



ZARZĄDZENIE

Nr 19/2018

**Rektora
Uniwersytetu Marii Curie-Skłodowskiej
w Lublinie**

z dnia 27 kwietnia 2018 r.

***w sprawie wdrożenia zasad prowadzenia analizy ryzyka i oceny skutków
przetwarzania danych na prawa i wolności podmiotu danych
w Uniwersytecie Marii Curie-Skłodowskiej w Lublinie***

Na podstawie art. 66 ust. 2 ustawy z dnia 27 lipca 2005 r. *Prawo o szkolnictwie wyższym* (t.j. Dz. U. z 2017 r. poz. 2183 z późn. zm.), w związku z art. 35 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* (tzw. Ogólne Rozporządzenie o Ochronie Danych Osobowych/RODO),

zarządzam:

§ 1

1. Mając na uwadze dbałość o ochronę praw i wolności osób, których dane przetwarza Uniwersytet jako administrator danych oraz prawidłowość realizacji obowiązków wynikających ze wskazanego powyżej art. 35 RODO, w celu maksymalizacji poziomu bezpieczeństwa danych osobowych wprowadza się obowiązek dokonania przed rozpoczęciem przetwarzania danych oceny skutków planowanych operacji przetwarzania dla ochrony danych.
2. Oceny skutków, o której mowa w ust. 1, dokonuje się jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
3. Do podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
4. Zgodnie z unormowaniami RODO ocena skutków wymagana jest w szczególności w przypadku:
 - 1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu (w systemie informatycznym), w tym profilowaniu, i jest podstawą decyzji wywołujących skutki

- prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
- 2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, tj. ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dotyczących danych genetycznych, biometrycznych, dotyczących stanu zdrowia, seksualności lub orientacji seksualnej osoby fizycznej lub wyroków skazujących i naruszeń prawa;
 - 3) systematycznego monitorowania na dużą skalę miejsc publicznie dostępnych.
5. Ocena skutków zawiera co najmniej:
 - 1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
 - 2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
 - 3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
 - 4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.
 6. Dokonując oceny skutków należy uwzględnić przestrzeganie obowiązujących u administratora przepisów prawa i aktów prawnych wewnętrznych.
 7. W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych, publicznych lub bezpieczeństwa operacji przetwarzania.
 8. Oceny skutków nie dokonuje się jeżeli przetwarzanie danych odbywa się w oparciu o przesłanki wskazane w RODO tzn. jest niezbędne do:
 - 1) wypełnienia obowiązku prawnego ciążącego na administratorze danych;
 - 2) wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi danych,i ma podstawę prawną w prawie Unii Europejskiej lub prawie krajowym i prawo takie reguluje daną operację przetwarzania danych lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej, chyba że w obowiązujących przepisach prawa zostanie wprowadzony obowiązek dokonania oceny skutków dla ochrony danych przed podjęciem przetwarzania danych.
 9. W razie potrzeby, a przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania danych, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków.
 10. W przypadku wdrażania/zakupu oprogramowania przetwarzającego dane osobowe dopuszcza się nałożenie obowiązku dokonania oceny skutków przetwarzania na ochronę danych osób fizycznych na podmiot dostarczający oprogramowanie.

§ 2

1. W celu zapewnienia rozliczalności w zakresie realizacji oceny skutków przetwarzania na ochronę danych wprowadza się obowiązek dokumentacji prowadzonych działań w postaci wzoru formularza oceny poziomu ryzyka naruszenia praw lub wolności osób i oceny skutków dla ochrony danych stanowiącego załącznik nr 1 do niniejszego zarządzenia będący

- dokumentem wewnętrznym nie podlegającym publikacji. Powyższy wzorzec nie ma zastosowania w przypadku zlecenia dokonania oceny skutków podmiotowi zewnętrznemu.
2. Za przeprowadzenie oceny skutków i dokumentację realizacji tego procesu odpowiedzialni są:
 - 1) kierownicy jednostek organizacyjnych nadzorujących merytorycznie obszar, w którym ma zostać wdrożona operacja przetwarzania danych – w przypadku zamiaru wdrożenia lub zmiany procesu przetwarzania danych (np. podjęcie nowych inicjatyw związanych z przetwarzaniem danych osobowych lub zakup/wdrożenie nowego oprogramowania) na szczeblu danej jednostki organizacyjnej;
 - 2) kierownicy jednostek organizacyjnych (w tym szczególnie administracji) nadzorujący określony obszar działania w Uniwersytecie – w przypadku zamiaru wdrożenia lub zmiany procesu przetwarzania danych w odniesieniu do operacji lub zestawu operacji przetwarzania danych, które mają być realizowane w obszarze całej Uczelni lub jej części.
 3. Osoba odpowiedzialna za dokonanie oceny skutków zobowiązana jest do zasięgnięcia konsultacji u Administratora Bezpieczeństwa Informacji (ABI)/po 25 maja 2018 r. Inspektora Ochrony Danych (IOD) na etapie dokonania oceny poziomu ryzyka przetwarzania danych oraz po dokonaniu oceny skutków przetwarzania dla ochrony danych.
 4. Konsultujący realizację procesu oceny skutków uprawniony jest do udzielania zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania zgodnie z wymogami art. 35 RODO oraz zasadami określonymi w niniejszym zarządzeniu.

§ 3

Zarządzenie wchodzi w życie w dniu podpisania.

R E K T O R

prof. dr hab. Stanisław Michałowski