych do firm, które prowadzą działalność na jego terenie, będzie wymagało zastosowania mechanizmów ochrony danych osobowych wskazanych w RODO. W pierwszej kolejności – standardowych klauzul umownych zatwierdzonych przez Komisję Europejską. Jest to zresztą zgodne z rekomendacją Urzędu Ochrony Danych Osobowych. O czym należy pamiętać w tej sytuacji? Niewątpliwie o fakcie, że dane przekazywane do Wielkiej Brytanii należy zidentyfikować już teraz, a także przygotować scenariusz działania na każdą z możliwych opcji Brexitu.

Autorzy:

Daniel Dudek, prawnik, Kancelaria Prawna Piszcz i Wspólnicy sp.k.

Jakub Pieniak, prawnik, Kancelaria Prawna Piszcz i Wspólnicy sp.k.