Sprawozdanie z działalności PUODO w 2020 r. – cz. III

W ramach pierwszej części omawiania sprawozdania z działalności Prezesa Urzędu Ochrony Danych Osobowych („UODO") w roku 2020 („Sprawozdanie") podsumowane zostały informacje statystyczne dotyczące skarg i naruszeń, jak również najczęstsze typy naruszeń ochrony danych osobowych zgłaszanych do organu. Część druga zawiera omówienie wybranych skarg wpływających do PUODO na podmioty z sektora publicznego. W ostatniej – trzeciej części omawiam natomiast wybrane skargi wnoszone do PUODO na podmioty z sektora prywatnego.

Przetwarzanie wizerunku utrwalonego za pomocą monitoringu wizyjnego

Jedna ze skarg wskazanych w Sprawozdaniu dotyczyła kwestii utrwalania, przeglądania oraz przesłania przez wspólnotę mieszkaniową do członków zarządu wspólnoty, w wiadomościach e-mail, danych osobowych skarżącego w postaci wizerunku, w związku z funkcjonującym na terenie nieruchomości wspólnej wspólnoty systemem monitoringu wizyjnego. Wspólnota wskazywała, że dane osobowe członka wspólnoty w postaci jego wizerunku, zarejestrowane przez system monitoringu, zostały wykorzystane dla celów zapewnienia bezpieczeństwa mieszkańcom budynku. Chodziło o ustalenie sprawcy zdarzenia, w związku z powtarzającą się sytuacją zamykania na klucz drzwi przeciwpożarowych, będących częścią drogi ewakuacyjnej w budynku.

Prezes UODO uznał, że przekazanie danych osobowych w wiadomości e-mail skierowanej do członków zarządu, którzy zgodnie z regulaminem funkcjonowania monitoringu byli uprawnieni do jego przeglądania, nie naruszyło przepisów o ochronie danych osobowych. Zgodnie jednak z zasadą ograniczenia przechowywania dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane. Cel, dla którego wspólnota mieszkaniowa przetwarzała dane osobowe swojego członka w postaci jego wizerunku, został osiągnięty, wobec tego organ nadzorczy nakazał wspólnocie usunięcie tych danych, zawartych w wiadomości e-mail skierowanej do członków zarządu wspólnoty, ze skrzynki poczty elektronicznej[1].

Przetwarzanie danych w celach marketingowych

W zakresie przetwarzania danych osobowych w celach marketingowych skarżący najczęściej wskazywali na otrzymywanie połączeń telefonicznych od nieznanych im wcześniej podmiotów i notoryczne otrzymywanie niechcianych wiadomości e-mail o charakterze marketingowym, gdy nie posiadali wiedzy o źródle pozyskania ich danych przez te podmioty.

W jednej ze spraw przytoczonych w Sprawozdaniu, z powodu niepoprawnej interpretacji lub nieznajomości przepisów, przetwarzanie danych administrator oparł na złej przesłance. Jak wskazał organ nadzorczy, administrator błędnie uznał, że skoro podmiot danych upublicznił swój adres e-mail, to wyraził chęć nawiązania kontaktów gospodarczych, wobec czego spółka domniemała legalność

[1] S. 43 Sprawozdania.

Kancelaria Adwokacka Adwokat Agnieszka Rapcewicz RODOwskaz Legal Consulting
ul. Narutowicza 248, 05-400 Otwock
NIP: 9512181110, REGON: 369581146
+48 668 264 604
kontakt@rodowskaz.pl, agnieszka@rodowskaz.pl

przetwarzania danych skarżącego na podstawie zgody. Prezes UODO zaznaczył, że samo umieszczenie adresu e-mail w ogólnodostępnym rejestrze nie może stanowić podstawy przetwarzania danych właściciela tego adresu opartej na zgodzie.

