Załącznik nr 2
Do Zarządzenia nr 38/2023 Rektora ASP w Krakowie
z dnia 16.06.2023

Informacja określająca procedury ochrony danych osobowych podczas wykonywania pracy w trybie zdalnym obowiązująca w Akademii Sztuk Pięknych im. Jana Matejki w Krakowie

§1
Podstawy prawne

1. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy.
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej RODO).

§2
Postanowienia ogólne

1. Pracownik wykonujący pracę zdalną otrzymuje od pracodawcy narzędzia (w tym urządzenia) i materiały służbowe niezbędne do wykonywania pracy po uprzednim sporządzeniu stosownego protokołu zdawczo – odbiorczego zawierającego zgodę na wyniesienie ich poza obiekty, w których pracodawca prowadzi działalność statutową, chyba że posiada uprzednią zgodę Rektora lub Kanclerza udzieloną zgodnie z Regulaminem pracy na okres obejmujący czas pracy zdalnej.
2. Pracodawca dopuszcza użycie urządzeń prywatnych pracownika wyjątkowo pod warunkiem poszanowania i ochrony informacji poufnych i innych tajemnic prawnie chronionych oraz danych osobowych, a także informacji, których ujawnienie mogłoby narazić Pracodawcę na szkodę. Zgodę na używanie urządzeń prywatnych do celów służbowych wydaje zgodnie z Regulaminem pracy Rektor lub Kanclerz.
3. Pracodawca ma prawo przeprowadzać kontrolę wykonywania pracy w zakresie przestrzegania wymogów procedury ochrony danych osobowych. Zasady kontroli określa § 7 Zarządzenia.
4. Jeżeli pracodawca w trakcie kontroli pracy zdalnej stwierdzi uchybienia w przestrzeganiu wymogów w zakresie procedur ochrony danych osobowych, zobowiązuje pracownika do usunięcia stwierdzonych uchybień we wskazanym terminie albo cofa zgodę na wykonywanie pracy zdalnej przez tego pracownika. W przypadku wycofania zgody na wykonywanie pracy zdalnej pracownik rozpoczyna pracę w zwykłym miejscu pracy w terminie określonym przez pracodawcę.

§3
Zasady ochrony danych osobowych podczas pracy zdalnej na urządzeniach prywatnych

Praca na urządzeniu prywatnym musi odbywać się z uwzględnieniem następujących zasad bezpieczeństwa:

- Konieczność utworzenia odrębnego konta użytkownika do pracy służbowej,

- Ustawienie hasła do powyższego konta użytkownika, składającego się z min. 8 znaków, w tym małych i wielkich liter, znaków specjalnych lub cyfr,
- Konieczność korzystania tylko z zabezpieczonych i sprawdzonych sieci,
- Logowanie się do systemów służbowych za pomocą VPN,

- Zakaz pozostawiania urządzeń mobilnych bez nadzoru w trakcie pracy, bez uprzedniego wylogowania się,
- Ustawienie wygaszacza ekranu, włączającego się po 3 minutach bezczynności,
- Posiadanie aktualnego programu antywirusowego,
- Korzystanie z legalnego i aktualnego oprogramowania,
- Konieczność korzystania z poczty służbowej na sprzęcie prywatnym, w ramach wykonywania pracy zdalnej,
- Konieczność usunięcia z urządzenia po zakończeniu pracy zdalnej danych osobowych, z którymi pracowano, w sposób uniemożliwiający ich odzyskanie.

§4
Forma komunikacji z pracodawcą, pracownikami, kontrahentami

1. Wskazanymi sposobami komunikacji podczas wykonywania pracy zdalnej są:
   a) aplikacja TEAMS, która jest narzędziem platformy Office 365,
   b) służbowa poczta e-mail,
   c) rozmowa telefoniczna.

