https://miedzychod.bip.policja.gov.pl/190/ochrona-danych-osobowyc/37371,KOMUNIKAT-O-NARUSZENIU-OCHRONY-DANYCH.html
2024-12-04, 22:30

KOMUNIKAT O NARUSZENIU OCHRONY DANYCH

Utrata pokwitowań zatrzymania dokumentu w Komendzie Powiatowej Policji w Międzychodzie

Zgodnie z art. 45 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości informujemy, że doszło do czasowej utraty druków pokwitowań zatrzymania dokumentu przez policjanta Ogniwa Ruchu Drogowego KPP w Międzychodzie.

Druki pokwitowań zatrzymania dokumentu zawierały m.in. dane osobowe (dane identyfikacyjne – imię i nazwisko oraz PESEL) osób, które w okresie od 14.06.2022 do 25.12.2022 roku miały zatrzymany dokument (dowód rejestracyjny pojazdu lub prawo jazdy) na pokwitowaniach: od seria **PAA** numer **0608251** do seria **PAA** numer **0608273**.

Możliwymi konsekwencjami powyższego naruszenia ochrony danych osobowych mogą być: utrata kontroli nad własnymi danymi osobowymi, kradzież lub sfałszowanie tożsamości lub naruszenie dobrego imienia. Powyższe skutkować może m.in. próbami uzyskania przez osoby trzecie, na szkodę osoby, której dane naruszono, kredytu w instytucjach pozabankowych czy uzyskania dostępu do korzystania ze świadczeń opieki zdrowotnej przysługujących osobie, której dane naruszono.

Aby zapobiec ewentualnym próbom wykorzystania danych osobowych można podjąć następujące środki zaradcze:

Zachować szczególną ostrożność w przypadku nieoczekiwanych kontaktów. Istnieje możliwość, że przestępcy będą podejmować próby uzyskania brakujących danych osobowych, np. poprzez podszycie się pod pracownika obsługi kadrowej instytucji, w której pracujesz.

Zachować szczególną ostrożność w przypadku wszelkich aktywności wymagających podawania danych osobowych (nie tylko w Internecie). Nie należy podawać danych osobowych osobom trzecim, zwłaszcza nieznajomym kontaktującym się z nami przez Internet lub telefon.

Sprawdzić czy nie doszło do przejęcia konta mailowego – jeżeli można zmienić hasło. Wielu użytkowników sieci Internet posługuje się hasłami opartymi na imieniu, nazwisku lub dacie urodzenia, **Rozważyć wprowadzenie dwuskładnikowego uwierzytelnienia**[1] **na swoim koncie email oraz w serwisach społecznościowych.**

Zachować szczególną czujność korzystając z mediów społecznościowych. Może w nich dojść do przejęcia Twojego profilu.

weryfikuj otrzymywane wiadomości dotyczące próśb o pożyczki, numery kodów i hasła;

niezwłocznie zmień hasło w mediach społecznościowych. **Nie odpowiadać na wiadomości email i smsy wysyłane przez spamerów.** Zachować najwyższą ostrożność zwłaszcza, gdy takie wiadomości dotyczą płatności. W sytuacji nękania telefonami z zagranicy **zachować czujność, nie odbierać takich połączeń. Skorzystać z bezpłatnego zastrzeżenia swojego nr PESEL.** Można to zrobić przy użyciu formularza na https://www.bezpiecznypesel.pl/pesel/. Partnerzy Systemu Bezpieczny Pesel (firmy pożyczkowe z sektora pozabankowego) zostaną poinformowani, że Twój numer PESEL jest zastrzeżony. Zastrzeżenie możesz bezpłatne cofnąć w każdej chwili. **Ponadto, zastrzeż swoje dane na obywatel.gov.pl oraz chronPESEL.pl.**

Sprawdzić czy na Twoje dane nie założono rachunków bankowych. Można to zrobić w centralnym rejestrze rachunków bankowych na centralnainformacja.pl

Rozważyć skorzystanie z usług Krajowego Rejestru Długów – załóż konto w Serwisie Ochrony Konsumenta (www.konsument.krd.pl). Z usług KRD korzystają banki, operatorzy telekomunikacyjni, czy dostarczyciele telewizji. Przed udzieleniem kredytu lub sprzedaży usługi z odroczoną płatnością, sprawdzają naszą rzetelność finansową w biurze informacji gospodarczej KRD. Każde takie sprawdzenie zostawia ślad w systemie do którego masz wgląd.