Z kolei w zakresie wykorzystania numeru telefonu w celach marketingowych skarżony podmiot twierdził, że przetwarzany przez niego numer telefonu nie jest powiązany z żadnymi innymi informacjami dotyczącymi skarżącego, a sam w sobie nie stanowi danych osobowych. Prezes UODO nie podzielił jednak ww. stanowiska. Zdaniem organu nadzorczego, administrator, wykorzystując informacje w postaci numeru telefonu, podejmował działania nakierowane na identyfikację osób. Identyfikacja ta nie wymagała od podmiotu nadmiernych kosztów bądź czasu, a przetwarzanie numeru telefonu służyło identyfikacji danej osoby jako klienta dla podmiotów współpracujących ze skarżonym. Prezes UODO wskazał też, że w tym przypadku nie jest możliwe powoływanie się na prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO), jak również nie istnieje żadna inna przesłanka uprawniająca administratora do przetwarzania danych. Nie zachodziło bowiem żadne powiązanie pomiędzy skarżącym a spółką, np. w postaci zawarcia umowy. Podmiot skarżony kupił bazę danych obejmującą dane osobowe skarżącego. Sama umowa sprzedaży bazy danych, stanowiąca źródło pozyskania przez administratora numeru telefonu skarżącego, nie jest bowiem przesłanką legalizującą proces przetwarzania danych osobowych do celów marketingowych. Co ciekawe, odmienne stanowisko zajął Wojewódzki Sąd Administracyjny w Warszawie w sprawie o sygn. akt II SA/Wa 1898/20, twierdząc, że sam numer telefonu nie pozwala na identyfikację konkretnej osoby fizycznej, a tym samym nie stanowi danych osobowych.

Sektor zdrowia

Jedna ze skarg dotyczyła nieuprawnionego udostępnienia przez ZUS danych osobowych lekarzowi oraz ich przetwarzania przez lekarza bez podstawy prawnej. Skarżąca twierdziła, na podstawie informacji udostępnionych na platformie elektronicznej PUE ZUS, że lekarz, wykorzystując uprawnienia nadane mu przez ZUS w celu wystawienia zaświadczeń ZUS ZLA, posługiwał się jej danymi osobowymi (nr PESEL) i wielokrotnie uzyskiwał dostęp do jej danych wrażliwych w okresie, kiedy nie korzystała ona z jego usług medycznych. Jak się okazało, w omawianej sprawie lekarz pozyskał informacje dotyczące skarżącej z PUE ZUS w celach prywatnych, m.in. w celu weryfikacji informacji co do długości trwania zwolnienia lekarskiego skarżącej, które zostało przedstawione przez skarżącą na kilka dni przed mającą się rozpocząć mediacją sądową w sprawie, w której lekarz i skarżąca byli stronami.

Jak wskazał organ nadzorczy, nie ma przepisów stanowiących podstawę do pozyskiwania przez lekarzy dostępu do danych osobowych za pośrednictwem PUE ZUS w celu innym niż wystawienie, anulowanie lub sprostowanie zaświadczenia lekarskiego. Prezes UODO podkreślił, że dane osobowe udostępniane wystawiającym zaświadczenie lekarskie w PUE ZUS dotyczą między innymi stanu zdrowia pacjentów, zatem informacji, które podlegać powinny szczególnej ochronie.[2] Działania lekarza w skarżonym zakresie były więc nieuprawnione.

[2] S. 49-50 Sprawozdanie.

Inna skarga dotyczyła nieuprawnionego przetwarzania danych osobowych przez psychologa, który udostępnił na rzecz sądu dane osobowe klienta zawarte w prywatnej opinii psychologicznej. Przetwarzanie danych klienta nie było jednak realizowane w omawianej sprawie na zlecenie sądu. Jak ustalił organ nadzorczy, psycholog udostępnił sporządzoną przez siebie opinię na rzecz sądu, uzasadniając swoje działanie uznaniem, że zagrożone jest dobro dzieci osoby składającej skargę. Prezes UODO podkreślił, że jeżeli psycholog wykorzystuje informacje o kliencie, w tym jego dane osobowe, do innych celów niż do informacji klienta, wymagane jest uzyskanie jego zgody na przetwarzanie zwykłych lub również szczególnych kategorii danych osobowych. W przypadku natomiast podejrzenia popełnienia ściganego z urzędu przestępstwa z użyciem przemocy w rodzinie, pomimo obowiązku zachowania informacji w tajemnicy, psycholog, który w związku z wykonywaniem swoich obowiązków zawodowych powziął powyższe podejrzenie, powinien niezwłocznie zawiadomić o tym policję lub prokuratora. W omawianej sprawie brak było podstawy prawnej zezwalającej na udostępnienie prywatnej opinii psychologicznej klienta na rzecz osób trzecich bez jego zgody, bądź gdy nie występują okoliczności zwalniające psychologa z tajemnicy zawodowej. Prezes UODO uznał udostępnienie przez psychologa opinii swojego klienta na rzecz sądu dla toczącego się postępowania rozwodowego za naruszające przepisy o ochronie danych osobowych, wobec czego udzielił upomnienia[3].

