



BIULETYN PRAWNY

UNIwersYTETU MIKOŁAJA KOPERNIKA W TORUNIU

Rok 2024; poz. 149

ZARZĄDZENIE Nr 66

Rrektora Uniwersytetu Mikołaja Kopernika w Toruniu

z dnia 13 maja 2024 r.

w sprawie określenia procedur nadawania upoważnień do przetwarzania danych osobowych na Uniwersytecie Mikołaja Kopernika w Toruniu

Na podstawie § 52 ust. 3 uchwały Nr 37 Senatu UMK z dnia 16 kwietnia 2019 r. Statut Uniwersytetu Mikołaja Kopernika w Toruniu (Biuletyn Prawny UMK z 2024 r., poz. 10)

z a r z ą d z a s i ę, co następuje:

Rozdział 1 **Postanowienia ogólne**

§ 1

1. Zarządzenie określa procedury nadawania upoważnień do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych dotyczy każdego pracownika Uniwersytetu Mikołaja Kopernika w Toruniu, zwanego dalej „Uniwersytetem”, niezależnie od formy prawnej zatrudnienia, w zakresie obowiązków którego znajdują się czynności wymagające dostępu do danych osobowych.
3. Ilekroć w zarządzeniu jest mowa o pracowniku, rozumie się przez to również osoby zatrudnione lub współpracujące z Uniwersytetem w oparciu o inny niż umowa o pracę stosunek prawny.

Rozdział 2 **Upoważnienie generalne**

§ 2

1. Mocą zarządzenia, w imieniu Administratora Danych Osobowych rektor nadaje upoważnienie do przetwarzania danych osobowych wszystkim pracownikom Uniwersytetu, z zastrzeżeniem § 3.
2. Zakres upoważnienia obejmuje wszystkie czynności wynikające z powierzonych obowiązków służbowych, których wykonanie wiąże się z dostępem do danych osobowych.
3. Poza przypadkami opisanymi w zarządzeniu nie jest wymagana inna, pisemna forma upoważnienia do przetwarzania danych osobowych.

Rozdział 3

Udokumentowane upoważnienie

§ 3

1. W przypadkach, o których mowa w zarządzeniu wymagane jest nadanie upoważnienia do przetwarzania danych osobowych w formie upoważnienia udokumentowanego.
2. Upoważnienie udokumentowane stanowi dokument elektroniczny opatrzony kwalifikowanym podpisem elektronicznym osoby uprawnionej do wydania upoważnienia.
3. Systemem informatycznym wspierającym proces zarządzania upoważnieniami jest system Elektronicznego Zarządzania Dokumentacją PUW, zwany dalej „systemem EZD”.
4. Upoważnienie udokumentowane jest upoważnieniem imiennym wystawianym dla danego pracownika i dotyczy całego obszaru jego obowiązków służbowych związanych z przetwarzaniem danych osobowych.
5. Upoważnienie udokumentowane wydawane jest w przypadku przetwarzania danych osobowych szczególnych kategorii, wymienionych w art. 9 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., tj. dla danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej.

§ 4

1. Upoważnienia udokumentowane podlegają wpisowi do rejestru.
2. Rejestr upoważnień udokumentowanych prowadzony jest w systemie EZD przez Inspektora Ochrony Danych.

§ 5

1. Upoważnienie udokumentowane wystawiane jest bezterminowo..
2. Upoważnienie udokumentowane wygasa w szczególności w przypadku:
 - 1) rozwiązania stosunku prawnego łączącego Uniwersytet z pracownikiem;
 - 2) zmiany stanowiska pracy lub zakresu obowiązków w przypadku, gdy nowe obowiązki nie wymagają dostępu do danych osobowych objętych upoważnieniem udokumentowanym;
 - 3) przewidywanej nieobecności pracownika przez okres dłuższy niż 30 dni.

Rozdział 4

Upoważnienie szczególne

§ 6

1. Upoważnienie szczególne przybiera formę upoważnienia udokumentowanego.
2. Upoważnienie szczególne wystawia się dla osób pełniących funkcje:
 - 1) rektora i prorektorów;
 - 2) kanclerza i zastępców kanclerza;
 - 3) kvestora i zastępców kvestora;
 - 4) pracowników zatrudnionych w kancelarii albo obsługujących punkt kancelaryjny;
 - 5) Inspektora Ochrony Danych.

