Zarządzenie Nr 37/2014/2015
Rektora Uniwersytetu Kazimierza Wielkiego
z dnia 21 kwietnia 2015 r.

zmieniające zarządzenie Nr 68/2012/2013 Rektora UKW w sprawie wprowadzenia instrukcji regulujących zagadnienia ochrony danych osobowych oraz pracy w systemach informatycznych służących do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego

Na podstawie art. 66 ust. 1 i 2 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2012 r., poz. 572 z późn. zm.), ustawy z dnia 29 sierpnia 1997 r. o Ochronie Danych Osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004, Nr 100, poz. 1024)

zarządzam,

co następuje:

§ 1

W Zarządzeniu Nr 68/2012/2013 Rektora UKW z dnia 29 kwietnia 2013 roku w sprawie wprowadzenia instrukcji regulujących zagadnienia ochrony danych osobowych oraz pracy w systemach informatycznych służących do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego wprowadzam następujące zmiany:

1. **W załączniku Nr 1 –** Polityka Bezpieczeństwa przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego:

   1) **§ 3** otrzymuje następujące brzmienie:

   „1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Rektora (administratora danych).
   2. Wnioski o nadanie upoważnienia do przetwarzania danych osobowych opiniuje Administrator Bezpieczeństwa Informacji.”

   2) **§ 4** otrzymuje następujące brzmienie:

   „1. Upoważnienie nadawane jest na pisemny wniosek przełożonego upoważnianej osoby, przedkładany Administratorowi Bezpieczeństwa Informacji. Wniosek powinien zawierać w szczególności: nazwisko i imię pracownika, nazwę stanowiska pracy, opis stanowiska lub zakresu obowiązków związanych z przetwarzaniem danych osobowych, określenie wnioskowanego zakresu danych osobowych oraz sposobu ich przetwarzania.
   2. Jeżeli osoba mająca przetwarzać dane osobowe nie jest pracownikiem Uczelni (realizacja zadań na podstawie umowy cywilno-prawnej, odbywanie stażu i inne), z wnioskiem o wydanie dla niej upoważnienia występuje kierownik jednostki zlecającej upoważnianej osobie przetwarzanie danych osobowych. Wniosek powinien zawierać

w szczególności: nazwisko i imię osoby mającej otrzymać upoważnienie, określenie zakresu wykonywanych czynności związanych z przetwarzaniem danych osobowych, określenie wnioskowanego zakresu danych osobowych i sposobu ich przetwarzania, uzasadnienie wniosku oraz, jeśli jest znany, termin ustania ważności upoważnienia.
3. Administrator Bezpieczeństwa Informacji zobowiązany jest zaopiniować wniosek w terminie 7 dni od dnia jego otrzymania. W szczególnych przypadkach termin ten może ulec wydłużeniu.
4. Administrator Bezpieczeństwa Informacji może:
1) zaopiniować wniosek pozytywnie,
2) zaopiniować nadanie ograniczonych uprawnień zawierających się we wnioskowanym zakresie,
3) zaopiniować wniosek negatywnie.
5. Opinię Administrator Bezpieczeństwa Informacji przekazuje osobie wnioskującej. W przypadku wydania opinii o ograniczeniu uprawnień lub opinii negatywnej, opinia musi być sporządzona w formie pisemnej i zawierać uzasadnienie.
6. Ostateczną decyzję o nadaniu upoważnienia podejmuje Rektor."

3) **§ 5** otrzymuje następujące brzmienie:

„1. Nadanie upoważnienia do przetwarzania danych osobowych (w szczególności w systemie informatycznym) obejmuje:
1) przeprowadzenie przez Administratora Bezpieczeństwa Informacji szkolenia w zakresie bezpieczeństwa danych osobowych oraz prawnych aspektów ochrony tych danych,
2) nadanie osobie przez Rektora pisemnego upoważnienia do przetwarzania danych osobowych, zawierającego zakres nadawanych uprawnień do przetwarzania danych osobowych, informację o zbiorze osób, do którego nadawane są uprawnienia, systemie informatycznym, w którym dane będą przetwarzane (jeśli dotyczy), datę nadania upoważnienia oraz, jeśli upoważnienie nadawane jest terminowo, datę wygaśnięcia upoważnienia,
3) w przypadku przetwarzania danych osobowych w wielostanowiskowym systemie informatycznym - nadanie osobie przez administratora systemu informatycznego identyfikatora oraz hasła, a także skonfigurowanie uprawnień w systemie.
2. W przypadku konieczności zmiany zakresu upoważnienia (inny zakres przetwarzania danych osobowych w określonym zbiorze, kolejny zbiór osób, zmiana stanowiska pracy przez pracownika) należy przedłożyć nowy wniosek o nadanie upoważnienia, stosując odpowiednio zapisy § 4.
3. W przypadku nadania nowego upoważnienia dotyczącego tego samego zbioru osób, moc traci poprzednie upoważnienie."

