RCB
Rządowe Centrum Bezpieczeństwa

RPW/39495/2021 P
Data:2021-05-10

Warszawa, 07 maja 2021 r.

Rządowe Centrum Bezpieczeństwa

Grzegorz Matyasik
Zastępca dyrektora

BIURO RZECZNIKA PRAW OBYWATELSKICH
WPŁ. 2021 -05- 10 Egz. nr 1
ZAŁ. 5 NR .....

WO.072.1.2021

KW.873.2021

Pan Stanisław TROCIUK
Zastępca Rzecznika Praw Obywatelskich

Szanowny Panie!

W związku z pandemią wywołaną rozprzestrzenianiem się wirusa SARS-CoV-2, powodującego chorobę COVID-19, Minister Zdrowia zawarł z Rządowym Centrum Bezpieczeństwa porozumienie w sprawie powierzenia przetwarzania danych osobowych. Minister Zdrowia, jako administrator danych osobowych, powierzył Rządowemu Centrum Bezpieczeństwa dane osobowe oznaczonych kategorii osób fizycznych, w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem wirusa SARS-CoV-2 oraz rejestracją na wykonanie szczepienia ochronnego przeciwko COVID-19. Dane osób, które znajdują się w grupie zawodowej uprawnionej do wykonania szczepienia, i które wyraziły wolę zaszczepienia, są niezbędne do wystawienia e-skierowania, które umożliwia zarejestrowanie się osoby fizycznej na szczepienie w dopuszczonej przepisami formie. Zgodnie z art. 21d ust.1 ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. z 2020 r. poz. 1845, z późn. zm.), szczepienia ochronne przeciwko COVID-19 są przeprowadzane na podstawie skierowania określonego w przepisach wydanych na podstawie art. 30 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

20 kwietnia 2021 r. w serwisie niebezpiecznik.pl pojawiła się informacja dotycząca wycieku danych osobowych funkcjonariuszy służb mundurowych, którzy wyrazili zgodę na udział w procesie szczepienia. Po wstępnych czynnościach wyjaśniających w sprawie tego incydentu, jeszcze tego samego dnia, Rządowe Centrum Bezpieczeństwa przekazało Ministerstwu Zdrowia informację o naruszeniu ochrony danych osobowych.

22 kwietnia 2021 r. Minister Zdrowia, jako Administrator danych, przekazał drogą elektroniczną do Prezesa Urzędu Ochrony Danych Osobowych zgłoszenie naruszenia ochrony

danych osobowych. Tego samego dnia Rządowe Centrum Bezpieczeństwa rozpoczęło wysyłanie do osób, których dane dotyczą, zawiadomień zawierających informacje o charakterze naruszenia ochrony danych osobowych, opis możliwych konsekwencji naruszenia ochrony danych osobowych, opis środków zastosowanych przez administratora w celu zminimalizowania ewentualnych negatywnych skutków, opis środków proponowanych osobie poszkodowanej w celu zminimalizowania ewentualnych negatywnych skutków oraz dane kontaktowe do upoważnionych osób w RCB, w celu uzyskania dodatkowych informacji.

Powołany przez Dyrektora RCB zespół prowadzi wewnętrzne postępowanie wyjaśniające, mające na celu przede wszystkim wyjaśnienie przyczyn i okoliczności naruszenia ochrony danych osobowych oraz wypracowanie środków zaradczych. Niezależnie od tego, po złożonym przez Dyrektora RCB zawiadomieniu do Prokuratury Okręgowej w Warszawie o możliwości popełnienia przestępstwa, trwają już czynności organów ścigania zmierzające do ustalenia, kto i w jaki sposób mógł wejść w posiadanie tych danych oraz czy może nimi nadal dysponować. Licząc się z tym ryzykiem, RCB prowadzi konsultacje (m. in. z Komisją Nadzoru Finansowego i Biurem Informacji Kredytowej) oraz zbiera informacje o innych możliwych działaniach redukujących ryzyko wystąpienia szkód dla funkcjonariuszy, poprzez wykorzystanie tych danych osobowych przez osoby nieuprawnione (fałszowanie tożsamości, nadużycia finansowe, naruszenia prywatności, itp.). Adekwatnie do ustalonych zagrożeń będą podejmowane dalsze instytucjonalne środki zaradcze oraz rekomendowane funkcjonariuszom środki ostrożnościowe.