§5
Stosowane zabezpieczenia organizacyjne

1. Zdalny dostęp do danych osobowych wymaga uwierzytelnienia loginem i hasłem, wydanym przez Administratora lub osobę wskazaną.
2. Dane osobowe oraz ich transfer zabezpiecza się kryptograficznie, minimum poprzez zaszyfrowanie pliku zawierającego dane osobowe oraz udostępnienie klucza dostępu inną drogą.
3. Nie dopuszcza się pozostawiania loginów oraz haseł w miejscach pracy urządzeń mobilnych, tak aby były dostępne dla osób nieupoważnionych.
4. Nie dopuszcza się pozostawiania urządzeń mobilnych bez uprzedniego wylogowania z systemu.
5. Ekrany laptopów należy zabezpieczyć przed niepożądanym wglądem osób postronnych np. poprzez zastosowanie folii prywatyzującej.
6. Urządzenia mobilne należy zabezpieczać przed kradzieżą, stosując np. linki zabezpieczające do laptopów.
7. Na wypadek zniszczenia urządzeń mobilnych dane należy zapisywać w aplikacji OneDrive lub Sharepoint, które są narzędziami platformy Office 365 lub w innym miejscu wskazanym przez Administratora lub przełożonego.

8. Zabrania się zapisywania danych osobowych bez zastosowania hasła na dysku/pamięci urządzenia mobilnego.
9. Podczas pracy zdalnej zabrania się wykorzystywania pendrive, dysków zewnętrznych lub tego typu urządzeń.
10. Praca zdalna jest zabroniona w miejscach publicznych.
11. W pracy zdalnej zabrania się korzystania z niezabezpieczonych lub otwartych sieci Wi-Fi.
12. Zabrania się zapisywania loginów i haseł do programów, w których przetwarzane są dane osobowe w przeglądarkach internetowych.
13. Zabrania się wynoszenia poza obiekty należące do Akademii Sztuk Pięknych im. Jana Matejki w Krakowie papierowej wersji dokumentów. W przypadku konieczności wykonywania pracy zdalnej z dostępem do dokumentów pracownik zgłasza przełożonemu wniosek o dostęp do elektronicznej wersji dokumentu, a po jego uzyskaniu skanuje dokument i przechowuje go zgodnie z obowiązującymi u Pracodawcy zasadami bezpieczeństwa. W szczególnie uzasadnionych przypadkach, gdy wykonywanie pracy zdalnej z dostępem do papierowej wersji dokumentów jest konieczne, pracownik zgłasza przełożonemu wniosek o udostępnienie dokumentów do miejsca świadczenia pracy zdalnej, a po uzyskaniu zgody Rektora lub Kanclerza i zaewidencjonowaniu udostępnionych dokumentów zobowiązany jest do ochrony danych objętych ich treścią poprzez:
    a) ograniczenie liczbę wynoszonych dokumentów do niezbędnie potrzebnych;
    b) zabezpieczenie transportowanych dokumentów w taki sposób, aby były niewidoczne dla osób trzecich;
    c) przechowywanie dokumentów przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej;
    d) zabezpieczenie danych w miejscu wykonywania pracy zdalnej (np. przechowywanie dokumentów w zamykanych na klucz szufladach, biurkach lub szafach, przestrzeganie zasady czystego biurka, zabezpieczanie dokumentów przed wglądem nieuprawnionych osób trzecich, m.in. członków rodziny);
    e) wykorzystywanie pozyskanych danych osobowych objętych treścią dokumentów wyłącznie w tym celu, w jakim byłyby wykorzystywane w obiektach Pracodawcy;
    f) zwrócenie udostępnionych dokumentów do siedziby Pracodawcy;

§6
Naruszenia bezpieczeństwa danych osobowych

W przypadku jakichkolwiek awarii bądź incydentów bezpieczeństwa danych osobowych, pracownik zobligowany jest do niezwłocznego powiadomienia Przełożonego, Działu Informatycznego (it@asp.krakow.pl) oraz Inspektora Ochrony Danych (e-mail: iod@asp.krakow.pl).

§7
Zapewnienie poufności

Pracownicy zobowiązani są do wykorzystywania danych osobowych jedynie w celach służbowych, a także do zapewnienia należytej poufności przetwarzanych danych, w trakcie i po ustaniu pracy zdalnej.

_