4) **§ 6** otrzymuje następujące brzmienie:

„1.Odebranie upoważnienia do przetwarzania danych osobowych może mieć miejsce, gdy:
1) z pracownikiem została rozwiązana (zakończona) umowa o pracę,
2) zakres obowiązków służbowych pracownika uległ zmianie, która spowodowała utratę potrzeby przetwarzania danych osobowych,
3) osoba spowodowała swoim celowym działaniem incydent mający negatywny wpływ na bezpieczeństwo przetwarzanych danych osobowych,
4) istnieje uzasadniona obawa, że przetwarzanie danych osobowych przez osobę wiąże

się z poważnym ryzykiem utraty poufności, integralności lub dostępności tych danych.
2. Odebranie uprawnień może nastąpić na wniosek:
1) Rektora,
2) przełożonego pracownika lub odpowiednio kierownika jednostki, o którym mowa w § 4 ust. 2,
3) kierownika Działu Kadr i Szkolenia,
4) Administratora Bezpieczeństwa Informacji.
3. Proces odebrania upoważnienia obejmuje:
1) przekazanie Administratorowi Bezpieczeństwa Informacji pisemnego wniosku o odebranie upoważnienia (za wyjątkiem sytuacji, gdy wnioskującym jest Administrator Bezpieczeństwa Informacji) z określeniem imienia i nazwiska osoby oraz jej identyfikatora w systemie informatycznym (jeśli osoba posiada dostęp do systemu informatycznego), a także przyczyny konieczności odebrania upoważnienia,
2) w przypadku posiadania przez osobę, której upoważnienie jest odbierane uprawnień do systemu informatycznego, przekazanie przez wnioskującego administratorowi systemu informatycznego polecenia unieważnienia hasła, zablokowania konta użytkownika, odebrania wszelkich uprawnień do systemu; administrator systemu winien możliwie szybko wykonać niezbędne czynności,
3) przekazanie przez Administratora Bezpieczeństwa Informacji złożonego wniosku o odebranie upoważnienia Rektorowi, który podejmuje decyzję o odebraniu upoważnienia,
4) poinformowanie przez Administratora Bezpieczeństwa Informacji wnioskodawcy o odebraniu osobie upoważnienia do przetwarzania danych osobowych."

5) **§ 7** otrzymuje następujące brzmienie:

„1. Upoważnienie do przetwarzania danych osobowych przygotowywane jest w dwóch egzemplarzach: po jednym dla upoważnianej osoby i dla Administratora Bezpieczeństwa Informacji. W przypadku nadania upoważnienia osobie, o której mowa w § 4 ust. 2, nie będącej pracownikiem Uczelni, przygotowywany jest trzeci egzemplarz upoważnienia, przechowywany w jednostce, której kierownik zlecał osobie przetwarzanie danych, występując z wnioskiem o nadanie upoważnienia.
2. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, obejmującą: imię i nazwisko osoby, datę nadania upoważnienia, datę ustania upoważnienia, zakres upoważnienia, identyfikator użytkownika w systemie informatycznym (jeśli dotyczy)."

6) **§ 9** otrzymuje następujące brzmienie:

„1. Przed dopuszczeniem do przetwarzania danych osobowych pracownik Uniwersytetu lub osoba, o której mowa w § 4 ust. 2, musi zostać przeszkolony w zakresie przepisów prawnych dotyczących ochrony danych osobowych oraz zasad ochrony danych osobowych obowiązujących w Uniwersytecie. Za zorganizowanie szkolenia odpowiada przełożony szkolonego pracownika lub odpowiednio kierownik jednostki, o którym mowa w § 4 ust. 2.
2. Szkolenie w szczególności powinno obejmować:
1) przedstawienie Ustawy o ochronie danych osobowych i jej wpływu na przebieg procesów związanych z przetwarzaniem danych osobowych w Uniwersytecie,
2) przedstawienie Rozporządzenia Ministra Spraw Wewnętrznych i Administracji,

3) przedstawienie przepisów wewnętrznych obowiązujących w Uniwersytecie, regulujących zasady ochrony danych osobowych,
4) przedstawienie praktycznych rozwiązań ochrony danych osobowych na danym stanowisku pracy.

3. Po odbytym szkoleniu przełożony pracownika lub odpowiednio kierownik jednostki, o którym mowa w § 4 ust. 2, może wystąpić do Rektora z wnioskiem o nadanie osobie upoważnienia do przetwarzania danych osobowych.

