



ZARZĄDZENIE nr 51/2016
REKTORA UNIWERSYTETU PAPIESKIEGO JANA PAWŁA II W KRAKOWIE
z dnia 14 listopada 2016 r.

w sprawie

ochrony danych osobowych
na Uniwersytecie Papieskim Jana Pawła II w Krakowie

Na podstawie art. 31 Statutu Uniwersytetu Papieskiego Jana Pawła II w Krakowie w zw. z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j.: Dz. U. z 2016 r. poz. 922 z późniejszymi zmianami) 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. Nr 100, poz. 1024) oraz pkt. I. 6 i instrukcji dotyczącej ochrony danych osobowych w działalności Kościoła katolickiego w Polsce z dnia 23 września 2009 r., opracowanej przez Generalnego Inspektora Ochrony Danych Osobowych oraz Sekretariat Konferencji Episkopatu Polski, zarządza się, co następuje:

§ 1

1. Ustala się zasady polityki bezpieczeństwa danych osobowych przetwarzanych w Uniwersytecie Papieskim Jana Pawła II w Krakowie.
2. Polityka Bezpieczeństwa UPJPII określa zasady postępowania przy przetwarzaniu danych osobowych, prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane, sposób zarządzania systemami informatycznymi oraz sposoby postępowania w przypadkach naruszania ochrony danych osobowych.
3. W celu realizacji wymagań formalnych i organizacyjnych dotyczących ochrony danych osobowych wprowadza się następujące dokumenty :

- a) zał. nr 1 zarządzenia nr 51/2016 - Polityka Bezpieczeństwa wraz z załącznikami:
Załącznik nr 1 Polityki Bezpieczeństwa – Upoważnienie dla ABI oraz zakres obowiązków
Załącznik nr 2 Polityki Bezpieczeństwa – Wykaz budynków
Załącznik nr 3 Polityki Bezpieczeństwa – Wykaz zbioru danych osobowych
Załącznik nr 4 Polityki Bezpieczeństwa – Opis struktury zbiorów danych osobowych
Załącznik nr 5 Polityki Bezpieczeństwa – Upoważnienie do przetwarzania danych osobowych

Załącznik nr 6 Polityki Bezpieczeństwa – Ewidencja osób przetwarzających dane osobowe
Załącznik nr 7 Polityki Bezpieczeństwa – Zestawienie danych osobowych
Załącznik nr 8 Polityki Bezpieczeństwa – Umowa powierzenia
Załącznik nr 9 Polityki Bezpieczeństwa – Oświadczenie osoby przetwarzającej dane osobowe
Załącznik nr 10 Polityki Bezpieczeństwa – Wniosek o nadanie/cofnięcie uprawnienia do przetwarzania danych osobowych
Załącznik nr 11 Polityki Bezpieczeństwa – Zgoda na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe
Załącznik nr 12 Polityki Bezpieczeństwa – Odwołanie zgody na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe
Załącznik nr 13 Polityki Bezpieczeństwa – Raport z naruszenia
b) załącznik nr 2 zarządzenia nr 51/2016 - Instrukcja zarządzania systemem informatycznym
c) załącznik nr 3 zarządzenia nr 51/2016 - Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń

4. Ilekroć z zarządzeniu jest mowa o:

1. **Ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922, z późn. zm.);
2. **Administratorze Danych Osobowych (ADO)** – oznacza to Uniwersytet Papieski Jana Pawła II w Krakowie, w imieniu Administratora Danych obowiązki określone w ustawie pełni Rektor Uczelni;
3. **Uczelni** - rozumie się przez to Uniwersytet Papieski Jana Pawła II w Krakowie;
4. **Administratorze Bezpieczeństwa Informacji (ABI)** – oznacza osobę powołaną przez Rektora, której zadaniem jest nadzorowanie i koordynowanie na Uczelni zasad postępowania przy przetwarzaniu danych osobowych;
5. **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące osoby fizycznej zidentyfikowanej bądź możliwej do zidentyfikowania;
6. **Administratorze Systemów Informatycznych (ASI)** – oznacza to osobę odpowiedzialną za sprawność, konserwację oraz wdrożenie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;
7. **Zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
8. **Przetwarzaniu danych** - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
9. **Systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

§ 2

Przepisy zawarte ww. dokumentach stosuje się do danych osobowych zawartych w zbiorach danych:

- a) tradycyjnych, w szczególności w kartotekach, teczках, księgach, skorowidzach, wykazach i innych zbiorach ewidencyjnych,
- b) znajdujących się w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych. Zbiory danych określa załącznik nr 3 Polityki Bezpieczeństwa.