Załączniki:

Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych.
Uzupełnienie do zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych.

Z poważaniem
Grzegorz Małyszek

Wykonano w 2 egzemplarzach

Egz. nr 1 – Adresat
Egz. nr 2 – a/a

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa
tel. +48 22 36 16 899 | fax +48 22 36 16 898
e-mail: sekretariat@rcb.gov.pl | www.rcb.gov.p

RZĄDOWE CENTRUM BEZPIECZEŃSTWA
00-583 Warszawa, Al. Ujazdowskie 5
(1)

Rządowe Centrum Bezpieczeństwa

Warszawa, dnia 22.04.2021 r.

Znak sprawy: WO.091.1.2021

Egz. pojedynczy

ZAWIADOMIENIE OSOBY KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Charakter naruszenia ochrony danych osobowych

W dniach od 12 do 20 kwietnia 2021 r. na portalu „ArcGIS Online" dla określonych służb mundurowych został udostępniony formularz elektroniczny w celu zbierania niezbędnych danych funkcjonariuszy na potrzeby szczepień przeciwko chorobie COVID-19. Wytypowani przedstawiciele tych służb w wyżej wymienionych dniach sukcesywnie wprowadzali do formularza dane osobowe funkcjonariuszy do szczepień. W formularzu zgłoszeniowym znajdowały się następujące dane: imię i nazwisko, nr PESEL, służbowy adres e-mail, numer telefonu, pełna nazwa macierzystej jednostki organizacyjnej oraz jej adres.

W dniu 20.04.2021 r. Rządowe Centrum Bezpieczeństwa otrzymało informację, że dostęp do formularza był możliwy dla innych osób posiadających konto na ArcGIS. Przez to mogło dojść do naruszenia poufności Pani/Pana danych osobowych.

Opis możliwych konsekwencji naruszenia ochrony danych osobowych

Następstwem naruszenia Pani/Pana danych osobowych może być:

- założenie na Pani/Pana dane osobowe konta internetowego (np. w serwisach społecznościowych, poczty elektronicznej),
- podszycie się pod inną osobę lub instytucję w celu wyłudzenia od Pani/Pana dodatkowych określonych informacji (np. danych do logowania, szczegółów karty kredytowej),
- wykorzystania Pani/Pana danych do zarejestrowania karty telefonicznej typu prepaid, która może posłużyć do celów przestępczych,
- podjęcie przez osoby trzecie próby uzyskania na Pani/Pana szkodę, pożyczek w instytucjach pozabankowych np. przez Internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości,
- osoby trzecie mogą podjąć próbę uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskać wgląd do danych o Pani/Pana stanie zdrowia, ponieważ czasem dostęp do systemów rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL,
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osobę trzecią do próby wyłudzenia ubezpieczenia,
- Pani/Pana dane osobowe mogą zostać wykorzystane np. do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego, tym samym skorzystać z Pani/Pana praw obywatelskich,
- osoby trzecie mogą podjąć próbę zawarcia na Pani/Pana szkodę umów cywilno-prawnych, np. najmu nieruchomości,
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osoby trzecie do ukrycia swojej tożsamości, np. przy otrzymywaniu mandatu,

- może Pani/Pan otrzymywać fałszywe SMS-y lub być narażona/y na przesyłanie spamu na podane konto poczty elektronicznej, linków do podrobionych stron elektronicznych płatności, aplikacji wykradających dane, fikcyjnych sklepów internetowych.

Opis środków zastosowanych przez administratora w celu zminimalizowania ewentualnych negatywnych skutków

W związku z zaistniałym naruszeniem ochrony danych osobowych:

- niezwłocznie zamknięto formularz zgłoszeniowy, celem uniemożliwienia komukolwiek dostępu do niego,
- w trybie pilnym zorganizowano spotkanie z firmą Esri Polska sp. z o.o. (dystrybutorem oprogramowania ArcGIS) celem przeanalizowana sytuacji i zabezpieczenia wszystkich danych, które mogły być dostępne dla osób nieuprawnionych,
- o incydencie poinformowano w dniu 20.04.2021 r. Administratora Danych – Ministra Zdrowia, który w dniu 22 kwietnia 2021 r. zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu ochrony danych osobowych,
- zdarzenie zgłoszono do CSIRT GOV,
- prowadzone jest wewnętrzne postępowanie wyjaśniające i podejmowane będą konsultowane z Ministerstwem Zdrowia inne środki zaradcze w zakresie ochrony danych osobowych,
- powiadomiono komendantów/szefów służb o zdarzeniu, których funkcjonariuszy to dotyczy,
- powiadomiono Prokuraturę Okręgową w Warszawie o uzasadnionym przypuszczeniu popełnienia przestępstwa.