4. Oprócz szkolenia określonego w ust. 1 i 2, w poszczególnych jednostkach organizacyjnych prowadzone być powinny w miarę możliwości szkolenia okresowe (powtórzeniowe) oraz szkolenia przedstawiające zmiany w przepisach o ochronie danych osobowych lub zmiany zasad ochrony danych osobowych obowiązujących w Uniwersytecie."

2. **W załączniku Nr 2** – Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych – **Rozdział 2** otrzymuje następujące brzmienie:

„1. Przed dopuszczeniem do pracy w systemach informatycznych oraz do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez przełożonego, administratora systemu lub administratora bezpieczeństwa informacji z zasadami obowiązującymi podczas pracy w systemach informatycznych, przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Uniwersytecie wewnętrznymi regulacjami w tym zakresie.

2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych nadane przez Rektora.

3. Wydanie upoważnienia oraz rejestracja użytkownika w systemie informatycznym przetwarzającym dane osobowe następuje na wniosek przełożonego użytkownika.

4. Jeżeli osoba mająca przetwarzać dane osobowe nie jest pracownikiem Uczelni, z wnioskiem o wydanie dla niej upoważnienia występuje kierownik jednostki zlecającej upoważnianej osobie przetwarzanie danych osobowych.

5. Procedury wydawania i odwoływania upoważnień do przetwarzania danych osobowych realizowane są według następujących zasad:

1) przełożony użytkownika lub kierownik jednostki, o którym mowa w ust. 4, składa do Rektora pisemny wniosek o wydanie upoważnienia, który zawiera:
   a) imię i nazwisko użytkownika (osoby upoważnianej),
   b) w przypadku pracownika Uczelni, stanowisko zajmowane przez użytkownika,
   c) nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik ma uzyskać dostęp,
   d) zakres upoważnienia do przetwarzania danych osobowych,
   e) datę, z jaką upoważnienie ma być wydane,
   f) okres ważności upoważnienia lub informację o jego bezterminowości,
2) wniosek opiniowany jest przez administratora bezpieczeństwa informacji,
3) w przypadku nadania upoważnienia, jeden egzemplarz zostaje przekazany upoważnianemu użytkownikowi, drugi egzemplarz zostaje włączony do wykazu prowadzonego przez administratora bezpieczeństwa informacji,

4) jeżeli osoba, której nadano upoważnienie nie jest pracownikiem Uczelni, przygotowywany jest trzeci egzemplarz upoważnienia, przekazywany wnioskującemu o nadanie upoważnienia kierownikowi jednostki zlecającej upoważnianej osobie przetwarzanie danych osobowych,
5) po nadaniu upoważnienia do przetwarzania danych osobowych, administrator systemu informatycznego nadaje użytkownikowi uprawnienia do systemu,
6) jeżeli dane osobowe przetwarzane są poza systemem informatycznym (sieciowym), jednostanowiskowo, identyfikator i hasło dostępu do bazy danych ustala użytkownik,
7) wyrejestrowania użytkownika z systemu informatycznego (pozbawienia dostępu do systemu) dokonuje, na wniosek administratora bezpieczeństwa informacji lub przełożonego użytkownika, administrator systemu informatycznego.

6. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na wprowadzeniu do systemu przez jego administratora dla użytkownika unikatowego identyfikatora, hasła oraz ustanowienia zakresu dostępnych danych i operacji, przy czym o brzmieniu identyfikatora administrator systemu informuje administratora bezpieczeństwa informacji.

7. Za przydzielenie identyfikatora i wygenerowanie hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator systemu. Późniejsze cykliczne zmiany hasła muszą być wymuszane automatycznie poprzez mechanizmy zawarte w systemie informatycznym lub poprzez działanie administratora systemu.

8. Jeżeli dane osobowe przetwarzane są poza systemem informatycznym (sieciowym), za zmianę hasła odpowiada użytkownik.

9. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego (zamknięciu dostępu do systemu), nie może być przydzielany innej osobie. W przypadku wyrejestrowania użytkownika z systemu, administrator systemu pozostawia w systemie identyfikator i zmienia hasło dostępu.

10. Przełożeni użytkowników lub kierownicy jednostek organizacyjnych, o których mowa w ust. 4, zobowiązani są pisemnie informować administratora bezpieczeństwa informacji o każdej zmianie dotyczącej użytkowników, mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych osobowych i występowania każdorazowo z wnioskiem o nadanie nowego upoważnienia z uwzględnieniem nowych uprawnień oraz anulowania starego upoważnienia.

11. Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.”

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

prof. dr hab. Janusz Ostoja-Zagórski