§ 7

1. Rektor otrzymuje imienne upoważnienie udokumentowane podpisane przez przewodniczącego Rady Uniwersytetu.

2. Upoważnienie rektora wygasa z chwilą upływu kadencji, na którą został powołany, wygaśnięcia mandatu lub odwołania.
3. Upoważnienie rektora obejmuje swoim zakresem dostęp do wszelkich danych osobowych niezbędnych do wykonywania sprawowanej funkcji.

§ 8

1. Prorektor otrzymuje imienne upoważnienie udokumentowane podpisane przez rektora.
2. Upoważnienie prorektora wygasa z chwilą upływu kadencji, na którą został powołany lub odwołania.
3. Upoważnienie prorektora obejmuje swoim zakresem dostęp do wszelkich danych osobowych niezbędnych do wykonywania sprawowanej funkcji.

§ 9

1. Kanclerz i zastępcy kanclerza oraz kwestor i zastępcy kwestora otrzymują imienne upoważnienie udokumentowane podpisane przez rektora.
2. Upoważnienia kanclerza i zastępców kanclerza oraz kwestora i zastępców kwestora wygasają z chwilą zakończenia zatrudnienia na tych stanowiskach.
3. Upoważnienie kanclerza i zastępców kanclerza oraz kwestora i zastępców kwestora obejmuje swoim zakresem dostęp do wszelkich danych osobowych niezbędnych do wykonywania powierzonych obowiązków.

§ 10

1. Pracownicy zatrudnieni w kancelarii albo obsługujący punkt kancelaryjny otrzymują imienne upoważnienie udokumentowane podpisane przez rektora.
2. Upoważnienie pracownika zatrudnionego w kancelarii albo obsługującego punkt kancelaryjny wygasa z chwilą zakończenia zatrudnienia w kancelarii albo obsługi punktu kancelaryjnego.
3. Upoważnienie pracownika zatrudnionego w kancelarii albo obsługującego punkt kancelaryjny obejmuje swoim zakresem dostęp do wszelkich danych osobowych niezbędnych do wykonywania powierzonych obowiązków.

§ 11

1. Inspektor Ochrony Danych otrzymuje imienne upoważnienie udokumentowane podpisane przez rektora.
2. Upoważnienie Inspektora Ochrony Danych wygasa z chwilą zakończenia zatrudnienia na tym stanowisku.
4. Upoważnienie Inspektora Ochrony Danych wynika z art. 38 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
3. W sprawach innych niż związane z wykonywaniem funkcji Inspektor Ochrony Danych podlega upoważnieniu na zasadach ogólnych.

Rozdział 5

Wystawianie i odwoływanie upoważnienia udokumentowanego

§ 12

1. O upoważnienie udokumentowane wnioskuje bezpośredni przełożony pracownika. Wzór wniosku o upoważnienie określa załącznik nr 1 do zarządzenia.
2. Wniosek przekazywany jest w systemie EZD do Inspektora Ochrony Danych.
3. Inspektor Ochrony Danych zakłada sprawę w EZD i gromadzi dokumentację, na którą składa się:
 - 1) oświadczenie o zachowaniu poufności, którego wzór stanowi załącznik nr 2 do zarządzenia;

- 2) oświadczenie o ukończeniu szkolenia wstępnego, którego wzór stanowi załącznik nr 3 do zarządzenia.
4. Za pozyskanie od pracownika stosownych oświadczeń, o których mowa w ust. 3 i przekazanie ich do Inspektora Ochrony Danych odpowiedzialny jest bezpośredni przełożony danego pracownika.
5. W przypadku spełnienia przez pracownika kryteriów, o których mowa w ust. 3, Inspektor Ochrony Danych przygotowuje dokument upoważnienia i przekazuje go w systemie EKD do podpisu rektora lub osoby przez niego upoważnionej.
6. W przypadku, gdy pracownik nie spełnia warunków, o których mowa w ust. 3, Inspektor Ochrony Danych wzywa do odbycia szkolenia lub podpisania oświadczenia o poufności..
7. Po podpisaniu upoważnienia jest ono odsyłane do Inspektora Ochrony Danych, który dokonuje jego rejestracji w systemie EKD i kończy sprawę, jednocześnie powiadamiając pracownika, którego sprawa dotyczy oraz jego przełożonego o wydaniu upoważnienia.