Opis środków proponowanych osobie w celu zminimalizowania ewentualnych negatywnych skutków

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy:

- ignorować nieoczekiwane wiadomości SMS lub poczty elektronicznej, w szczególności od nieznanych nadawców,
- zachować ostrożność w sytuacji odbierania połączeń telefonicznych od nieznanych numerów telefonów, w szczególności przy podawaniu danych osobowych innym osobom,
- skorzystać z możliwości założenia konta w systemie informacji kredytowej lub gospodarczej, w celu dodatkowego zabezpieczenia swoich danych przed nieuprawnionym wykorzystaniem, w tym monitorowania prób uzyskania kredytu.

Jeśli dowie się Pani/Pan o wykorzystaniu Pani/Pana danych przez osobę nieuprawnioną, prosimy o jak najszybsze przekazanie tej informacji nam oraz swoim przełożonym.

Dane kontaktowe w celu uzyskania dodatkowych informacji

Jeżeli ma Pani/Pan jakiekolwiek pytania lub chciałaby nam Pani/Pan przekazać dodatkowe informacje w związku z zaistniałym zdarzeniem, prosimy o kontakt z:

1) Gestor zbioru danych osobowych – Beata Janowczyk
   Adres e-mail: beata.janowczyk@rcb.gov.pl
   Telefon: 22 36 16 930,
   lub
2) Inspektor Ochrony Danych RCB – Jan Teleon
   Adres e-mail: iod@rcb.gov.pl
   Telefon: 22 36 16 970.

DYREKTOR
Rządowego Centrum Bezpieczeństwa
płk Konrad Korgwacki

Rządowe Centrum Bezpieczeństwa

Warszawa, dnia 30.04.2021 r.

Znak sprawy: WO.091.1.2021

Egz. pojedynczy

UZUPEŁNIENIE DO ZAWIADOMIENIA OSOBY KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Charakter naruszenia ochrony danych osobowych

W związku z przetwarzaniem danych osobowych funkcjonariuszy i pracowników służb mundurowych związanych ze zbieraniem danych niezbędnych do przeprowadzenia szczepień przeciwko COVID-19, Rządowe Centrum Bezpieczeństwa jako podmiot przetwarzający zawiadamia, że mogło dojść do naruszenia poufności Pani/Pana danych osobowych.

Zawiadomienie kierowane jest do osób, które w dniach 12-20 kwietnia br. poprzez stronę internetową http://szczepieniakadry.rcb.gov.pl/ za pomocą formularza przekazali dane zawierające imię i nazwisko, nr PESEL, służbowy adres e-mail, numer telefonu, nazwę macierzystej jednostki organizacyjnej oraz jej adres.

Należy podkreślić, że każda utrata poufności danych osobowych niesie za sobą wzrost ryzyka kradzieży tożsamości oraz nieuprawnionego jej wykorzystania poprzez np. zaciągnięcie kredytu lub pożyczki.

Istotne jest, że zestaw danych, które były przedmiotem podejrzenia wycieku (nie zawierający danych dokumentu tożsamości), najprawdopodobniej będzie niewystarczający do podszycia się pod inną osobę i wzięcia pożyczki lub kredytu na jej dane. Jednak ryzyko istnieje i jest zdecydowanie wyższe niż przed zaistnieniem zdarzenia, z następujących powodów:

- wprawdzie większość instytucji finansowych weryfikuje tożsamość wykorzystując informacje z rejestrów publicznych, co pozwala na potwierdzenie wewnętrznej spójność zestawu danych, w szczególności imienia, nazwiska, numeru PESEL i numeru dowodu osobistego, **jednak niektóre instytucje finansowe nie przeprowadzają takiej weryfikacji, co umożliwia np. zaciągnięcie pożyczki na imię, nazwisko, odpowiadający im numer PESEL i niewłaściwy (nieistniejący w obrocie prawnym) numer dowodu. Istotne jest, iż numer dowodu osobistego można bez przeszkód wygenerować tak, aby jego struktura odpowiadała obowiązującym w tym zakresie wymaganiom**.
- **zakres ujawnionych danych jest na tyle szeroki, że pozwala dość precyzyjnie sprofilować daną osobę i nawiązać z nią kontakt**. Nie można też wykluczyć, że przestępcy już są w posiadaniu innych fragmentarycznych danych osób dotkniętych potencjalnym wyciekiem i mogą połączyć posiadane dane z danymi nowo pozyskanymi.

