

Komenda Powiatowa Policji w Słupcy

<https://slupca.bip.policja.gov.pl/198/ochrona-danych-osobowyc/komunikat-o-naruszeniu-ochrony/38680,Komunikat-o-naruszeniu-ochrony-danych-osobowych.html>
2024-09-27, 11:28

Charakter naruszenia ochrony danych osobowych:

W dniu 11.08.2023 r. funkcjonariusz pełniący służbę patrolową, podczas wykonywania czynności służbowych, zagubił notatnik służbowy. Notatnik został odzyskany po 8 godzinach i 35 minutach. Z uzyskanych informacji wynika, że osoba, która notatnik odnalazła, nie zapoznała się z jego zawartością i nikomu notatnika nie udostępniała. Zapisy w notatniku dotyczą osób legitymowanych w okresie 28.07.2023 - 11.08.2023 r. Notatnik służbowy służy funkcjonariuszowi do rejestrowania czynności podejmowanych w stosunku do osób legitymowanych i może zawierać m.in. Pana/Pani imię i nazwisko, nazwisko rodowe, numer PESEL, datę urodzenia, imię ojca, imię matki, nazwisko rodowe matki, adres zamieszkania, numer telefonu, informację o przeprowadzonej interwencji, informację o nałożonym mandacie karnym.

Możliwe konsekwencje naruszenia ochrony danych osobowych:

Poprzez to zdarzenie zaistniało prawdopodobieństwo wystąpienia negatywnych dla Pana/Pani skutków wynikających z nieuprawnionego wykorzystania należących do Pana/Pani danych osobowych. Są to m.in.: kradzież lub sfałszowanie tożsamości, naruszenie dobrego imienia, szykany, utrata kontroli nad własnymi danymi osobowymi, wzięcie kredytu w instytucjach pozabankowych, próba zawarcia umowy na świadczenie usług, wyłudzenie od Pana/Pani dalszych danych osobowych podszywając się pod firmę lub instytucję.

Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszenia, w tym zminimalizowaniu ewentualnych negatywnych skutków:

Przedmiotowe naruszenie ochrony danych osobowych będzie omawiane podczas cyklicznych szkoleń z zakresu ochrony danych osobowych oraz najbliższych odpraw do służby. Wszczęte zostanie także postępowanie wyjaśniające, które prowadzić będzie do wyciągnięcia konsekwencji wobec osoby odpowiedzialnej za dopuszczenie do utraty poufności Pana/Pani danych.

Aby zminimalizować ewentualne negatywne skutki naruszenia może Pan/Pani:

- Zachować szczególną ostrożność w przypadku nieoczekiwanych kontaktów - istnieje bowiem możliwość, że przestępcy będą podejmować próby pozyskania brakujących danych, np. poprzez podszycie się pod pracownika urzędu;
- Zachować szczególną ostrożność w przypadku wszelkich aktywności wymagających podania danych osobowych. Nie należy podawać danych osobom trzecim, zwłaszcza nieznanym kontaktującym się z nami poprzez Internet lub telefon;
- Sprawdzić czy nie doszło do przejęcia konta mailowego i jeżeli to możliwe należy zmienić hasło;
- Rozważyć wprowadzenie dwuskładnikowego uwierzytelniania w serwisach, które umożliwiają taką opcję;
- Zachować szczególną czujność korzystając z mediów społecznościowych. Może dojść do próby przejęcia profilu;
- Zachować szczególną czujność podczas odbierania telefonów z zagranicy;
- Zastrzec PESEL;
- W rejestrze rachunków bankowych sprawdzić czy na Pana/Pani dane nie założono rachunków bankowych;
- Rozważyć skorzystanie z usług Krajowego Rejestru Długów (www.konsument.krd.pl) oraz Biura Informacji Kredytowej (www.bik.pl). Z rejestrów tych korzystają banki, operatorzy telekomunikacyjni, dostarczyciele telewizji. Serwis umożliwia włączenie alertów powiadamiających nas SMS, że ktoś próbuje na nasze dane podpisać umowę lub wziąć pożyczkę;
- Zachować szczególną ostrożność w sytuacji usiłowania wyłudzenia pieniędzy metoda „na BLIKA”. Polega ona na wyłudzeniu kodu do płatności telefonem. Osoba logując się do swojego banku musi wygenerować w aplikacji kod do płatności telefonem, a następnie przesłać go „znajomemu”. Niestety w przeciwieństwie do płatności przelewem, transakcji dokonanych za pomocą tego kodu nie można już cofnąć, gdyż przestępca od razu wpisuje podany kod BLIK w bankomacie i wypłaca z niego pieniądze.
- Jeżeli podejrzewa Pan/Pani, że przestępcy podrobili Pana/Pani dowód, proszę zastrzec go w Systemie Dokumenty Zastrzeżone prowadzonym przez Związek Banków Polskich (www.dokumentyzastrzezone.pl).

Komendant Powiatowy Policji w Słupcy dołoży wszelkich starań, aby podobne zdarzenie w przyszłości nie miało miejsca. Niniejsze zawiadomienie sporządzono w oparciu o obowiązujące przepisy prawa, jednocześnie zrealizowany zostanie obowiązek notyfikacyjny względem Prezesa UODO spoczywający na Administratorze Danych Osobowych.

Więcej informacji mogą uzyskać Państwo kontaktując się z Inspektorem Ochrony Danych:

Rafał Świciński - tel.: 47 77 38 322; e-mail: iod.slupca@po.policja.gov.pl.

Adres do korespondencji: ul. Poznańska 13, 62-400 Słupca.

Metryczka

Data publikacji : 16.08.2023
Data modyfikacji : 18.09.2024
[Rejestr zmian](#)

Podmiot udostępniający informację:
Komenda Powiatowa Policji w Słupcy

Osoba wytwarzająca/odpowiadająca za informację:
Rafał Świciński

Osoba udostępniająca informację:
Rafał Świciński Zespół ds. Ochrony Informacji
Niejawnych

Osoba modyfikująca informację:
Rafał Świciński