§ 13

1. W przypadkach określonych zarządzeniem bezpośredni przełożony niezwłocznie po powzięciu informacji o okolicznościach będących podstawą wygaśnięcia upoważnienia udokumentowanego, informuje Inspektora Ochrony Danych za pośrednictwem systemu EKD.
2. Inspektor Ochrony Danych przygotowuje dokument stwierdzający wygaśnięcie upoważnienia udokumentowanego i przesyła go do podpisu rektora lub osoby przez niego upoważnionej.
3. Po podpisaniu dokumentu stwierdzającego wygaśnięcie upoważnienia udokumentowanego jest on odsyłany do Inspektora Ochrony Danych, który dokonuje stosownej adnotacji w rejestrze upoważnień i dołącza do sprawy upoważnienia, którego dotyczy, jednocześnie informując bezpośredniego przełożonego pracownika tracącego upoważnienie.

Rozdział 6

Ograniczenia zakresu upoważnień

§ 14

1. Niedozwolone jest żądanie przez pracownika dostępu do danych osobowych na podstawie posiadanego upoważnienia w zakresie szerszym niż jest to niezbędne do wykonywania powierzonych mu zadań.
2. Upoważnienie do przetwarzania danych osobowych ogranicza się do danych niezbędnych do realizacji zadań wynikających z zakresu obowiązków lub powierzonych przez przełożonego.

Rozdział 7

Udokumentowane polecenie

§ 15

Udokumentowane polecenie przetwarzania danych osobowych jest podstawą do przetwarzania danych osobowych przez każdego pracownika Uniwersytetu.

§ 16

Udokumentowanym poleceniem jest:

- 1) pisemny zakres obowiązków (w tym w formie elektronicznej potwierdzony podpisem elektronicznym);
- 2) postanowienia umowy cywilno-prawnej lub innego aktu (uchwały, zarządzenia, mianowania, powołania);

- 3) polecenie przełożonego wystosowane na piśmie, mailowo lub przy pomocy innego środka komunikacji umożliwiającego jego udokumentowanie.

§ 17

1. W przypadku, gdy polecenie przełożonego wykracza poza pisemny zakres obowiązków, o którym mowa w § 16 pkt 1, przełożony ma obowiązek wydać polecenie w sposób określony w § 16 pkt 3.
2. Pracownik, który otrzyma polecenie wykraczające poza jego pisemny zakres obowiązków w sposób inny niż określony w § 16 pkt 3, ma obowiązek powstrzymania się od jego wykonania do czasu otrzymania tego polecenia w wymaganej formie.

Rozdział 8

Oświadczenie o zachowaniu poufności

§ 18

1. Każdy pracownik Uniwersytetu niezwłocznie po ukończeniu szkolenia wstępnego podpisuje oświadczenie o zachowaniu poufności.
2. Wzór oświadczenia udostępniany jest bezpośredniemu przełożonemu danego pracownika przez Inspektora Ochrony Danych.

§ 19

1. Oświadczenie o zachowaniu poufności przyjmuje formę papierową.
2. Oświadczenie jest podpisywane własnoręcznie przez pracownika.
3. Oświadczenie przechowywane jest w teczce osobowej pracownika, a w przypadku umów cywilno-prawnych dołączane i przechowywane wraz z umową.
4. Oświadczenie osoby, którą z Uniwersytetem łączy inny akt niż wymienione w § 16 pkt. 2 i 3 przechowuje się wraz z tym aktem.

§ 20

1. Za odebranie od pracownika oświadczenia o zachowaniu poufności odpowiedzialny jest jego bezpośredni przełożony.
2. Brak podpisanego oświadczenia o zachowaniu poufności uniemożliwia dostęp do danych osobowych.

