UNIWERSYTET WARSZAWSKI

Inspektor Ochrony Danych

Warszawa, dnia 18 listopada 2019 roku

IOD-042-189/2019

Szanowni Państwo
Dziekani Wydziałów,
Kierownicy Jednostek Organizacyjnych,
Samorząd Studentów
Uniwersytetu Warszawskiego

Szanowni Państwo,

działając na podstawie art. 39 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. Urz. UE L 119 z 04.05.2016 r., str. 1, z późn. zm.), dalej „RODO", oraz § 5 Zarządzenia nr 51 Rektora Uniwersytetu Warszawskiego z dnia 15 maja 2018 r. w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim (Monitor UW z 2018, poz. 142), pragnę zwrócić Państwa **uwagę na konieczność stałego nadzorowania przestrzegania zasad bezpieczeństwa danych osobowych na Uniwersytecie Warszawskim**.

W dniu 14 listopada br. na stronie internetowej Szkoły Głównej Gospodarstwa Wiejskiego (SGGW) pojawiła się informacja o zaistniałym naruszeniu ochrony danych osobowych kandydatów na studia, studentów i absolwentów tej uczelni. Do naruszenia doszło w wyniku kradzieży prywatnego komputera przenośnego, na którym przechowywane były przez pracownika SGGW dokumenty i dane uczestników rekrutacji na studia z kilku lat.[1] Z informacji podanych w późniejszym komunikacie rzecznika prasowego SGGW wynika, że nie są znane ani dokładna liczba osób ani zakres danych osobowych objętych naruszeniem. Naruszenie zostało zgłoszone zarówno do Prezesa Urzędu Ochrony Danych Osobowych, jak i organów ścigania.[2]

---

[1] https://www.sggw.pl/aktualnosci/komunikat-o-naruszeniu-danych-osobowych
[2] https://www.sggw.pl/aktualnosci/dla-kandydatow_/komunikat-rzecznika-prasowego-sggw

ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa
tel.: 22 55 22 042
e-mail: iod@adm.uw.edu.pl

W związku z opisanym incydentem pragnę przypomnieć i jeszcze raz zwrócić Państwa uwagę na konieczność przestrzegania zasad ochrony danych osobowych wynikających z przepisów RODO, jak i zasad bezpieczeństwa określonych w „Polityce Ochrony Danych Osobowych na Uniwersytecie Warszawskim", takich jak w szczególności:

1. **Zasada ochrony informacji służbowej/służbowych dokumentów** – zabronione jest kopiowanie i wynoszenie dokumentów służbowych (oryginałów, kopii, wersji elektronicznych) oraz ich przesyłanie drogą elektroniczną w innym celu niż służbowy. Dane osobowe powinny być zawsze przetwarzane z wykorzystaniem wyłącznie urządzeń służbowych zapewnionych pracownikowi przez Uniwersytet Warszawski.
2. **Zasada wiedzy koniecznej** – ograniczenie dostępu użytkownika jedynie do tych informacji, które są niezbędne do wykonywania obowiązków lub zadań.
3. **Zasada zamkniętego pomieszczenia** – osoby nieuprawnione nie pozostają same w pomieszczeniu pod nieobecność pracownika Uniwersytetu Warszawskiego. Drzwi zamykane są na klucz, który pozostaje pod nadzorem (nie w zamku).
4. **Zasada czystego biurka/drukarki/kosza** – dokumenty papierowe oraz nośniki danych, nie pozostają bez nadzoru i są niszczone przy użyciu niszczarki przed wyrzuceniem.
5. **Zasada czystego ekranu** – użytkownik blokuje komputer przed każdym opuszczeniem pomieszczenia. W przypadku dłuższej nieobecności w pomieszczeniu konieczne jest wylogowanie z systemu.
6. **Zasada minimalizacji danych** – dane osobowe powinny być adekwatne, stosowne do celu przetwarzania danych osobowych oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Szczegółowe zasady bezpieczeństwa dotyczące korzystania ze służbowych komputerów przenośnych oraz innych nośników danych zostały określone w „Instrukcji Zarządzania Systemem Informatycznym Przetwarzającym Dane Osobowe na Uniwersytecie Warszawskim". Pracownicy wykorzystujący przenośne komputery, a także inne urządzenia i nośniki (np. pendrive, płyta CD/DVD, karta pamięci) zobowiązani są m.in. do **stosowania bezpiecznych haseł** oraz **mechanizmów kryptograficznych**, które uniemożliwiają uzyskanie dostępu do zawartości dysków i innych nośników danych osobom nieuprawnionym (np. szyfrowanie dysków i pamięci przenośnych programem Bitlocker).

Samo hasło do systemu Windows nie stanowi skutecznego zabezpieczenia, ponieważ niezaszyfrowany dysk można odczytać bez użycia hasła np. wyjmując go z komputera.

W związku z powyższym, zwracam się z uprzejmą prośbą o dokonanie przeglądu stosowanych w Państwa jednostkach zabezpieczeń ze szczególnym uwzględnieniem poniższych punktów:

1. Czy na wszystkich komputerach, smartfonach oraz nośnikach pamięci stosowane są zabezpieczenia kryptograficzne oraz bezpieczne hasła?
2. Czy pracownicy przetwarzają dane osobowe wyłącznie na służbowych komputerach, smartfonach oraz nośnikach pamięci?
3. Czy komputery, smartfony oraz nośniki pamięci są przenoszone przez pracowników poza stanowisko pracy wyłącznie w sytuacjach, kiedy jest to niezbędne?
4. Czy przestrzegana jest zasada czystego biurka oraz zasada zamkniętego pomieszczenia?

Pragnę również zwrócić Państwa uwagę, że niestosowanie się przez pracowników do zasad bezpieczeństwa wynikających ze wskazanych wyżej dokumentów może w niektórych przypadkach stanowić nawet ciężkie naruszenie obowiązków pracowniczych. Ponadto, stosowanie niedostatecznych zabezpieczeń lub nieprzestrzeganie zasad bezpieczeństwa może samo w sobie zostać uznane przez Prezesa Urzędu Ochrony Danych Osobowych za naruszenie przepisów RODO, co może skutkować nałożeniem na Uniwersytet Warszawski administracyjnej kary pieniężnej w wysokości do 100 000 złotych.

Z wyrazami szacunku

UNIWERSYTET WARSZAWSKI
Inspektor Ochrony Danych
Ferenc
mgr Dominik Ferenc