

OBOWIĄZKI I UPRAWNIENIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI W PAŃSTWOWEJ WYŻSZEJ SZKOLE TEATRALNEJ IM. L. SOLSKIEGO W KRAKOWIE

1. W Państwowej Wyższej Szkole Teatralnej im. L. Solskiego w Krakowie został powołany i zgłoszony do GIODO Administrator Bezpieczeństwa Informacji (dalej ABI), w osobie p. Iwony Kołodziejczyk, dane kontaktowe: tel. 12 422 81 96, w. 17, e-mail iwona.kolodziejczyk@pwst.krakow.pl
2. ABI podlega bezpośrednio rektorowi PWST.
3. ABI zapewnia przestrzeganie przepisów o ochronie danych osobowych w szczególności przez:
 - a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych;
 - b) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz przestrzegania zasad w niej określonych (podstawowym dokumentem jest Polityka Bezpieczeństwa zawierająca wykaz budynków, pomieszczeń lub ich części, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, charakterystykę struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i relacje między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami. W Polityce Bezpieczeństwa należy również zawrzeć charakterystykę środków technicznych i organizacyjnych właściwych dla zapewnienia poufności, integralności i rozliczności przetwarzanych danych),
 - c) zapewnianie zapoznania pracowników PWST z przepisami o ochronie danych osobowych.
4. ABI prowadzi i aktualizuje:
 - a) rejestr zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, których mowa w art. 43 ust. 1 ustawy o ochronie danych osobowych (np. zbiorów zawierających informacje niejawnne), zawierający nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 ustawy o ochronie danych osobowych,
 - b) ewidencję osób upoważnionych do przetwarzania danych osobowych, w celu umożliwienia rzetelnego nadzoru nad systemem określającym dostęp pracowników do poszczególnych zbiorów danych, w szczególności w systemie informatycznym.
5. ABI z upoważnienia rektora PWST nadaje i anuluje upoważnienia dla pracowników PWST do przetwarzania danych osobowych oraz dba o aktualność przyznanych upoważnień do przetwarzania danych osobowych w związku ze zmianami kadrowymi.
6. Każde upoważnienie powstaje w dwóch egzemplarzach: jeden dla osoby upoważnionej, drugi do dokumentacji ABI.
7. ABI zgłasza i aktualizuje zbiory danych osobowych do GIODO, jeżeli jest to wymagane.
8. ABI nadzoruje Administratora Systemu Informatycznego w zakresie:
 - a) przeglądu, konserwacji oraz uaktualnienia systemów służących do przetwarzania danych,
 - b) kontroli systemu komunikacji w sieci komputerowej,
 - c) uwierzytelniania personelu, w szczególności poprzez nadawanie zmian lub pozbawienie uprawnień dostępu do systemu użytkowników,
 - d) wykonywania polityki ochrony antywirusowej,
 - e) wykonywania kopii bezpieczeństwa.
9. ABI nadzoruje:
 - a) fizyczne zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe, w tym nadzoruje dostęp do tych pomieszczeń oraz kontrolę przebywających w nich osób,
 - b) szkolenia personelu z zakresu bezpieczeństwa przetwarzania danych osobowych;
 - c) bieżące procesy przetwarzania danych, w tym analizę sytuacji oraz przyczyn, które doprowadziły do naruszenia zasad bezpieczeństwa,
 - d) techniczne elementy systemu ochrony danych osobowych, takie jak m.in. administrowanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających zasady ich

- zmiany, zgodnie z ustalonymi wytycznymi, dopilnowywanie, aby komputery pracowników, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby nie były udostępniane osobom nieupoważnionym,
- e) obieg oraz przechowywanie dokumentów zawierających dane osobowe, tworzonych w systemie informatycznym.
10. ABI uczestniczy w czynnościach kontrolnych Generalnego Inspektora Ochrony Danych Osobowych.
 11. ABI prowadzi postępowania wyjaśniające w przypadku naruszenia ochrony danych osobowych przy współpracy z Administratorem Danych Osobowych.
 12. ABI sporządza dla rektora PWST sprawozdanie z czynności wykonanych co najmniej raz w roku w ramach sprawdzenia przestrzegania ochrony danych osobowych.
 13. ABI uprawniony jest do dostępu do wszystkich pomieszczeń, w których przetwarzane są dane osobowe, wglądu we wszystkie dokumenty zawierające dane osobowe oraz dostępu do wszystkich nośników, na których zapisane są dane osobowe przetwarzane w PWST.
 14. Wszyscy pracownicy PWST zobowiązani są współpracować z ABI i przestrzegać jego zaleceń w zakresie bezpieczeństwa przetwarzania danych osobowych.
 15. ABI uprawniony jest do wydawania i wdrażania instrukcji, procedur, zasad dotyczących bezpiecznego przetwarzania danych osobowych, a stanowiących uszczegółowienie Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.
 16. ABI uprawniony jest (w porozumieniu z rektorem i kanclerzem) do wyznaczania określonym pracownikom zadań dotyczących ochrony danych osobowych.
 17. ABI raz w roku dokonuje podsumowania funkcjonowania systemu ochrony danych osobowych w PWST. W tym celu realizowane jest sprawdzenie systemu ochrony danych osobowych (tj. czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych), wykonywane przez ABI lub osoby przez niego wskazane.
 18. ABI przygotowuje Plan sprawdzeń systemu ochrony danych osobowych w cyklu rocznym wskazując komórki organizacyjne, które podlegać będą sprawdzeniu. W Planie sprawdzeń określony jest przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń. W tym celu przygotowuje Plan Sprawdzeń podlega akceptacji ADO.
 19. Zakres sprawdzenia obejmuje weryfikację wymagań zawartych:
 - a) w ustawie o ochronie danych osobowych,
 - b) w dokumentacji systemu ochronnych danych osobowych.
 20. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez ADO lub ABI o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia (usuwających przyczyny zaistniałych nieprawidłowości). Ustalania zapisywane są w sprawozdaniu.
 21. Podczas kolejnego sprawdzenia sprawdzana jest skuteczność wykonanych działań.
 22. ADO może zarządzić sprawdzenie doraźne celem weryfikacji skuteczności wykonanych działań po stwierdzonych nieprawidłowościach.
 23. Pracownik odpowiedzialny za obszar danych osobowych, którego dotyczy sprawdzenie (dotyczy to również ASI) jest zobowiązany udostępnić wszystkie żądane dane, dokumenty, zapisy, udzielić wyczerpujących wyjaśnień oraz dokonywać okazania pomieszczeń, urządzeń na życzenie sprawdzającego oraz zapewnić pełną, merytoryczną współpracę.
 24. Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje Roczne sprawozdanie z funkcjonowania systemu ochrony danych osobowych.
 25. W przypadku wykrycia podczas weryfikacji nieprawidłowości ABI ustala ich przyczyny, zaleca wdrożenie działań korekcyjnych (usuwających nieprawidłowości) i korygujących.

Rektor PWST

prof. dr hab. Dorota Segda