Rozdział 9

Dostęp do danych osobowych pozostających w dyspozycji jednostek organizacyjnych i komórek administracji Uniwersytetu

§ 21

Administratorem Danych Osobowych jest Uniwersytet i wszystkie jego jednostki organizacyjne i komórki administracji mają dostęp do przetwarzanych przez Uniwersytet danych osobowych na takich samych zasadach.

§ 22

Dostęp do danych osobowych pozostających w dyspozycji poszczególnych jednostek organizacyjnych i komórek administracji Uniwersytetu wynika bezpośrednio z przypisanych im ról i zadań, zgodnie z obowiązującymi przepisami na Uniwersytecie.

§ 23

W przypadku, gdy pracownik jednostki organizacyjnej lub komórki administracji Uniwersytetu do wykonania powierzonych mu zadań potrzebuje uzyskać dostęp do danych osobowych znajdujących się w gestii innej jednostki lub komórki, o dane te w sposób udokumentowany –

procedurę wynikającą z § 16 pkt 3 stosując się odpowiednio – występuje osoba kierująca daną jednostką organizacyjną lub komórką administracji do osoby kierującej jednostką lub komórką, w gestii której znajdują się dane osobowe.

Rozdział 10

Szkolenia wstępne

§ 24

Każdy nowo zatrudniony pracownik, niezależnie od formy stosunku prawnego, zobowiązany jest do ukończenia szkolenia wstępnego z zakresu ochrony danych osobowych i zapoznania się z wewnętrznymi procedurami w tym zakresie.

§ 25

1. Za przygotowanie szkoleń wstępnych z zakresu ochrony danych osobowych, odpowiedzialny jest Inspektor Ochrony Danych.
2. Szkolenia wstępne mogą być przeprowadzane w formie:
 - 1) stacjonarnej,
 - 2) online,
 - 3) elektronicznej na zasadzie samokształcenia.

§ 26

1. W celu ukończenia szkolenia wstępnego z zakresu ochrony danych osobowych, pracownik w dniu rozpoczęcia pracy kontaktuje się z Inspektorem Ochrony Danych.
2. Szkolenie, w formie ustalonej przez Inspektora Ochrony Danych, należy ukończyć najpóźniej dnia następnego po dniu rozpoczęcia pracy.
3. Ukończenie szkolenia wstępnego jest warunkiem uzyskania upoważnienia do przetwarzania danych osobowych.

§ 27

1. Pracownik, w terminie do 14 dni od rozpoczęcia pracy zobowiązany jest do zapoznania się z wewnętrznymi procedurami w zakresie ochrony danych osobowych.
2. Procedury, o których mowa w ust. 1 znajdują się w repozytorium dokumentów pod adresem: <https://dokumenty.umk.pl> i dostępne są po uprzednim zalogowaniu przez centralny punkt logowania, w sekcji Ochrona Danych Osobowych.

Rozdział 11

Postanowienia końcowe

§ 28

1. Rektor może udzielić, w formie pisemnej, pełnomocnictwa do podpisywania upoważnień w jego imieniu.
2. Wszelkie upoważnienia wydane do dnia wejścia w życie zarządzenia tracą moc po upływie miesiąca od jego opublikowania w Biuletynie Prawnym UMK.
3. W celu wydania nowych, zgodnych z zarządzeniem, upoważnień kierownicy jednostek organizacyjnych lub komórek administracji Uniwersytetu przygotowują i przekazują do Inspektora Ochrony Danych w systemie EZD listy pracowników, dla których wymagane jest upoważnienie udokumentowane.
4. Po weryfikacji list Inspektor Ochrony Danych przygotowuje i przekazuje do podpisu rektora upoważnienia udokumentowane zgodnie z procedurą opisaną zarządzeniem.

§ 29

1. Z chwilą wejścia w życie zarządzenia system BDO zostaje wyłączony, a jego bazy danych zarchiwizowane.
2. Archiwum baz danych systemu BDO, w formie elektronicznej, przechowuje się przez okres 5 lat licząc od pierwszego stycznia roku następującego po roku, w którym zaczęło obowiązywać zarządzenie.

§ 30

Zarządzenie wchodzi w życie z dniem 1 czerwca 2024 r.

REKTOR

prof. dr hab. Andrzej Sokala