Realizacja przez banki prawa do przenoszenia danych zgodnie z art. 20 RODO

Jedna z wniesionych skarg dotyczyła kwestii realizacji przez bank prawa do przenoszenia danych osobowych. Prezes UODO podkreślił, że bank będący administratorem, w chwili rozpoczęcia stosowania przepisów RODO powinien być przygotowany na zapewnienie swoim klientom możliwości realizowania wszystkich praw wynikających z przepisów o ochronie danych osobowych. Po wpłynięciu wniosku dotyczącego prawa do przenoszenia danych administrator powinien dokonać analizy, czy złożony wniosek jest zasadny i czy zachodzą przesłanki do zastosowania prawa do przenoszenia danych osobowych. W przypadku stwierdzenia zasadności takiego wniosku, administrator jest zobowiązany do poinformowania osoby składającej wniosek o sposobie jego realizacji. Informacja taka powinna zostać przekazana bez zbędnej zwłoki – najpóźniej do miesiąca od daty wpłynięcia przedmiotowego wniosku do administratora. Co istotne, prawo do przenoszenia danych może zostać zrealizowane tylko w zakresie danych osobowych wnioskującego o spełnienie tego prawa oraz danych przez niego przekazanych administratorowi. Wobec tego wszelkie dane anonimowe lub niedotyczące takiej osoby, jak też dane wywnioskowane i wywiedzione na podstawie danych przekazanych przez osobę, której dotyczą, nie podlegają prawu do przenoszenia danych na podstawie art. 20 RODO[4].

[3] S. 50-51 Sprawozdania.
[4] S. 71-72 Sprawozdania.

Przetwarzanie danych osobowych w celu ochrony przed ewentualnymi roszczeniami

Na tle jednej ze skarg Prezes UODO wyraził stanowisko, które jest istotne dla wszystkich administratorów danych. Dotyczy ono przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f RODO w zakresie ustalenia, dochodzenia lub obrony roszczeń. Organ nadzorczy wskazał, że wspomniana podstawa prawna przetwarzania dotyczy sytuacji już istniejącej, w której celem wynikającym z prawnie uzasadnionych interesów realizowanych przez administratora jest konieczność udowodnienia, potrzeba dochodzenia lub obrony przed roszczeniem istniejącym, nie dotyczy zaś sytuacji, gdy dane są przetwarzane w celu zabezpieczenia się przed ewentualnym, przyszłym i niepewnym roszczeniem, a więc „na zapas". Zdaniem Prezesa UODO brak jest uzasadnienia dla przyjęcia, iż terminy dotyczące przedawnienia roszczeń wynikających ze stosunków zobowiązaniowych określają jednocześnie ramy czasowe, w których dane osobowe mogą być przetwarzane. Okolicznością usprawiedliwiającą przetwarzanie danych osobowych w celu dochodzenia roszczeń jest sam fakt istnienia roszczenia oraz zamiar jego dochodzenia[5].

Przetwarzanie przez operatorów telekomunikacyjnych danych osobowych zawartych w kserokopii dokumentów tożsamości w celu potwierdzenia możliwości wykonania umowy

W kontekście skarg składanych na operatorów telekomunikacyjnych Prezes UODO zaznaczył, że wielokrotnie wskazywał, iż dane osobowe zawarte w dowodzie osobistym, takie jak wizerunek i rysopis nie są danymi, które mogą być przetwarzane w celu wykonania umowy o świadczenie usług telekomunikacyjnych. Takie przetwarzanie narusza zasadę minimalizacji. Organ nadzorczy nie zgadza się z operatorami telekomunikacyjnymi, że podstawą do przetwarzania danych osobowych zawartych w kserokopii ww. dokumentu może być art. 161 ust. 2 ustawy Prawo telekomunikacyjne. Dowód osobisty nie jest w ocenie organu nadzorczego dokumentem potwierdzającym możliwość wykonania umowy o świadczenie usług telekomunikacyjnych. Dane zawarte w dowodzie służą przede wszystkim identyfikacji osoby, nie zaś potwierdzeniu, czy użytkownik będzie w stanie regulować rachunki za udostępnione mu usługi telekomunikacyjne[6].

