Załącznik nr 6
do Zasad pracy zdalnej w Uniwersytecie Komisji Edukacji Narodowej w Krakowie

Procedura ochrony danych osobowych w ramach pracy zdalnej

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 art. 67^{18} i nast. Kodeksu pracy.

II. Podstawowe pojęcia

1. Dane osobowe – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
2. Naruszenie ochrony danych osobowych – oznacza 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.
3. Pracownik wykonujący pracę zdalną – osoba zatrudniona w ramach stosunku pracy, wykonująca pracę w jeden ze sposobów określonych w art. 67^{19} oraz art. 67^{33} Kodeksu pracy (w rozumieniu procedury nie jest pracownikiem wykonującym pracę zdalną osoba zatrudniona na podstawie umowy cywilnoprawnej).

III. Obowiązki ogólne

1. Każdy pracownik wykonujący pracę zdalną jest zobowiązany do stosowania obowiązujących u pracodawcy wewnętrznych aktów dotyczących ochrony informacji oraz danych osobowych, a także procedur lub instrukcji dotyczących działania systemów informatycznych obowiązujących u pracodawcy.
2. Każdy pracownik ma obowiązek uczestniczenia w szkoleniach z zakresu ochrony danych osobowych, na które kieruje go pracodawca.
3. Każdy pracownik ma obowiązek zgłaszania wszelkich podejrzeń naruszenia ochrony danych osobowych. Każdy incydent należy zgłosić bezpośredniemu przełożonemu oraz na adres iod@up.krakow.pl
4. Pracownik nie jest uprawniony do wynoszenia poza teren pracodawcy papierowej wersji dokumentów zawierających dane osobowe oraz inne dane będące w zasobach pracodawcy.

5. Pracownik przetwarza dokumenty znajdujące się w systemie informatycznym pracodawcy po wcześniejszym zalogowaniu zgodnie z zasadami bezpieczeństwa jakie obowiązują w Uczelni podczas pracy stacjonarnej.
6. W szczególnie uzasadnionych przypadkach, gdy wykonywanie pracy zdalnej z dostępem do papierowej wersji jest konieczne, pracownik składa do przełożonego wniosek o udostępnienie kopi dokumentów do miejsca pracy zdalnej, a po jego uzyskaniu i zaewidencjonowaniu udostępnionych kopi dokumentów zobowiązany jest do ich ochrony oraz ochrony danych w nich się znajdujących w następujący sposób:
   a) ograniczenie do niezbędnego minimum liczby wynoszonych kopii dokumentów,
   b) zabezpieczenie transportowanych dokumentów w taki sposób, aby zawarte w nich dane nie były dostępne dla osób trzecich,
   c) przechowywanie zabezpieczonych kopii dokumentów przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej,
   d) zabezpieczenie dokumentów w miejscu wykonywanej pracy zdalnej (np. przechowywanie kopii dokumentów w szufladach biurka, szafach meblowych zamykanych na klucz, przestrzeganie zasady czystego biurka, zabezpieczenie dokumentów przed wglądem nieuprawnionych osób trzecich w tym członków rodziny przed uszkodzeniem lub utratą), ponadto zabrania się wtórnego kopiowania tych dokumentów. Po zakończeniu pracy z kopią dokumentu wyrejestrowujemy go z ewidencji, następnie niszczymy kopię,
   e) wykorzystywanie posiadanych danych osobowych oraz innych danych objętych treścią dokumentów wyłączne w tym celu, w jakim były wykorzystywane w siedzibie pracodawcy,
7. Należy ograniczyć do niezbędnego minimum drukowanie dokumentacji zawierającej dane osobowe oraz inne dane, a jeżeli taka konieczność zaistnieje, należy niszczyć wydruki po zakończeniu pracy z nimi.
8. Nie jest dopuszczalne korzystanie i zapisywanie na własnych nośnikach plików zawierających dane osobowe oraz inne dane których administratorem jest pracodawca, bez uzyskania zgody i bez wcześniejszego zabezpieczenia takiego nośnika (tj. zaszyfrowania go) przez Dział Obsługi Informatycznej (DOI).
9. Nie jest dopuszczalne umożliwianie dostępu do wszelkich przetwarzanych danych, służbowej poczty elektronicznej lub systemów informatycznych osobom nieuprawnionym (w tym domownikom) oraz próbujących uzyskać dostęp drogą telefoniczną lub mailową, podającym się za przedstawicieli serwisu lub konkretnych instytucji, bez ich uprzedniej weryfikacji i potwierdzenia u pracodawcy takiego kontaktu.
10. Podczas pracy zdalnej przetwarzamy dane osobowe oraz inne dane będące w zasobach pracodawcy w systemach teleinformatycznych pracodawcy. Zabronione jest korzystanie z nieautoryzowanych przez pracodawcę innych systemów informatycznych.

IV. Obowiązki pracowników korzystających wyłącznie z poczty elektronicznej

Każdy pracownik korzystający z poczty elektronicznej jest zobowiązany do:

1) przechowywania loginu i hasła do poczty elektronicznej w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych, w tym domowników,
2) korzystania z poczty elektronicznej wyłącznie w celach służbowych,
3) archiwizowania korespondencji służbowej przy użyciu dedykowanych temu celowi narzędzi poczty elektronicznej,
4) nieprzesyłania korespondencji służbowej na jakąkolwiek prywatną skrzynkę mailową.

V. Obowiązki pracowników korzystających z poczty elektronicznej i systemów teleinformatycznych

Każdy pracownik korzystający z poczty elektronicznej i systemów teleinformatycznych Pracodawcy jest zobowiązany do:

1) stosowania zasad określonych w pkt IV,
2) nieudostępniania danych dostępowych do systemów informatycznych osobom nieuprawnionym, w tym domownikom,
3) niepobierania danych osobowych oraz innych danych z systemów informatycznych pracodawcy w celu innym niż służbowy,
4) pobierania i zapisywania tylko niezbędnych dokumentów,
5) opuszczania systemu informatycznego poprzez wylogowanie się z niego.

VI. Obowiązki podczas spotkań zdalnych, wideokonferencji

1. Organizacja spotkań może nastąpić tylko przy użyciu dostarczonych przez pracodawcę rozwiązań informatycznych.
2. Podczas spotkań przebiegających z ujawnianiem wizerunków należy ograniczyć do minimum rejestrowanie spotkań.
3. 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.
4. Wszystkie pliki zapisywane w zespołach lub dedykowanej do tego przestrzeni w aplikacji do wideokonferencji należy cyklicznie przeglądać i usuwać po ustaniu ich przydatności.
5. Linki do wideokonferencji powinny być udostępniane tylko i wyłącznie uczestnikom spotkania, bezpiecznym kanałem komunikacji, zaproszenia powinny być kierowane wyłącznie na służbowe adresy e-mail.