

Administrator danych osobowych - Uniwersytet Jagielloński, realizując art. 34 RODO informuje o naruszeniu ochrony danych osobowych przetwarzanych na Wydziale Geografii i Geologii UJ w związku z nieuprawnionym dostępem osoby postronnej do systemów informatycznych UJ. Dostęp do wspomnianych systemów został umożliwiony poprzez udostępnienie zarządzania kontem jednego z nauczycieli akademickich Uczelni i skutkowało możliwością przetwarzania danych osobowych administrowanych w Uniwersytecie przez osobę niebędącą pracownikiem. Osoba nieupoważniona mogła mieć dostęp do systemów informatycznych od semestru letniego roku akademickiego 2022/23.

Zakres danych stanowiących przedmiot naruszenia obejmuje dane studentów oraz doktorantów UJ, w tym dane uczestników wymiany akademickiej CEEPUS, dane osobowe pracowników Uczelni oraz osób współpracujących z Uniwersyteciem na mocy zawartych umów. Nieuprawniona osoba mogła mieć dostęp do imion i nazwisk, wizerunku, danych adresowych, rodzaju i numeru dokumentu potwierdzającego tożsamość, dat urodzenia oraz numeru PESEL, adresu email, numeru telefonu oraz informacji o wydziale, roku i kierunku studiów, a także o postępach w nauce. Nieuprawniona osoba mogła mieć również dostęp do informacji o stanie zdrowia uczestników wymiany CEEPUS oraz studentów, z którymi zajęcia prowadził nauczyciel akademicki.

Administrator nie jest w stanie zapewnić, że nieuprawniona osoba nie pobrała wyżej wymienionych danych osobowych i nie wykorzystała lub nie wykorzysta ich w przyszłości. W celu zminimalizowania skutków naruszenia Administrator zaleca niezwłoczne zastrzeżenie numeru PESEL. Zastrzeżenia można dokonać w systemie [mObywatel.gov.pl](https://mObywatel.gov.pl) lub osobiście stawiając się w urzędzie gminy. Ponadto Administrator zaleca założenie konta w systemie informacji kredytowej BIK celem monitorowania prób uzyskania kredytu oraz zgłoszenie faktu naruszenia danych właściwym organom i bankowi prowadzącemu Państwa rachunek bankowy w celu zapobieżenia tzw. „kradzieży tożsamości”.

Przez „kradzież tożsamości” należy rozumieć posłużenie się Państwa danymi osobowymi w celu ukrycia swojej tożsamości (np. w przypadku otrzymania mandatu), zawarcia w Państwa imieniu umowy, założenia z wykorzystaniem Państwa danych konta w serwisie internetowym, wykorzystania Państwa danych do zarejestrowania karty telefonicznej typu prepaid, która może posłużyć do celów przestępczych, a także innej próby „podszycia” się pod Państwa. Pobrane dane mogą zostać wykorzystane do zaciągnięcia przez osoby trzecie na Państwa szkodę zobowiązań w instytucjach bankowych oraz pozabankowych. Utrata kontroli nad danymi osobowymi może także skutkować ograniczeniem Państwa praw, stratą finansową, dyskryminacją lub naruszeniem dobrego imienia.

W celu zminimalizowania skutków naruszenia Administrator niezwłocznie po powzięciu informacji o naruszeniu, zablokował dostęp do konta pracownika, tym samym odcinając możliwość dostępu do uczelnianych systemów informatycznych agregujących dane osobowe. Wobec pracownika wszczęto procedurę pociągnięcia go do odpowiedzialności pracowniczej. Uczelnia złożyła zawiadomienie o zdarzeniu oraz o podjętych środkach zaradczych do Urzędu Ochrony Danych Osobowych, a także podjęła decyzję o niezwłocznym zawiadomieniu organów ścigania.

Administrator zaleca szczególną ostrożność przy otwieraniu wiadomości otrzymywanych od niezidentyfikowanych osób, nieotwieranie załączonych plików oraz powstrzymanie się od klikania w widniejące w wiadomościach linki z odniesieniami do innych stron. W przypadku korespondencji otrzymywanej z banków lub dostawców usług, Inspektor Ochrony Danych zaleca każdorazowe upewnienie się, że odnośna strona rzeczywiście jest oficjalną stroną banku, w którym posiadacie Państwo rachunek rozliczeniowy lub dostawcy usług, a w przypadku wezwań do niezwłocznej zapłaty czy informacji o zaległościach i związanej z nimi windykacji, telefoniczny kontakt z pracownikiem Państwa banku lub dostawcy usług. Ponadto Inspektor zaleca ostrożność w przypadku otrzymania wiadomości wzywającej do podania

haseł dostępu do Państwa profili założonych u innych operatorów np. profil zaufany, konto pacjenta, Tauron, PGNiG, administrator poczty elektronicznej, u którego posiadacie Państwo założone konto lub skrzynkę pocztową itp.

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

Również w przypadku dodatkowych pytań lub wątpliwości prosimy o kontakt z Inspektorem Danych Osobowych: mgr inż. Monika Tokarczyk tel. 12 663 12 25 lub [iod@uj.edu.pl](mailto:iod@uj.edu.pl)

Niniejszy komunikat został przygotowany zgodnie z wymogami 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) Dz. U. UE. L. 2016.119.1. z dnia 4 maja 2016 r.