Kontrole sektorowe w bankach

Sprawozdanie zawiera również ciekawe informacje związane nie tyle ze skargami, co z sektorowymi kontrolami przeprowadzonymi przez Prezesa UODO w bankach. Jak wynika ze Sprawozdania, banki różnie interpretują przepisy i zalecenia regulatorów, w szczególności jeśli chodzi o kopiowanie dokumentów tożsamości. Jeden z banków wskazał ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (przepisy art. 34 ust. 4, art. 37 oraz art. 49 ust. 1 pkt 1) jako podstawę prawną zmiany dotychczasowej praktyki w zakresie kopiowania dokumentów tożsamości (wcześniej dokumenty te nie były kopiowane). Bank ten zaczął pozyskiwać kopie dokumentów tożsamości obecnych, nowych i potencjalnych klientów, np. wtedy, gdy zaszła konieczność aktualizacji danych

[5] S.73 Sprawozdania.
[6] S.75 Sprawozdania.

zawartych w dokumencie tożsamości, w szczególności danych zawartych w dowodzie osobistym. Klient (osoba posiadająca produkt bankowy) miał możliwość odmowy wykonania skanu dokumentu, ale wtedy proszony był o podpisanie stosownego oświadczenia. Jednak przy nawiązywaniu relacji z bankiem brak zgody na zeskanowanie dokumentu tożsamości powodował odmowę świadczenia przez bank wybranej przez klienta usługi. Inny bank również wykonywał kopie dokumentów tożsamości i powołał jako podstawę prawną dla tych działań art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. a rozporządzenia 2016/679, art. 34 ust. 4, art. 35, art. 37 oraz art. 43 ust. 4 pkt 2 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu i art. 112b ustawy z 29 sierpnia 1997 r. Prawo bankowe. Zgodnie z obowiązującymi w tym banku procedurami, bank na potrzeby stosowania środków bezpieczeństwa finansowego może przetwarzać informacje zawarte w dokumentach tożsamości klienta i osób upoważnionych do działania w jego imieniu oraz sporządzać ich kopie, a w razie braku zgody na sporządzanie kopii, pozyskiwać oświadczenie zgodnie z regulacjami wewnętrznymi banku.

Z kolei w innym z kontrolowanych banków, przy podpisywaniu umowy z klientem, nie było zalecenia sporządzania kserokopii dokumentów tożsamości. Pracownik banku pozyskiwał dokument tożsamości do wglądu i spisywał dane oraz potwierdzał to na przeznaczonym do tego celu formularzu. Kserokopia dokumentów pozyskiwana była jedynie w przypadkach podejrzenia prania pieniędzy, kiedy z informacji pochodzących z baz danych, z których korzystał bank wynikało, że mogą pojawić się wątpliwości, co do danego dokumentu tożsamości przedstawionego przez klienta[7]. Banki pozyskiwały kserokopie dokumentów tożsamości klientów także w związku z oferowaniem usług obarczonych większym ryzykiem w zakresie identyfikacji klientów, związanym ze zdalnym zawieraniem umów.

Ustalenia dokonane przez Prezesa UODO wskazały więc na niejednolite podejście banków do kopiowania dokumentów tożsamości przy zawieraniu umów, jednak z uwagi na przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu, procedury wewnętrzne banków zawsze przewidywały możliwość wspomnianego kopiowania. Jak podał organ nadzorczy w Sprawozdaniu, wobec trzech banków zostały wszczęte postępowania administracyjne w zakresie niedopuszczalności przetwarzania danych osobowych, pozyskanych w wyniku sporządzenia kopii dokumentów tożsamości, w celach innych, niż wynikających z art. 35 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[8].

adw. Agnieszka Rapcewicz

[7] S. 103-104 Sprawozdania.
[8] S. 104-105 Sprawozdania.

Kancelaria Adwokacka Adwokat Agnieszka Rapcewicz RODOwskaz Legal Consulting
ul. Narutowicza 248, 05-400 Otwock
NIP: 9512181110, REGON: 369581146
+48 668 264 604
kontakt@rodowskaz.pl, agnieszka@rodowskaz.pl

Kancelaria Adwokacka Adwokat Agnieszka Rapcewicz RODOwskaz Legal Consulting
ul. Narutowicza 248, 05-400 Otwock
NIP: 9512181110, REGON: 369581146
+48 668 264 604
kontakt@rodowskaz.pl, agnieszka@rodowskaz.pl