Rozważyć skorzystanie z Alertów BIK. Alerty informują o próbach zaciągania zobowiązań na dane konkretnej osoby, a także próbach zawarcia umów z operatorami sieci komórkowych czy dostawcami mediów. Ostrzeżenia przychodzą w formie SMS i e-mail.

Możesz sprawdzić historię kredytową w BIK. Jeśli uruchomiłeś Alerty, możesz sprawdzić całą swoją historię kredytową w BIK. W ten sposób potwierdzisz, że na Twój PESEL nie zostało wcześniej zaciągnięte jakieś zobowiązanie. Istotne jest, że Biuro Informacji Kredytowej współpracuje z całym sektorem bankowym i większością firm pożyczkowych. Dane można sprawdzić rejestrując się na www.bik.pl i pobierając raport.

Zachować szczególną ostrożność w sytuacji usiłowania wyłudzenia pieniędzy „metodą na blika”. Metoda ta polega na wyłudzeniu kodu do płatności przez telefon. 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.

Jeśli otrzymasz prośbę o pożyczkę, nie działaj pochopnie. Sprawdź czy osoba, która do Ciebie napisała lub której prośba dotyczy rzeczywiście potrzebuje naszej pomocy\

Możesz skorzystać również z innych alertów w serwisach informacji gospodarczej. Ustawienie alertów w kilku serwisach informacji gospodarczej zwiększa prawdopodobieństwo powodzenia działań zapobiegawczych, ponieważ firmy pożyczkowe korzystają z różnych systemów weryfikacyjnych. Serwisy informacji gospodarczej: centralnainformacja.pl , infoKonsument.pl

Zastrzec dowód osobisty. W przypadku podejrzenia, że przestępcy na podstawie posiadanych danych podrobili Twój dowód osobisty, zastrzeż dokument w Systemie Dokumenty Zastrzeżone prowadzonym przez Związek Banków Polskich. W przypadku, gdy sprawdzenie w rejestrze dokumentów zastrzeżonych da wynik pozytywny, umowa na taki numer dowodu nie będzie mogła zostać zawarta. Lista banków zastrzegających dokumenty od wszystkich osób znajduje się pod adresem https://dokumentyzastrzezone.pl/lista-bankowzastrzegajacych-dokumenty-od-wszystkich-osob/.

Niektóre wskazane usługi mogą być płatne zgodnie z cennikiem ich dostawcy.

Jednocześnie informujemy, że o zdarzeniu został powiadomiony organ nadzorczy Prezes Urzędu Ochrony Danych Osobowych, a w Komendzie Powiatowej Policji w Międzychodzie trwają czynności zmierzające do wyjaśnienia przedmiotowego zdarzenia i wyciągnięcia konsekwencji służbowych wobec osoby, która dopuściła do utraty poufności Państwa danych osobowych. W związku ze zdarzeniem rekomendowano działania korygujące, zmierzające do wyeliminowania prawdopodobieństwa wystąpienia podobnych incydentów w ochronie danych osobowych. Ponadto powyższy przypadek będzie przedmiotem odpraw służbowych, szkoleń z jednoczesnym poleceniem zwiększenia nadzoru nad dokumentacją służbową.

Za zaistniałą sytuację przepraszamy.

Kontakt z Inspektorem Ochrony Danych w Komendzie Powiatowej Policji w Międzychodzie:

Inspektor Ochrony Danych KPP w Międzychodzie: Ewa Weber

Adres do korespondencji:

Komenda Powiatowa Policji w Międzychodzie

ul. Gen. Sikorskiego 22a

64-400 Międzychód

Adres e-mail: iod.miedzychod@po.policja.gov.pl

Numer tel. 47 77 36 322

Objaśnienia:

[1] Uwierzytelnianie dwuskładnikowe (ang. Two Factor Authenticaton, 2FA) może pomóc chronić Twoje konta w sieci Internet. Zapewnia „podwójne sprawdzanie” (czy jesteś osobą, za którą się podajesz) przy korzystaniu z usług online. Podczas konfigurowania 2FA usługa poprosi Cię o podanie „drugiego składnika”, do którego masz dostęp tylko Ty. Mogą nim być różne dane, np. kod wysyłany do Ciebie SMS-em lub utworzony przez aplikację zainstalowaną na Twoim urządzeniu mobilnym lub wygenerowana wcześniej lista kodów, którą przechowujesz w bezpiecznym miejscu..

Metryczka

Data publikacji : 20.01.2023
Rejestr zmian

Podmiot udostępniający informację:
Komenda Powiatowa Policji w Międzychodzie

Osoba udostępniająca informację:
Krystian Filipiak KPP Międzychód