Opis środków proponowanych osobie w celu zminimalizowania ewentualnych negatywnych skutków

W celu ochrony przed kradzieżą tożsamości zasadne jest **utrzymywanie zwiększonego poziomu ostrożności i uwagi przez osoby, której dane mogły zostać ujawnione.** Rekomendowane są między innymi następujące działania:

1. **Zachowaj 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.

2. **Zachowaj 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.

3. **Sprawdź czy nie doszło do przejęcia konta mailowego – jeżeli możesz zmień hasło.** Wielu użytkowników sieci Internet posługuje się hasłami opartymi na imieniu, nazwisku lub dacie urodzenia,

4. **Rozważ wprowadzenie dwuskładnikowego uwierzytelnienia[1] na swoim koncie email oraz w serwisach społecznościowych.**

5. **Zachowaj 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.

6. **Nie odpowiadaj na wiadomości email i smsy wysyłane przez spamerów.** Zachowaj najwyższą ostrożność zwłaszcza, gdy takie wiadomości dotyczą płatności.

7. W sytuacji nękania telefonami z zagranicy **zachowaj czujność, nie odbieraj takich połączeń.**

8. **Skorzystaj z bezpłatnego zastrzeżenia swojego nr PESEL.** Możesz 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.**

9. **Sprawdź czy na Twoje dane nie założono rachunków bankowych.** Można to zrobić w centralnym rejestrze rachunków bankowych na .

10. **Rozważ 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.

11. **Rozważ 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.

12. **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.

13. **Zachowaj 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.

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

15. **Możesz skorzystać również z innych alertów w serwisach informacji gospodarczej.** Ustawienie alertów w kilku serwisach informacji gospodarczej zwiększa

[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..

prawdopodobieństwo powodzenia działań zapobiegawczych, ponieważ firmy pożyczkowe korzystają z różnych systemów weryfikacyjnych. Serwisy informacji gospodarczej:

- centralnainformacja.pl
- infoKonsument.pl

16. **Zastrzeż 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-bankow-zastrzegajacych-dokumenty-od-wszystkich-osob/.

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

Dane kontaktowe w celu uzyskania dodatkowych informacji

Jeżeli ma Pani/Pan jakiekolwiek pytania lub informacje dotyczące przekazanego komunikatu, Rządowe Centrum Bezpieczeństwa uruchomiło specjalne numery telefonów **22 3616932** oraz **22 3616850** obsługiwane przez n/wym. pracowników w dni robocze w godzinach 8:15 – 16:15:

1) Magdalena Kilis-Sokołowska;
2) Ewa Michałkiewicz;
3) Piotr Błaszczyk.

Dodatkowo do kontaktu utworzono adres email: naprawa_naruszenia@rcb.gov.pl

Zastępca Dyrektora
Rządowego Centrum Bezpieczeństwa

Grzegorz Matyasik

/podpisano kwalifikowanym podpisem elektronicznym/

RCB
Rządowe Centrum Bezpieczeństwa

Rządowe Centrum **Bezpieczeństwa**

00 – 583 Warszawa, Al. Ujazdowskie 5

OPŁATA POBRANA
TAXE PERCUE-POLOGNE
Umowa z Pocztą Polską S.A.
ID NR 448446/W

WARSZAWA 12
07052021
UŁ

KW.873.2021

R (00)359007731128560528

Rzecznik Praw Obywatelskich

Al. Solidarności 77

00-090 Warszawa

Poczta Polska
Opłata pobrana _____ zł ____ gr

2020
BIURO RZECZNIKA PRAW OBYWATELSKICH
WPŁ. 2021 -05- 10
ZAŁ. ..... NR .....

POLECONE

PRIORYTET
PRIORITAIRE