ZARZĄDZENIE

Nr 23/2018

Rektora
Uniwersytetu Marii Curie-Skłodowskiej
w Lublinie

z dnia 27 kwietnia 2018 r.

w sprawie trybu postępowania w przypadku incydentów w zakresie bezpieczeństwa informacji i danych osobowych w Uniwersytecie Marii Curie-Skłodowskiej w Lublinie

Na podstawie art. 66 ust. 2 oraz art. 228 ust. 1 ustawy z dnia 27 lipca 2005 r. *Prawo o szkolnictwie wyższym* (t.j. Dz. U. z 2017 r. poz. 2183 z późn. zm),

zarządzam:

§ 1

1. Mając na uwadze prawidłowość realizacji obowiązków wynikających z art. 33 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/ dalej: RODO), tj. stosowania unormowań RODO w zakresie notyfikacji naruszeń ochrony danych osobowych oraz w celu maksymalizacji poziomu bezpieczeństwa danych administrowanych przez Uniwersytet Marii Curie-Skłodowskiej w Lublinie jako Administratora Danych Osobowych (dalej: Uniwersytet lub ADO) wprowadza się niniejszą procedurę postępowania w przypadku incydentów w zakresie bezpieczeństwa informacji i danych osobowych stanowiącą doprecyzowanie unormowań Regulaminu ochrony danych osobowych.
2. W ramach przedmiotowej procedury nakazuje niżej określony tryb postępowania:
    1) każda osoba, która przetwarza dane zobowiązana jest do bezzwłocznego informowania bezpośredniego przełożonego, a ten z kolei Inspektora Ochrony Danych (dalej: IOD) lub bezpośrednio IOD, o wszelkich incydentach

bezpieczeństwa noszących znamiona naruszenia ochrony danych osobowych w celu umożliwienia mu podjęcia czynności w ramach postępowania wyjaśniającego. W przypadku, gdy incydent dotyczy przetwarzania danych w systemie informatycznym konieczne jest dodatkowo poinformowanie o powyższym Administratora Systemu Informatycznego (dalej jako: ASI) w Dziale Lubman UMCS. Zgłoszenie incydentu odbywa się poprzez przekazanie informacji w postaci formularza zgłoszeniowego, którego wzór stanowi załącznik nr 1 do niniejszego zarządzenia,

2) IOD, a także ASI, do którego wpłynęło zgłoszenie w postaci formularza, o którym mowa w ust. 2 pkt 1), podejmuje działania sprawdzające mające na celu wyjaśnienie okoliczności zdarzenia oraz ustalenie, czy doszło do naruszenia ochrony danych osobowych. W toku prowadzonych czynności IOD, ASI lub inna osoba prowadząca postępowanie pod nadzorem IOD uprawniona jest do podejmowania wszelkich działań mogących służyć wyjaśnieniu sytuacji, w tym wstępu do wszelkich pomieszczeń i dostępu do wszelkich danych, systemów, raportów i innych dokumentów mogących mieć wpływ na wyjaśnienie okoliczności zdarzenia. Osoby uczestniczące w postępowaniu zobowiązane są do pełnej współpracy z prowadzącym postępowanie wyjaśniające.

   Z prowadzonych czynności sporządzana jest dokumentacja składająca się z formularza dokumentacji incydentu w zakresie bezpieczeństwa danych osobowych, którego wzór stanowi załącznik nr 2 do niniejszego zarządzenie oraz załączników do niego. Wytworzoną dokumentację IOD przedkłada ADO wraz z rekomendacją dalszego trybu postępowania, w szczególności wskazaniem, czy doszło do naruszenia ochrony danych osobowych i czy konieczne jest spełnienie obowiązków notyfikacji naruszeń do organu nadzorczego oraz osób, których dane dotyczą.;

3) w przypadku stwierdzenia w toku prowadzonych czynności wyjaśniających wystąpienia naruszenia ochrony danych osobowych podlegającego notyfikacji do organu nadzorczego, zgodnie z art. 33 RODO, po otrzymaniu stosowanej informacji od IOD, ADO - bez zbędnej zwłoki - w miarę możliwości nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że mało prawdopodobne jest, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

   Zgłoszenia ADO dokonuje z wykorzystaniem formularza zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego, którego wzór stanowi załącznik nr 3 do niniejszego zarządzenia.

Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin konieczne jest dołączenie wyjaśnienia przyczyn opóźnienia.

3. Jeżeli naruszenie ochrony danych osobowych stwierdzone zostanie przez IOD w trakcie prowadzonych przez niego czynności monitorujących stosowanie przepisów prawa w zakresie ochrony danych osobowych tryb podstępowania w zakresie dokumentacji, informowania ADO oraz notyfikacji naruszeń jest analogiczny jak opisany w ust. 2.
4. W przypadku konieczności zgłoszenia naruszenia organowi nadzorczemu, zgłoszenie – zgodnie ze wzorem, o którym mowa w ust. 2 pkt 3) musi co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) zawierać imię i nazwisko oraz dane kontaktowe IODO lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane przez administratora danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

W przypadku, gdy w momencie zgłoszenia naruszenia ochrony danych osobowych nie da się udzielić organowi nadzorczemu wszystkich informacji Administrator Danych, w tym zakresie, udziela je sukcesywnie bez zbędnej zwłoki.

5. Dokumentacja dotycząca naruszeń ochrony danych prowadzona przez ADO musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania zasad zgłaszania naruszeń wynikających z RODO.
6. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO – poza zgłoszeniem takiego naruszenia do organu nadzorczego – bez zbędnej zwłoki zawiadamia o naruszeniu osobę, której dane dotyczą.

   Zawiadomienie osoby, której dane dotyczą, jasnym i prostym językiem opisuje:
   1) charakter naruszenia;
   2) zawiera imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
7. Zawiadomienie osoby, której dane dotyczą, o którym mowa w ust. 6, nie jest wymagane jeżeli:
   1) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do danych;
   2) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   3) wymagałoby to niewspółmiernie dużego wysiłku – w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje środek, za pomocą osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.
8. Zawiadomienia o naruszeniu osoby, której dane dotyczą, może zażądać od ADO również organ nadzorczy w przypadku, gdy stwierdzi, że powyższe jest konieczne, a nie został spełniony żaden z warunków wskazanych w ust. 7.

§ 2

Za prawidłowość realizacji niniejszego zarządzenia i obowiązków związanych z notyfikacją naruszeń odpowiedzialni są kierownicy jednostek organizacyjnych, zaś za stosowanie zasad wynikających z unormowań zarządzenia odpowiedzialni są wszyscy pracownicy Uniwersytetu.

§ 3

Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.

R E K T O R

prof. dr hab. Stanisław Michałowski