Załącznik nr 1 do Zarządzenia nr R021.1.49.2023
Rektora UJD w Częstochowie z dnia 24.04.2023
w sprawie wprowadzenia Procedur ochrony danych osobowych
na potrzeby wykonywania pracy zdalnej
w Uniwersytecie Humanistyczno-Przyrodniczym
im. Jana Długosza w Częstochowie

Procedury ochrony danych osobowych na potrzeby wykonywania pracy zdalnej w Uniwersytecie Humanistyczno-Przyrodniczym im. Jana Długosza w Częstochowie

I. Zakres podmiotowy Procedury

1. Procedura określa zasady postępowania z danymi osobowymi w przypadku ich przetwarzania podczas pracy poza siedzibą Uczelni.
2. Zakresem procedury objęci są pracownicy wykonujący pracę zdalną na podstawie:
   a) art. 67^{19} § 1 Kodeksu pracy (praca zdalna uzgodniona między pracownikiem a pracodawcą),
   b) art. 67^{19} § 3 Kodeksu pracy (obligatoryjna praca zdalna wykonywana na polecenie pracodawcy),
   c) art. 67^{19} § 6 Kodeksu pracy (obligatoryjna praca zdalna na wniosek pracownika).

II. Podstawowe pojęcia

1. „Administrator" – Uniwersytet Humanistyczno-Przyrodniczy im. Jana Długosza w Częstochowie, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
2. „dane osobowe" – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, np. imię i nazwisko, numer PESEL, adres zamieszkania, adres e-mail, itp.,
3. „naruszenie ochrony danych osobowych" – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
4. „pracownik wykonujący pracę zdalną" – osoba zatrudniona na podstawie przepisów Kodeksu pracy, w jeden ze sposobów określonych w art. 67^{19} § 1 Kodeksu pracy.

III. Obowiązki ogólne

Pracownik wykonujący pracę zdalną jest zobowiązany do:

1. przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych oraz wewnętrznymi aktami obowiązującymi w Uczelni, zwłaszcza z Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym,

2. odbywania szkoleń z zakresu ochrony danych osobowych, na które kieruje go Administrator,
3. przetwarzania udostępnionych mu danych osobowych jedynie w celach służbowych, określonych w umowie o pracę,
4. przekazania Administratorowi pisemnej informacji o wystąpieniu incydentu/ podejrzeniu wystąpienia incydentu niezwłocznie, najpóźniej w przeciągu 24 godzin od zaistnienia zdarzenia.

IV. Bezpieczeństwo obszaru przetwarzania

Pracownik wykonujący pracę zdalną jest zobowiązany do:

1. właściwego zabezpieczenia danych osobowych przetwarzanych przez niego w ramach pracy zdalnej,
2. zachowania poufności informacji, w szczególności podczas służbowych rozmów telefonicznych lub wideokonferencji,
3. zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją,
4. założenia odrębnych kont użytkowników chronionych silnym hasłem w przypadku korzystania z komputera prywatnego przez wiele osób, na przykład domowników,
5. uniemożliwienia wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu, stosowanie filtrów prywatyzujących na ekran,
6. blokowania sprzętu komputerowego w przypadku oddalenia się od miejsca pracy.
7. wylogowania się z programów wykorzystywanych do pracy zdalnej i z systemu każdorazowo po zakończeniu pracy na sprzęcie elektronicznym,
8. bezpiecznego przechowywania danych osobowych zawartych w dokumentacji w formie papierowej, na przykład w szafkach zamykanych na klucz.

V. Bezpieczeństwo przechowywania danych osobowych

1. Pracownik wykonujący pracę zdalną jest zobowiązany do szyfrowania sprzętu komputerowego i innych mobilnych nośników danych (np. pendrive, dysk zewnętrzny) wykorzystywanych w celach służbowych zawierających dane osobowe, w tym laptop, telefon lub tablet.
2. Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci.
3. Nie jest dopuszczalne umożliwianie dostępu do danych, poczty elektronicznej lub systemów informatycznych osobom nieuprawnionym, podającym się, np.

telefonicznie czy mailowo, za przedstawicieli serwisu lub konkretnych instytucji, bez ich weryfikacji i potwierdzenia u Administratora.

4. Nie jest dopuszczalne samodzielne lub z wykorzystaniem wsparcia podmiotów zewnętrznych naprawianie sprzętu służbowego wykorzystywanego do pracy zdalnej. W celu naprawy uszkodzonego sprzętu służbowego należy bezzwłocznie zwrócić go do Działu Infrastruktury Informatycznej Uczelni lub informatyka wydziałowego.
5. W przypadku uszkodzenia prywatnego sprzętu komputerowego, na którym przetwarzane były służbowe dane osobowe, pracownik wykonujący pracę zdalną ma obowiązek, przed skorzystaniem z usług zewnętrznego serwisanta, skontaktować się z Działem Infrastruktury Informatycznej Uczelni lub informatykiem wydziałowym.
6. Po zakończeniu pracy zdalnej pracownik jest zobowiązany bezzwłocznie przekazać do Administratora wszystkie dane związane z wykonywanymi zadaniami służbowymi zapisane na prywatnym sprzęcie (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje), a następnie usunąć je w sposób trwały.
7. Należy ograniczyć do niezbędnego minimum drukowanie dokumentacji zawierającej dane osobowe, a jeżeli taka konieczność zaistnieje, należy skutecznie niszczyć wydruki po zakończeniu pracy z nimi. Jeżeli nie ma możliwości takiego zniszczenia w warunkach domowych, to należy zniszczyć je w niszczarkach na Uczelni.
8. Nie jest dopuszczalne drukowanie dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów czy osób trzecich.
9. Pracownik zobowiązany jest przechowywać udostępnione przez Administratora dokumenty papierowe tylko przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (zasada ograniczenia przetwarzania). Po tym czasie zobowiązany jest niezwłocznie zwrócić je do Administratora.
10. Bezpośredni przełożony jest zobowiązany do ewidencjonowania powierzonej pracownikowi dokumentacji zawierającej dane osobowe. Preferowana jest praca na kopiach dokumentów. Pracownik musi chronić dane osobowe zawarte w kopiach dokumentów, tak samo jak w dokumentacji oryginalnej.

