Zarządzenie nr 15/2020
Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
z dnia 17 marca 2020 roku

1. Wprowadzam „*Wytyczne postępowania z danymi osobowymi na czas pracy zdalnej z uwagi na ogłoszenie stanu epidemiologicznego”,* stanowiące załącznik nr 1 do niniejszego zarządzenia.
2. Zarządzenie wchodzi w życie z dniem 17 marca 2020 roku.

REKTOR
/- / Prof. dr hab. Wojciech Malajkat

Załącznik nr 1 do Zarządzenia Rektora nr 15/2020 z dnia 17 marca 2020 roku

Wytyczne postępowania z danymi osobowymi na czas pracy zdalnej

Kierownicy jednostek podejmują decyzje, które zadania są niezbędne w celu zachowania ciągłości działania jednostki i decydują o możliwości przetwarzania danych osobowych poza siedzibą jednostki.

Wszelkie wynoszone dokumenty i nośniki danych, a także sprzęt wykorzystywany poza obszarem przetwarzania danych osobowych, muszą być odpowiednio zabezpieczone w sposób zapewniający:

- Zabezpieczenie przed kradzieżą, utratą lub zniszczeniem – zasada dostępności danych;
- Uniemożliwienie zmiany treści danych/zawartości dokumentów lub nośników przez osobę nieupoważnioną – zasada integralności danych;
- Zabezpieczenie treści danych/zawartości dokumentów lub nośników przed osobami nieuprawnionymi – zasada poufności.

W szczególności:

Dokumenty.

- Dokumenty w formie papierowej powinny być umieszczane w koszulkach lub foliach, a następnie twardych i zamykanych teczkach aktowych, zabezpieczających przed uszkodzeniami fizycznymi;
- Dokumenty w formie papierowej powinny być podczas transportu pod opieką osoby, której zostały wydane. Nie mogą być pozostawiane bez opieki także w zamkniętym samochodzie;
- Dokumenty w formie papierowej powinny być przetrzymywane w miejscu wykonywania pracy poza siedzibą jednostki w sposób bezpieczny i uniemożliwiający wgląd do nich także członkom rodziny.

Urządzenia i nośniki elektroniczne (m.in. pendrive, CD-ROM).

- Nośniki powinny być podczas transportu pod opieką osoby, której zostały wydane. Nie mogą być pozostawiane bez opieki także w zamkniętym samochodzie;
- Nośniki powinny być przetrzymywane w miejscu wykonywania pracy poza siedzibą jednostki w sposób bezpieczny i uniemożliwiający wgląd do nich także członkom rodziny;
- Nośniki w miarę możliwości powinny być szyfrowane.

Prywatne komputery i urządzenia.

- W przypadku korzystania z komputerów prywatnych należy ograniczyć zapisywanie plików, wiadomości e-mail na prywatnych dyskach i komputerach;
- Zabezpieczenia na prywatnych komputerach i urządzeniach powinny w miarę możliwości obejmować antywirusy oraz firewalle;
- Hasła nie powinny być przechowywane/zapisywane, a jedynie wpisywane w celu logowania do sytemu.

Transport (przenoszenie, przewożenie).

1. Dokumenty papierowe, nośniki elektroniczne, urządzenia przenośne mogą być transportowane wyłącznie w zamkniętej torbie/plecaku/walizce/skrzyni uniemożliwiających łatwe poznanie ich zawartości. Niedozwolone jest ich przenoszenie w zewnętrznych kieszeniach ubrań, reklamówkach, worka foliowych lub torbach nieposiadających zamknięcia, a także w inny sposób mogący skutkować uszkodzeniem, zniszczeniem, zalaniem (np. ze względu na warunki atmosferyczne). Torba/plecak/walizka/skrzynia musi przez cały czas znajdować się pod bezpośrednią kontrolą użytkownika i w zasięgu jego wzroku;
2. W przypadku transportowania dużej ilości dokumentów w formie papierowej i/lub kilku elektronicznych urządzeń przenośnych (tj. takiej ich ilości, która nie zmieści się w jednej torbie/plecaku/walizce/skrzyni), powinno odbywać się to w asyście innej osoby (osób) upoważnionych (upoważnionej), przy użyciu stosownej liczby toreb/plecaków/walizek/skrzyń zapewniających odpowiednie zabezpieczenie dokumentów i elektronicznych urządzeń przenośnych;

3. Zaleca się przewożenie znacznej ilości dokumentów papierowych lub elektronicznych urządzeń przenośnych przy pomocy pracowników korzystających ze zgodą pracodawcy z samochodów prywatnych do celów służbowych;
4. W przypadku korzystania ze środków komunikacji publicznej/taksówek, należy zachować szczególną ostrożność;
5. Niedopuszczalne jest przekazywanie torby / plecaka / walizki / skrzyni, zawierającej dokumenty lub elektroniczne urządzenia przenośne w bezpośrednie władanie osób postronnych ani informowanie tych osób o ich zawartości;
6. Niedopuszczalne jest pozostawienie torby / plecaka / walizki / skrzyni bez nadzoru, np. w szatni, depozycie, samochodzie.