§ 3

1. Administratorem danych osobowych w rozumieniu ustawy, zwanym dalej "ADO", jest Uniwersytet, natomiast w sensie praktycznym za realizację podstawowych obowiązków ADO odpowiedzialny jest Rektor.
2. Rektor wyznacza Administratora Bezpieczeństwa Informacji w osobie mgr inż. Aleksandry Ochałek oraz zastępcę Administratora Bezpieczeństwa Informacji w osobie mgr Katarzyny Młyńskiej.
3. Prorektorowi, odpowiedzialnemu za politykę kadrową Rektor zgodnie z §33 Statutu Uczelni deleguje nadzór nad ABI oraz jego zastępcą, którzy pozostają w bezpośredniej podległości służbowej w stosunku do ww. prorektora.
4. Wymienione w § 5 ust.2 Polityki Bezpieczeństwa zadania ABI oraz jego zastępcą wykonuje z pomocą Administratora Systemów Informatycznych (ASI).
5. Administratora Bezpieczeństwa Informacji zobowiązuje się do prowadzenia dokumentacji odzwierciedlającej wykonywanie zadań z zakresu ochrony danych osobowych i baz danych.

§ 4

1. Rektor zobowiązuje prorektorów, kanclerza, dziekanów, kierowników komórek organizacyjnych do spowodowania aby osoby w podległych im jednostkach organizacyjnych posiadały uprawnienia do przetwarzania danych osobowych. Uprawnienia nadaje ABI na pisemny wniosek ww. osób, zgodnie z *zał. nr 10 Polityki Bezpieczeństwa*.
2. Podmioty wskazane w § 4 ust. 1 równocześnie z zakończeniem współpracy z osobą przetwarzającą dane osobowe w poległych im jednostkach, powinny złożyć wniosek o cofnięcie uprawnień, zgodnie z *zał. 10 Polityki Bezpieczeństwa*.
3. Rektor może samodzielnie wykonywać wszystkie uprawnienia powierzone ABI.

§ 5

1. Podmioty przewidziane w § 4 ust. 1 są zobowiązane, w terminie do 31.12.2016 r., do wypełnienia wniosków o nadanie uprawnień zgodnie z *zał. 10 Polityki Bezpieczeństwa* dla pracowników Uniwersytetu zatrudnionych przy przetwarzaniu danych osobowych.
2. Każdy z pracowników, zatrudniony przy przetwarzaniu danych osobowych w dniu wejścia w życie niniejszego zarządzenia, jest zobowiązany w terminie do 12.12.2016 r.

złożyć swojemu przełożonemu wypełniony wniosek o nadanie uprawnienia do przetwarzania danych osobowych Uniwersytetu Papieskiego Jana Pawła II w Krakowie, do jego podpisu.

2. Pracownik z podpisanym oświadczeniem oraz zaakceptowanym przez przełożonego wnioskiem o nadanie uprawnień zgłasza się do ABI w celu uzyskania upoważnienia do przetwarzania danych.

3. ABI na podstawie wniosków oraz wydanych upoważnień sporządza ewidencję osób przetwarzających dane osobowe na UPJPII zgodnie z *zał. Nr 6 Polityki Bezpieczeństwa* oraz przekazuje do Działu Kadr, Płac i Spraw Socjalnych upoważnienia z wnioskami do akt osobowych pracowników.

4. Akta osobowe pracowników przetwarzających dane osobowe powinny zawierać:

a) wnioski o nadanie uprawnień pracownikom, którzy mają dostęp do danych osobowych, podpisane przez ich bezpośrednich przełożonych,

b) imienne upoważnienia do przetwarzania danych osobowych, wydane przez podmioty przewidziane w § 3 ust. 2, zgodnie z *zał. nr 5 Polityki Bezpieczeństwa*.

c) oświadczenia, z których wynika, że pracownicy zapoznali się z aktualnymi przepisami dotyczącymi ochrony danych osobowych, że zobowiązują się do zachowania w tajemnicy danych osobowych, zasad bezpieczeństwa tych danych stosowanych w czasie ich przetwarzania, nawet po ustaniu stosunku pracy w Uniwersytecie, oraz że są świadomi indywidualnej odpowiedzialności za nieprzestrzeganie przepisów o ochronie danych osobowych, *zał. nr 9 Polityki Bezpieczeństwa*.

