Pismo okólne nr 1 /2011

z dnia 18 listopada 2011 r. Kanclerza Uniwersytetu Śląskiego w sprawie ochrony danych osobowych przetwarzanych w Administracji Ogólnouczelnianej.

Na podstawie rozdziału III pkt 2 ppkt 2c i pkt 4 „Polityki Bezpieczeństwa Informacji w Uniwersytecie Śląskim" stanowiącej załącznik nr 1 do zarządzenia Rektora UŚ nr 45 z dnia 22 lipca 2008 r. w sprawie wprowadzenia do użytku służbowego „Polityki Bezpieczeństwa Informacji w Uniwersytecie Śląskim" ustala się, co następuje:

§ 1

Do zakresu realizowanych przez Kanclerza obowiązków Lokalnego Administratora Danych Osobowych należy wyznaczenie „Pełnomocników Lokalnego Administratora Danych" oraz „Lokalnych Administratorów Bezpieczeństwa Informacji" dla jednostek Administracji Ogólnouczelnianej, w których przetwarza się dane osobowe.

§ 2

1. Wyznaczam w Administracji Ogólnouczelnianej osoby wskazane w ust. 2 na Pełnomocników Lokalnego Administratora Danych Osobowych, którzy bezpośrednio realizować będą obowiązki Administratora Danych w podległych im pionach i jednostkach administracji, określając tym samym obszar, w którym przetwarzane są dane.

2. Pełnomocnikami Lokalnego Administratora Danych Osobowych w Administracji Ogólnouczelnianej są:
   1) Zastępca Kanclerza ds. Zarządzania Logistycznego – dla obszaru określonego w załączniku pkt A,
   2) Zastępca Kanclerza ds. Technicznych – dla obszaru określonego w załączniku pkt B,
   3) Zastępca Kanclerza ds. Rozwoju i Współpracy z Gospodarką – dla obszaru określonego w załączniku pkt C,
   4) Kwestor – dla obszaru określonego w załączniku pkt D,
   5) Dyrektor Gabinetu Rektora – dla obszaru określonego w załączniku pkt E,
   6) kierownicy jednostek administracyjnych Administracji Ogólnouczelnianej podlegli bezpośrednio Rektorowi i Kanclerzowi – dla obszaru jednostki, którą kierują, wymienionych w załączniku pkt F.

3. Obowiązki Pełnomocników Lokalnego Administratora Danych Osobowych określone są w rozdziale III pkt. 4 „Polityki Bezpieczeństwa Informacji w Uniwersytecie Śląskim".

4. Zobowiązuję Pełnomocników wskazanych w ust. 2 do:
   1) uczestnictwa w szkoleniach w zakresie realizacji nałożonych na nich obowiązków; szkolenia przeprowadzane będą przez Pełnomocnika Danych, zgodnie z grafikiem zatwierdzonym na dany rok,
   2) prowadzenia szkoleń dla podległych pracowników, zgodnie z zasadami wynikającymi z rozdziału VI pkt 1 ppkt b „Polityki Bezpieczeństwa Informacji w Uniwersytecie Śląskim”,
   3) do prowadzenia ewidencji, o której mowa w rozdziale IV pkt 4 „Polityki Bezpieczeństwa Informacji w Uniwersytecie Śląskim”.

§ 3

1. Wyznaczam na Lokalnych Administratorów Bezpieczeństwa Informacji osoby, które bezpośrednio realizować będą obowiązki Administratora Bezpieczeństwa Informacji w jednostkach Administracji Ogólnouczelnianej:
   1) w zakresie danych osobowych przetwarzanych w systemach informatycznych administrowanych przez Dział Administracji Sieci i Usług Sieciowych – kierownika Działu Administracji Sieci i Usług Sieciowych,
   2) w zakresie danych osobowych przetwarzanych w systemach informatycznych administrowanych przez Dział Informatycznej Obsługi Toku Studiów – kierownika Działu Informatycznej Obsługi Toku Studiów,
   3) w zakresie danych osobowych przetwarzanych w systemach informatycznych administrowanych przez Dział Informatycznych Systemów Zarządzania – kierownika Działu Informatycznych Systemów Zarządzania,
   4) w zakresie danych osobowych przetwarzanych w systemach informatycznych administrowanych przez Dział Portalu i Serwisu WWW – kierownika Działu Portalu i Serwisu WWW,
   5) w zakresie danych osobowych przetwarzanych na stacjach roboczych w jednostkach administracji w Cieszynie, Chorzowie oraz Osiedlach Akademickich i Domach Asystenta – właściwi administratorzy lokalnych sieci komputerowych.

2. Do podstawowych zadań Lokalnego Administratora Bezpieczeństwa Informacji należy w szczególności:
   1) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
   2) dopilnowanie aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby mikrokomputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych,
   3) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
   4) opracowanie i zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które będą zawarte w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,

5) nadzór czynności związanych ze sprawdzeniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
6) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu oraz rejestracja kopii awaryjnych,
7) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
8) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
9) nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowanych przez system informatyczny,
10) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych,
11) dopilnowanie, aby jeżeli istnieją odpowiednie możliwości, ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie się wyłączały po upływie ustalonego czasu nieaktywności użytkownika,
12) podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych osobowych.

§ 4

Zobowiązuję Dyrektora ds. Informatyzacji do sporządzenia imiennego wykazu Lokalnych Administratorów Bezpieczeństwa Informacji, o których mowa w § 3 ust. 1 i przekazania go: Kanclerzowi, Administratorowi Bezpieczeństwa Informacji w Uniwersytecie Śląskim oraz Pełnomocnikom Lokalnych Administratorów Danych Osobowych według ich właściwości, w terminie 14 dni od ogłoszenia niniejszego zarządzenia.

§ 5

Traci moc Zarządzenie nr 1 z dnia 14 maja 2009 r. Kanclerza Uniwersytetu Śląskiego w sprawie ochrony danych osobowych przetwarzanych w Administracji Ogólnouczelnianej.

§ 6

Pismo okólne wchodzi w życie z dniem podpisania.

Kanclerz

Dr Agnieszka Skołucka