Przechowywanie.

1. Dokumenty i elektroniczne urządzenia przenośne, które zostały wyniesione poza obszar przetwarzania, muszą być przechowywane w miejscu odpowiednio zabezpieczonym przed dostępem osób nieupoważnionych lub osób trzecich, a także uszkodzeniami fizycznymi;
2. Niedopuszczalne jest pozostawienie dokumentów i elektronicznych urządzeń przenośnych bez nadzoru w prywatnych mieszkaniach osób trzecich, recepcjach, oddawanie w depozyt, itp.;
3. Niedopuszczalne jest przechowywanie środków dostępu do dokumentów i/lub elektronicznych urządzeń przenośnych (np. kluczy do toreb, haseł dostępu do komputera, PIN-u do telefonu) bezpośrednio przy dokumentach i/lub sprzęcie.

Korzystanie.

1. Dokumenty papierowe, nośniki i urządzenia elektroniczne powinny być przygotowane do pracy (wyjmowane z teczek, uruchamiane) wyłącznie na czas pracy i niezwłocznie chowane, wyłączane (wygaszane, szyfrowane) po zakończeniu pracy;
2. Po ustaniu konieczności przetwarzania danych osobowych, należy je niezwłocznie trwale zniszczyć lub usunąć z elektronicznego urządzenia przenośnego lub stacjonarnego nie będącego własnością administratora;
3. W przypadku korzystania z prywatnych elektronicznych urządzeń przenośnych i stacjonarnych, będących własnością użytkownika, przez osoby inne niż użytkownik, należy założyć osobne, zahasłowane profile na tych urządzeniach, ograniczające nieupoważnionym osobą – w tym członkom rodziny – dostęp do zasobów służbowych przechowywanych na tych urządzeniach. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec domowników i osób bliskich, identyfikator oraz hasło do profilu, o którym mowa w zdaniu poprzedzającym i ponosi za to odpowiedzialność;
4. Niedopuszczalne jest współdzielenie służbowego elektronicznego urządzenia przenośnego z osobami nieuprawnionymi, a także zapoznawanie ich z treścią dokumentacji;
5. Niedopuszczalne jest korzystanie na służbowym elektronicznym urządzeniu przenośnym z niezabezpieczonych, publicznych sieci Wi-Fi. Nie zaleca się korzystania z takich sieci na prywatnym elektronicznym urządzeniu przenośnym;
6. Niedopuszczalne jest samodzielne instalowanie na służbowym elektronicznym urządzeniu przenośnym jakichkolwiek programów czy aplikacji ani łączenie ich z innymi niezależnymi i niezabezpieczonymi urządzeniami elektronicznymi;
7. Niedopuszczalne jest korzystanie z dokumentacji i elektronicznych urządzeń przenośnych w bezpośredniej obecności osób nieuprawnionych, w sposób naruszający zasady określone powyżej lub stwarzających ryzyko takiego naruszenia. Szczególną ostrożność należy z zachować w środkach komunikacji publicznej.

Incydenty.

W przypadku utraty / zniszczenia / zagubienia dokumentów lub elektronicznych urządzeń przenośnych lub wystąpienia innych okoliczności stwarzających ryzyko naruszenia ochrony danych osobowych, w związku z przetwarzaniem danych osobowych poza obszarem przetwarzania, należy zawiadomić o tym fakcie kierownictwo jednostki oraz inspektora ochrony danych.

Wykaz osób, które zapoznały się z dokumentem i którym umożliwiono przetwarzanie danych osobowych poza siedzibą jednostki.

Imię i nazwisko	Podpis*

*oświadczam, iż zapoznałem/am się z dokumentem „Wytyczne postępowania z danymi osobowymi na czas pracy zdalnej z uwagi na ogłoszenie stanu epidemiologicznego.” i zobowiązuję się do dołożenia należytej staranności i zabezpieczenia przetwarzanych danych osobowych przed nieuprawnionym dostępem, kradzieżą, utratą lub zniszczeniem.

Wykaz dokumentów papierowych/nośników z danymi osobowymi wynoszonymi poza obszar przetwarzania danych.

Typ dokumentacji	Komórka organizacyjna	Podpis kierownika	Podpis osoby otrzymującej