§ 6

1. Podmioty przewidziane w § 4 ust. 1 są zobowiązane do:

1) wykonywania zaleceń ABI w zakresie ochrony danych osobowych i baz danych w systemach informatycznych funkcjonujących w podległych im jednostkach,

2) przekazywania, w przypadku zaistnienia jakichkolwiek zmian na bieżąco do ABI aktualnych danych w zakresie:

a) listy osób zatrudnionych przy przetwarzaniu danych w podlegających im komórkach organizacyjnych (nadanie lub cofnięcie uprawnień),

b) informacji ABI o stwierdzonych nieprawidłowościach przy przetwarzaniu danych osobowych, przy czym taka informacja winna zostać przekazana niezwłocznie,

3) tworzenia warunków organizacyjnych i wnioskowania o zapewnienie koniecznych warunków technicznych umożliwiających spełnienie wymogów wynikających z ustawy w podległych im jednostkach.

2. Pracownicy Uniwersytetu, którzy są zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani do:

a) wykonywania zaleceń ABI w zakresie ochrony danych osobowych i baz danych w systemach informatycznych, z których korzystają,

b) niezwłocznego informowania przełożonego oraz ABI o stwierdzonych nieprawidłowościach przy przetwarzaniu danych osobowych,

c) dbania o powierzone dane osobowe oraz przestrzegania zasad określonych w ustawie oraz w rozdziale *IV Polityki Bezpieczeństwa*.

§ 7

1. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby posiadające stosowne upoważnienie ADO lub podmiotów wymienionych w § 3 ust. 2 niniejszego zarządzenia. Upoważnienie do przetwarzania danych osobowych Uniwersytetu zostaje udzielone na wniosek podmiotów wskazanych w § 4 ust. 1 oraz po podpisaniu przez pracownika przetwarzającego dane osobowe oświadczenia zgodnie z *zał. nr 9 Polityki Bezpieczeństwa*.

2. Osoby nieprzestrzegające przepisów w zakresie ochrony danych osobowych podlegają sankcjom przewidzianym w rozdziale 8 ustawy oraz w rozdziale *V Polityki Bezpieczeństwa*.

§ 8

1. Uniwersytet, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych.

2. Udostępnianie danych osobowych osób, o których mowa w rozdziale *III Polityki Bezpieczeństwa*, odbywa się wyłącznie za pośrednictwem ADO. Dane osobowe udostępnia się na pisemny wniosek, zawierający informacje zgodne z § 16 *Polityki Bezpieczeństwa*.

3. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia ADO może mieć miejsce wyłącznie w przypadku działań podmiotów uprawnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.

§ 9

1. Uniwersytet gwarantuje osobom fizycznym, których dane osobowe są przetwarzane w związku z realizacją jego celów statutowych, realizację uprawnień wynikających z obowiązujących przepisów prawa.

2. Każdej osobie fizycznej, której dane osobowe są przetwarzane przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych na zasadach określonych w ustawie, zgodnie z § 19 i §20 *Polityki Bezpieczeństwa*.

§ 10

Uniwersytet, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, zapewnia zgodną z ustawą ochronę zbiorom danych osobowych sporządzanym doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku

z dydaktyką realizowaną na Uniwersytecie, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, chyba, że przepisy prawa stanowią inaczej.

§ 11

Zobowiązuje się ABI w terminie do 31.01.2017 r. do przekazania bezpośredniemu przełożonemu oraz Rektorowi raportu w sprawie realizacji zadań wynikających z niniejszego zarządzenia.

§ 12

Zarządzenie wchodzi w życie z dniem podpisania.

W dniu wejścia w życie niniejszego zarządzenia, traci moc Zarządzenie nr 19/2012 Rektora Uniwersytetu Papieskiego Jana Pawła II w Krakowie z dnia 11 lipca 2012 roku w sprawie ochrony danych osobowych na Uniwersytecie Papieskim Jana Pawła II w Krakowie.



ks. prof. dr hab. Wojciech Zyzak
REKTOR