PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

Warszawa, dnia października 2019 r.

ZSPR.027.431.2019

Pan
Krzysztof Pietraszkiewicz
Prezes Związku Banków Polskich
ul. Kruczkowskiego 8
00-380 Warszawa

w związku z pojawiającymi się sygnałami, o niezgodnych z prawem praktykach pracowników banków, polegających na nielegalnym sprzedawaniu baz danych klientów banków, w tym potencjalnie na to wskazującymi ogłoszeniami na portalach takich jak: X, Y, zwracam się do Pana Prezesa z uprzejmą prośbą o informacje, czy Związek Banków Polskich podjął lub rozważa podjąć działania, które przyczyniłyby się do zminimalizowania zjawiska nielegalnego wykorzystywania przez pracowników banków danych osobowych klientów.

Handel danymi osobowych (bazami je zawierającymi) jest niebezpiecznym zjawiskiem, które występuje na tzw. czarnym rynku. Nielegalnie pozyskane dane osobowe mogą być wykorzystywane nie tylko w celach przedstawiania niechcianych ofert marketingowych, ale także do zaciągania zobowiązań finansowych na cudze konto, oczywiście bez wiedzy i zgody osób, których dane dotyczą. Przyczyną wycieków może być brak mechanizmów zabezpieczania danych czy też ich niewłaściwe lub nieskuteczne wdrożenie przez administratorów. Osobami, które przyczyniają się do wycieku danych osobowych oraz do nielegalnego obrotu tymi danymi są nierzadko pracownicy podmiotów posiadających takie dane, zwłaszcza osoby kończące współpracę z tymi podmiotami. Dotyczy to także pracowników banków. W wielu przypadkach do udostępniania danych przez pracowników dochodzi w wyniku błędu, stosowania niewłaściwych środków ostrożności, czasem jednak także poprzez zamierzone działania.

O próbie nielegalnej sprzedaży bazy danych przez osobę podającą się za byłego pracownika banku w ostatnim czasie poinformowały media.

W związku z zaistniałą sytuacją, Prezes Urzędu Ochrony Danych Osobowych skierował do prokuratury zawiadomienie o podejrzeniu popełnienia przestępstwa, organ nadzorczy podejmuje także przewidziane przepisami prawa inne działania w sygnalizowanych mu sprawach.

Pracownicy dopuszczający się naruszeń polegających na nielegalnym udostępnianiu danych osobowych, czy też inne osoby winne w tym zakresie za działania/zaniechania niezgodne z prawem, - powinny ponosić odpowiedzialność przewidzianą przepisami prawa.

Istotne jest jednak także to, jakie działania podejmują banki, aby takim sytuacjom zapobiegać, nie tylko czy wyciągają konsekwencje wobec pracowników nieprzestrzegających zasad ochrony danych osobowych, ale także czy wprowadziły i stosują rozwiązania systemowe w tym zakresie.

Z punktu widzenia ochrony danych osobowych oraz ochrony tajemnicy bankowej, niedopuszczalne jest przenoszenie czy przesyłanie przez pracowników banków danych osobowych klientów na prywatne skrzynki mailowe czy nośniki danych osobowych. Nawet jeśli pracownik nie zamierza w nielegalny sposób wykorzystywać baz danych, które zgrał na prywatny nośnik danych lub przesłał na prywatną skrzynkę pocztową, ryzyko związane z naruszeniem bezpieczeństwa danych, niewłaściwym ich wykorzystaniem czy ich utratą jest wysokie.

W związku z powyższym istotne jest, aby banki kontrolowały pracowników pod kątem przestrzegania przez nich procedur ochrony danych osobowych a także rozliczały w tym zakresie pracowników - zarówno w trakcie trwania stosunku pracy jak i w okresach wypowiedzenia stosunku pracy - a także odpowiednio, systematycznie ale i skutecznie szkoliły pracowników z zakresu ochrony danych osobowych.

Ryzyko powstania naruszenia bezpieczeństwa, niewłaściwego przetwarzania, utraty czy udostępnienia danych osobowych osobom nieupoważnionym dotyczy wszystkich podmiotów przetwarzających dane osobowe. Dlatego każdy administrator na podstawie 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 04.06.2016, st. 1 oraz Dz. Urz. L 127 z 23.05.2018, str. 2) jest zobowiązany do przestrzegania zasad ochrony danych osobowych, przeprowadzania ocen ryzyka dla ochrony danych, a także do stosowania i monitorowania wprowadzanych, odpowiednich zabezpieczeń organizacyjnych i technicznych, które powinny chronić przed ewentualnym wyciekiem danych osobowych, czy innym naruszeniem ochrony danych osobowych.

Banki natomiast, jako instytucje zaufania publicznego powinny dbać o wymienione wyżej kwestie, w tym właściwe zabezpieczenie danych osobowych i chronić je w sposób szczególny, co

wynika ze zobowiązania nałożonego mocą art. 104 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. 2018 r. poz. 2187) do zachowywana tajemnicy bankowej[1]. Zatem bank nie może ujawniać informacji objętych tajemnicą innym podmiotom, chyba że klient banku zgodzi się, aby te informacje przekazać.

W związku z powyższym, Prezes Urzędu Ochrony Danych Osobowych zwraca się do Pana Prezesa o odniesienie się do przedstawionych w niniejszym piśmie kwestii przez Związek Banków Polskich, stowarzyszenie reprezentujące interesy banków, w tym czy Związek Banków Polskich wydał rekomendacje dla banków celem zapobieżenia nielegalnym wyciekom danych osobowych w bankach, (także spowodowanych działaniami nierzetelnych pracowników/byłych pracowników banków).

Uprzejmie proszę Pana Prezesa o potraktowanie powyższej sprawy jako istotnej i pilnej.

[1] W myśl art. 104 Prawa bankowego *bank, **osoby w nim zatrudnione** oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, **są obowiązane zachować tajemnicę bankową**, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje.*