VI. Bezpieczeństwo domowej sieci

1. Sprzęt komputerowy wykorzystywany do pracy zdalnej należy podłączyć do zabezpieczonej, domowej sieci WiFi. Zabronione jest korzystanie z otwartych sieci WiFi (na przykład WiFi hotelowe, w galeriach handlowych, hot-spot w kawiarniach).
2. Dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) należy zabezpieczyć silnym hasłem, którym nie jest hasło domyślne, zdefiniowane podczas pierwszej konfiguracji urządzenia.

3. Sprzęt komputerowy wykorzystywany do pracy zdalnej musi być wyposażony w uruchomione i regularnie aktualizowane oprogramowanie antywirusowe. Właściciel sprzętu odpowiada za legalność oprogramowania.
4. Należy wyłączyć lub ograniczyć tylko do zdefiniowanych adresów IP możliwość konfiguracji sprzętu sieciowego z urządzeniami znajdującymi się poza siecią LAN.
5. W przypadku jakichkolwiek wątpliwości dotyczących posiadanych zabezpieczeń należy skonsultować się z Działem Infrastruktury Informatycznej Uczelni lub informatykiem wydziałowym.

VII. Obowiązki pracowników korzystających z poczty elektronicznej i systemów informatycznych

Pracownik wykonujący pracę zdalną, korzystający z poczty elektronicznej i systemów informatycznych jest zobowiązany do:

1. przechowywania loginów i haseł w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych, w tym domowników.
   Zabronione jest domyślne zapamiętywanie hasła dostępu do konta użytkownika systemu na sprzęcie wykorzystywanym w pracy zdalnej,
2. stosowania Polityki haseł Administratora, wskazanej w Instrukcji zarządzania systemem informatycznym UJD,
3. korzystania z poczty elektronicznej wyłącznie w celach służbowych, niepobierania danych osobowych z systemów informatycznych w celu innym niż służbowy,
4. pobierania i zapisywania tylko niezbędnych dokumentów,
5. przesyłania danych osobowych mailowo jedynie wtedy, gdy jest to absolutnie niezbędne,
6. szyfrowania danych osobowych udostępnianych w przesyłanych wiadomościach, przesyłania hasła innym kanałem komunikacji,
7. korzystania z opcji „UDW" podczas wysyłania korespondencji zbiorczej poza Uczelnię, dzięki czemu odbiorcy wiadomości nie zobaczą wzajemnie swoich adresów e-mail,
8. weryfikowania nadawców wiadomości e-mail. W przypadku wątpliwości co do tożsamości nadawcy zabronione jest otwieranie załączników do wiadomości e-mail oraz hiperłączy znajdujących się w treści,
9. nieprzesyłania korespondencji służbowej na prywatną skrzynką pocztową,
10. niewłączania opcji autouzupełniania formularzy w opcjach przeglądarki internetowej,
11. w przypadku korzystania z przeglądarki internetowej sprawdzenia informacji o jej zabezpieczeniach.

VIII. Obowiązki podczas spotkań zdalnych, wideokonferencji

1. Organizacja spotkań może nastąpić tylko przy użyciu dopuszczonych przez Administratora rozwiązań informatycznych. Dopuszczalne są jedynie programy/ platformy należące do Administratora, ewentualnie zewnętrzne, z dostawcami których Administrator zawarł umowę powierzenia przetwarzania danych osobowych.
2. Przy podłączaniu się do programu z funkcją telekonferencji zalecane jest korzystanie z kodów dostępu/ PIN-ów.
3. Przed rozpoczęciem korzystania z programów z funkcją telekonferencji zalecane jest przeskanowanie ich systemem antywirusowym lub antymalware'owym.
4. Podczas spotkań przebiegających z ujawnianiem wizerunków należy ograniczyć do minimum ich rejestrowanie, zaleca się wyłączenie opcji nagrywania i przechowywania.
5. Zaleca się korzystanie z opcji „poczekalnia" tak, aby kontrolować uczestników telekonferencji, w celu uniknięcia przypadkowych lub niechcianych osób.
6. W trakcie korzystania z programów/ platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych (zasada minimalizacji danych).
7. W przypadku konieczności udostępniania konkretnych dokumentów podczas spotkań należy zamknąć używane wcześniej inne dokumenty, aplikacje, okna przeglądarek, aby udostępnić uczestnikom spotkania tylko i wyłącznie dedykowany dla nich plik.
8. Wszystkie pliki zapisywane w dedykowanej do tego przestrzeni w aplikacji do wideokonferencji należy cyklicznie przeglądać i usuwać po ustaniu ich przydatności.
9. Linki do wideokonferencji powinny być udostępniane tylko i wyłącznie uczestnikom spotkania, bezpiecznym kanałem komunikacji, zaproszenia powinny być kierowane wyłącznie na służbowe adresy e-mail.
10. Zabrania się udostępniania dokumentów służbowych, za pomocą publicznego czatu lub innych komunikatorów.