Zaktualizowany komunikat w trybie art. 34 RODO z dnia 15 kwietnia 2020

BD – I.0160.5.2020

Szanowna Pani/Szanowny Panie

Działając na podstawie art. 34 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), zwane dalej RODO, przedstawiamy doprecyzowaną, na podstawie najnowszych ustaleń, informację o naruszeniu ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia Pani/Pana praw lub wolności.

Opis charakteru naruszenia

Naruszenie ochrony danych osobowych polegało na kradzieży danych użytkowników Platformy Szkoleniowej KSSiP, zarejestrowanych do dnia 21.02.2020 r., których administratorem jest Krajowa Szkoła Sądownictwa i Prokuratury z siedzibą w Krakowie, ul. Przy Rondzie 5, 31-547 Kraków. W efekcie kradzieży, dane przedostały się do Internetu.

Dotychczasowe ustalenia wskazują, że przedmiotem kradzieży były:
a/ dane wskazane przez użytkowników przy rejestracji, zgromadzone w następujących kategoriach: nazwa użytkownika, imię, nazwisko, numer lub numery telefonu, adres e-mail, jednostka, wydział, adres jednostki, miasto.
b/ dane o charakterze technicznym: adres IP i daty pierwszego i ostatniego logowania, hasło (zaszyfrowane).
W zakres tych danych nie wchodzą żadne informacje o miejscu zamieszkania ani o charakterze finansowym.

Należy podkreślić, że z uwagi na wąski zakres danych wymaganych przy rejestracji, wiele wskazanych kategorii nie zawiera żadnych wpisów lub zawiera nieliczne wpisy niewielkiej grupy osób, nadto wiele z danych ma charakter służbowy albo jest już nieaktualna.

Aktualnie trwają czynności analityczne celem ustalenia, czy przedmiotem kradzieży były również numery PESEL, gdyż obecnie nie można całkowicie wykluczyć takiej możliwości.

Możliwe konsekwencje naruszenia

Dysponując wskazanymi wyżej skradzionymi danymi, osoba nieuprawniona może podejmować działania związane z możliwością posługiwania się nimi tam, gdzie uwierzytelnienie wymaga podania imienia i nazwiska, numeru telefonu lub/oraz adresu email, i tym samym osoba taka może:

- podejmować próby zawierania umów uzyskania na Pani/Pana szkodę, pożyczek w instytucjach pozabankowych np. przez Internet lub telefonicznie, w przypadkach niewymagających okazywania dokumentu tożsamości i podawania nr PESEL;

- próbować wykorzystać Pani/Pana dane osobowe np. do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego (o ile nie będzie to podawania nr PESEL), a tym samym skorzystać z Pani/Pana praw obywatelskich;
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osoby trzecie do ukrycia swojej tożsamości;
- Pani/Pana dane mogą zostać wykorzystane do zakładania kont na stronach internetowych, forach, sklepach i innych serwisach tam, gdzie brak jest weryfikacji zwrotnej za pomocą e-maila lub numeru telefonu (sms/mms)

Z uwagi na to, że obecnie nie potwierdzono aby zachodziła możliwość posługiwania się Pani/Pana numerem PESEL, nie zachodzi niebezpieczeństwo działań związanych z takim działaniem.

Działania przez nas podjęte

Informujemy, że natychmiast po stwierdzeniu przez KSSiP naruszenia ochrony danych osobowych:

- usunięto wszystkie hasła dostępu do Platformy Szkoleniowej KSSiP oraz Platformy e-KSSiP, wymuszając jednocześnie dokonanie ich zmiany przez użytkowników;
- powiadomiono niezbędne instytucje i organy m.in. Policję, CERT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego), Ministerstwo Sprawiedliwości, Prokuraturę Krajową oraz zgłoszono naruszenie ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych (polskiemu organowi nadzorczemu zajmującemu się sprawami ochrony danych osobowych);
- podjęto czynności zmierzające do zablokowania i usunięcia możliwości rozpowszechniania skradzionych danych, poprzez zwrócenie się przez KSSiP o ich usunięcie do administratorów serwisów, które udostępniły skradzione dane;
- niezwłocznie dokonano, dodatkowej weryfikacji zabezpieczeń systemu informatycznego wykorzystywanego do administrowania zasobami informatycznymi KSSiP;
- podjęto pilne prace zmierzające do ujawnienia okoliczności naruszenia ochrony danych osobowych, we współpracy z powiadomionymi przez KSSiP instytucjami i organami (w tym ścigania).

Co może Pani/Pan zrobić

W celu zabezpieczenia się przed negatywnymi skutkami zaistniałego naruszenia zalecamy, aby osoby których dane osobowe mogły ulec naruszeniu, podjęły kroki minimalizujące ryzyko wystąpienia negatywnych konsekwencji i nieuprawnionego wykorzystania danych m.in. poprzez::

a) ignorowanie nieoczekiwanych wiadomości wysyłanych poprzez pocztę elektroniczną i/lub telefonicznie, w szczególności pochodzące od nieznanych nadawców;
b) zachowanie ostrożność w sytuacji odbierania połączeń telefonicznych pochodzących z nieznanych numerów telefonów, w szczególności międzynarodowych i nieoddzwanianie na te numery;

c) zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
d) założenie konta w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej (na rynku dostępne są systemy, instytucje i przedsiębiorstwa, które oferują usługi pozwalające na monitorowanie swojej aktywności kredytowej. Podajemy przykładowe: Biuro Informacji Kredytowej S.A. strona https://www.bik.pl, Biuro Informacji Gospodarczej InfoMonitor S.A. strona https://big.pl, Krajowy Rejestr Długów Biuro Informacji Gospodarczej S.A. stron https://krd.pl, Serwis CHRONPESEL strona https://www.chronpesel.pl). W przypadku stwierdzenia jakichkolwiek nieprawidłowości – zgłoszenie tego faktu organom ścigania; – w celu dodatkowego zabezpieczenia swoich danych przed nieuprawnionym wykorzystaniem.

Jeżeli dowie się Pani/Pan o wykorzystaniu Pani/Pana danych przez osobę nieuprawnioną, prosimy o jak najszybsze zawiadomienie o tym organów ścigania (Policję, Prokuraturę) oraz przekazanie nam tej informacji.

Gdzie można uzyskać więcej informacji?

W razie dodatkowych pytań lub wątpliwości prosimy o kontakt z Inspektorem Ochrony Danych – lub gdyby chciałaby/chciałby nam Pani/Pan przekazać dodatkowe informacje, które pomogą w wyjaśnieniu sprawy i mają z nią związek:

Inspektor Ochrony Danych – Tomasz Gacka
Adres e-mail: iod@kssip.gov.pl
Telefon: kom.: +48 603 450 231

Krajowa Szkoła Sądownictwa i Prokuratury
ul. Przy Rondzie 5
31-547 Kraków
Adres e-mail: sekretariat@kssip.gov.pl
Adres ePUAP: /kssip_krakow/SkrytkaESP

Z poważaniem

DYREKTOR
KRAJOWEJ SZKOŁY SĄDOWNICTWA I PROKURATURY

dr hab. Małgorzata Manowska
sędzia Sądu Najwyższego

/pismo podpisane podpisem elektronicznym/