

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Uniwersytet Przyrodniczy w Poznaniu

Leśny Zakład doświadczalny Murowana Goślina, ul. Rogozińska 38

62-095 Murowana Goślina

Murowana Goślina, 05.10.2026 r.

Szanowni Państwo,

działając na podstawie art. 34 ust. 1 i 2 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 („RODO”), informujemy o wystąpieniu naruszenia ochrony danych osobowych.

1. Charakter naruszenia

W dniu **16.01.2026 r.** stwierdziliśmy nieuprawniony dostęp do służbowego konta e-mail należącego do Leśnego Zakładu Doświadczalnego Murowana Goślina. Osoba nieuprawniona uzyskała dostęp do zawartości skrzynki pocztowej, w której znajdowała się korespondencja prowadzona z Państwem. Nieuprawniona osoba uzyskała dostęp do skrzynki e-mail oraz pobrała jej zawartość.

2. Jakie dane mogły zostać objęte naruszeniem

W treści wiadomości e-mail oraz załącznikach mogły znajdować się dane osobowe, w szczególności:

- imię i nazwisko,
- adres zamieszkania,
- adres e-mail,
- numer telefonu,
- numer dokumentu tożsamości,
- numer PESEL,
- inne informacje przekazane w korespondencji.

Na obecnym etapie ustaleń **nie stwierdzono**, aby dane zostały wykorzystane przez osoby nieuprawnione. Sam fakt wystąpienia naruszenia powoduje jednak konieczność

poinformowania Państwa o możliwym ryzyku oraz o środkach podjętych w celu ograniczenia jego skutków.

3. Możliwe konsekwencje naruszenia ochrony danych osobowych

- w związku z naruszeniem poufności takich danych jak imię, nazwisko oraz nr PESEL, osoby trzecie mogą podejmować próby posłużenia się Pani/Pana danymi w celu zaciągnięcia zobowiązań kredytów/pożyczek;
- naruszenie prywatności lub poufności korespondencji;
- wykorzystanie danych przez osoby nieuprawnione w celu podszywania się pod osobę, której dane dotyczą;
- próby kontaktu telefonicznego, elektronicznego lub korespondencyjnego z wykorzystaniem uzyskanych danych, w celu wyłudzenia pieniędzy, haseł, kodów autoryzacyjnych lub innych danych/informacji;
- kierowanie wiadomości typu phishing lub innych prób socjotechnicznych;
- możliwość naruszenia dobrego imienia, prywatności lub innych praw osoby, której dane dotyczą.

4. Środki zastosowane przez Administratora

Niezwłocznie po stwierdzeniu naruszenia Administrator podjął działania mające na celu wyjaśnienie zdarzenia, jego zatrzymanie oraz ograniczenie ewentualnych negatywnych konsekwencji.

W szczególności:

- dokonano identyfikacji źródła oraz charakteru naruszenia;
- zabezpieczono system, dokumentację, logi dotyczące zdarzenia;
- zablokowano możliwość dalszego nieuprawnionego dostępu do danych;
- zawiadomiono osoby, których dane osobowe mogły zostać objęte naruszeniem ochrony danych osobowych;
- zawiadomiono Urząd Ochrony Danych Osobowych;
- zmieniono stary system pocztowy na system poczty elektronicznej z dwuetapową autoryzacją;
- podjęto działania organizacyjne mające ograniczyć ryzyko wystąpienia podobnego zdarzenia w przyszłości;

- prowadzony jest monitoring czy dane, do których miały dostęp osoby nieuprawnione nie pojawiły się w Internecie.

5. Środki proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia

W celu ograniczenia potencjalnego ryzyka zalecamy zachowanie szczególnej ostrożności w przypadku otrzymywania nietypowych wiadomości e-mail, SMS, połączeń telefonicznych lub korespondencji, w których nadawca powołuje się na dane osobowe objęte niniejszym naruszeniem.

W szczególności rekomendujemy:

- z uwagi na fakt, że naruszeniem mógł zostać objęty również numer PESEL, zalecamy zastrzeżenie numeru PESEL oraz zachowanie szczególnej ostrożności przy zawieraniu umów i dokonywaniu czynności wymagających potwierdzenia tożsamości;
- nieprzekazywanie osobom kontaktującym się telefonicznie lub elektronicznie dodatkowych danych osobowych, haseł, kodów dostępu ani danych uwierzytelniających bez uprzedniego potwierdzenia tożsamości rozmówcy;
- zachowanie ostrożności wobec wiadomości zawierających linki do stron internetowych lub załączniki, zwłaszcza jeżeli wiadomość wymaga pilnego podania dodatkowych danych;
- weryfikowanie autentyczności wiadomości i żądań poprzez kontakt z daną instytucją za pośrednictwem oficjalnych kanałów komunikacji;
- zmianę hasła, jeżeli w ramach naruszenia mogły zostać ujawnione dane umożliwiające dostęp do konta lub systemu, oraz niestosowanie tego samego hasła w kilku usługach;
- obserwowanie rachunków, kont oraz usług, których dane mogą pozostawać w związku z zakresem informacji objętych naruszeniem;
- niezwłoczne zgłoszenie Administratorowi wszelkich podejrzanych prób kontaktu lub zdarzeń mogących pozostawać w związku z naruszeniem.

6. Dalsze działania Administratora

Administrator kontynuuje analizę zdarzenia oraz wdraża dodatkowe rozwiązania techniczne i organizacyjne mające na celu ograniczenie ryzyka wystąpienia podobnego naruszenia w przyszłości.

W szczególności planowane lub realizowane są:

- współpraca z Urzędem Ochrony Danych Osobowych w zakresie naruszenia,
- dalsze prace, które mają na celu poprawę bezpieczeństwa systemów informatycznych i procedur obowiązujących u administratora;
- okresowe kontrole w zakresie korzystania przez pracowników z poczty elektronicznej.

6. Dane kontaktowe

W przypadku pytań dotyczących naruszenia ochrony danych osobowych lub potrzeby uzyskania dodatkowych informacji prosimy o kontakt z Inspektorem Ochrony Danych:

e-mail: iod@up.poznan.pl

telefon: +48 506 396 357