KPP DLA POWIATU WARSZAWSKIEGO ZACHODNIEGO

https://kppbabice.policja.waw.pl/pwz/aktualnosci/100128,Informacja-o-mozliwym-naruszeniu-poufnosci-danych-osobowych.html
2021-04-19, 05:00

INFORMACJA O MOŻLIWYM NARUSZENIU POUFNOŚCI DANYCH OSOBOWYCH

Data publikacji 22.01.2021

Realizując wymogi zawarte art. 34 ust. 1 w związku z ust. 3 lit c) Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO), informujemy o potencjalnej możliwości naruszenia ochrony danych osobowych osób objętych kwarantanną w dniach 1, 3, 13 września oraz 2, 5, 7, 12 października 2020 roku na terenie gminy Kampinos. Nieuprawniony dostęp do danych osobowych jest jedynie prawdopodobny lecz nieprzesądzony, gdyż zagrożenie istniało w momencie transferu danych lub włamania na skrzynkę odbiorcy. Odbiorca nie stwierdził nieuprawnionego dostępu do swojej skrzynki pocztowej, zaś otrzymaną korespondencję zawierającą niezabezpieczone dane wykasował.

Informujemy o potencjalnej możliwości naruszenia ochrony danych osobowych w związku z incydentami, do jakich doszło w dniach 1, 3, 13 września oraz 2, 5, 7, 12 października 2020 roku w Kampinosie, polegających na wysłaniu pocztą elektroniczną ze skrzynki służbowej funkcjonariusza maili zawierających załącznik – plik niezabezpieczony hasłem, zawierający wykaz osób objętych kwarantanną, na adres mailowy uprawnionego do otrzymania informacji przedstawiciela Urzędu Gminy.

Przesłane dane obejmowały dane osób odbywających kwarantannę/izolację we wskazanych powyżej dniach w związku z Covid-19 na terenie gminy Kampinos. Przesłane dane obejmowały dane osobowe (m.in. imiona i nazwiska osób, adresy zamieszkania, adresy poczty elektronicznej, numery PESEL, telefonów, numery dokumentów tożsamości).

Realizując obowiązek wynikający z treści art. 34 RODO informujemy, iż istnieje potencjalne ryzyko, w przypadku przechwycenia przesłanych danych, do nieuprawnionego dostępu do ww. danych osobowych i zapoznania się z ich treścią.

Możliwymi konsekwencjami powyższego naruszenia ochrony danych osobowych mogą być:

- założenie konta internetowego (np. w portalach społecznościowych);
- podszycie się pod inną osobę lub instytucję w celu wyłudzenia od poszkodowanej osoby dodatkowych określonych informacji (np. danych do logowania, szczegółów karty kredytowej);
- wykorzystania danych do zarejestrowania karty telefonicznej typu prepaid, która może posłużyć do celów przestępczych;
- uzyskania przez osoby trzecie korzyści finansowych (np. kredytów w instytucjach pozabankowych);

uzyskania dostępu do systemów rejestracji świadczeń opieki zdrowotnej (np. ujawnienia informacji o stanie zdrowia);

korzystania z praw obywatelskich (np. przy głosowaniu nad środkami budżetu obywatelskiego);

podjęcia próby wyłudzenia ubezpieczenia lub środków z ubezpieczenia;

podjęcia próby zawarcia umowy o świadczenie usług;

naruszenia dobra osobistego w postaci prawa do prywatności; mandatów.

Nieuprawniony dostęp do danych osobowych jest jedynie prawdopodobny lecz nieprzesądzony, gdyż zagrożenie istniało w momencie transferu danych lub włamania na skrzynkę odbiorcy. Odbiorca nie stwierdził nieuprawnionego dostępu do swojej skrzynki pocztowej, zaś otrzymaną korespondencję zawierającą niezabezpieczone dane wykasował.

W związku z zaistniałą sytuacją proponuje się zachowanie ostrożności przy podawaniu danych osobowych osobom trzecim, w szczególności za pośrednictwem Internetu czy telefonu oraz monitorowanie aktywności kredytowej i gospodarczej, co może pozwolić na zminimalizowanie ewentualnych negatywnych skutków naruszenia ochrony danych osobowych.

Aby zapobiec ewentualnym próbom wykorzystania danych osobowych można podjąć środki zaradcze w postaci np. założenia konta w Biurze Informacji Kredytowej oraz aktywowanie funkcji alerty BIK, która poinformuje SMS-em o próbie uzyskania kredytu. Inną instytucją, weryfikującą dane osobowe, jest Krajowy Rejestr Długów, który na stronie www.konsument.krd.pl umożliwia wszystkim konsumentom bezpłatne założenie konta. Dzięki temu można sprawdzić, czy jakiś podmiot złożył zapytanie dotyczące ich osoby oraz jakie informacje zostały udzielone. Strona wprowadza możliwość powiadomienia SMS-em lub e-mailem w sytuacji pytań o historię kredytową bez pozwolenia. Daje to możliwość szybkiej reakcji – skontaktowania się z firmą, która pobrała raport bądź z Policją.

Jednocześnie informujemy, że o zdarzeniu został powiadomiony organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych, a w Komendzie Powiatowej Policji dla Powiatu Warszawskiego Zachodniego z siedzibą w Starych Babicach przeprowadzone zostały czynności wyjaśniające z ww zdarzenia prowadzące do wyciągnięcia konsekwencji służbowych wobec osoby, która dopuściła się możliwości utraty poufności Państwa danych osobowych.

W związku z powyższym rekomendowano działania korygujące, zmierzające do wyeliminowania prawdopodobieństwa wystąpienia podobnych incydentów w zakresie ochrony danych osobowych w przyszłości.

Więcej informacji możecie Państwo uzyskać kontaktując się z Inspektorem Ochrony Danych w Komendzie Powiatowej Policji dla Powiatu Warszawskiego Zachodniego z siedzibą w Starych Babicach, ul.Warszawska 276 podinsp. Grzegorzem Sokołowskim, tel. kontaktowy (47) 72 43 280 lub adres e-mail: iod.kpp_zachod@ksp.policja.gov.pl.

Jeszcze raz podkreślamy, że zagrożenie istniało wyłacznie podczas transferu danych lub włamania na skrzynkę odbiorcy, dlatego nieuprawniony dostęp do danych osobowych jest jedynie prawdopodobny lecz nieprzesądzony. Tym bardziej, że odbiorca nie stwierdził nieuprawnionego dostępu do swojej skrzynki pocztowej, a otrzymaną korespondencję zawierającą niezabezpieczone dane wykasował.

podinsp. Grzegorz Sokołowski, ego