

Warszawa, dnia 22 kwietnia 2026 roku

## **KOMUNIKAT**

### **w sprawie zasad minimalizacji i bezpieczeństwa danych osobowych**

W związku z zaistniałym incydem naruszenia ochrony danych osobowych przypominamy o obowiązku ścisłego przestrzegania poniższych zasad bezpieczeństwa informacji oraz ochrony danych osobowych.

#### **Kluczowe zasady postępowania**

##### **1. Minimalizacja danych**

Należy zawsze przetwarzać dane osobowe w najmniejszym możliwym zakresie, który umożliwia realizację konkretnych celów przetwarzania. Wszystkie dane osobowe, które nie są bezwzględnie niezbędne do wykonywania obowiązków służbowych należy uznać za dane nadmiarowe i nie należy ich przechowywać na urządzeniach służbowych.

##### **2. Zakaz przechowywania danych zbędnych**

Zabronione jest przechowywanie danych osobowych bez wyraźnie określonego celu i podstawy prawnej. Jeżeli cele przetwarzania konkretnych danych zostały już w pełni zrealizowane, to niedopuszczalne jest dalsze przechowywanie tych informacji „na zapas”, „na przyszłość”, „na wszelki wypadek”, itd.

##### **3. Usuwanie danych nadmiarowych oraz zbędnych**

Jeżeli zostanie stwierdzone, że konkretne dane osobowe są nadmiarowe względem określonych celów przetwarzania lub cele przetwarzania tych danych stały się nieaktualne, pliki z tymi danymi należy niezwłocznie usunąć z urządzeń służbowych. Dotyczy to w szczególności plików zduplikowanych oraz kopii zapasowych, które wolno tworzyć jedynie w stosunku do aktualnie przetwarzanych danych.

##### **4. Kopie zapasowe i dane archiwalne**

Kopie zapasowe aktualnie przetwarzanych danych osobowych oraz lokalne archiwa danych:

- muszą być tworzone na podstawie konkretnych celów przetwarzania oraz podstaw prawnych,
- muszą być odpowiednio zabezpieczone, m.in. za pomocą szyfrowania,
- powinny być przenoszone do wyznaczonych repozytoriów zapewniających bezpieczeństwo.

## 5. Przegląd urządzeń i zasobów sieciowych

Użytkownicy są zobowiązani do samodzielnego okresowego przeglądu danych przechowywanych na:

- komputerach służbowych,
- dyskach sieciowych i lokalnych,
- przenośnych nośnikach danych (np. pendrive, karta SD, płyty CD/DVD, itd.),
- innych wykorzystywanych zasobach cyfrowych (np. Sharepoint, Dysk Google, itd.).

## 6. Przegląd korespondencji elektronicznej

Użytkownicy uniwersyteckiej poczty elektronicznej są zobowiązani do:

- regularnego przeglądu zawartości skrzynek poczty elektronicznej,
- usuwania na bieżąco zbędnych wiadomości i załączników zawierających dane osobowe,
- stosowania zasady minimalizacji danych przy prowadzeniu korespondencji elektronicznej.

**Powyższe działania mają na celu:**

- ograniczenie ryzyka wystąpienia ponownego wycieku danych osobowych,
- zwiększenie poziomu bezpieczeństwa informacji,
- zapewnienie zgodności działań z zasadami minimalizacji danych oraz ograniczenia przechowywania określonymi w przepisach prawa (RODO),
- poprawę zarządzania informacją w jednostkach.



**Przechowywanie danych musi być celowe, adekwatne i ograniczone do niezbędnego zakresu.**