Załącznik nr 9
do Porozumienia o zasadach wykonywania pracy zdalnej w UEP

Procedura ochrony danych osobowych przy pracy zdalnej

1. Każdy pracownik Uniwersytetu Ekonomicznego w Poznaniu (UEP), w tym również wykonujący pracę w trybie pracy zdalnej, jest zobowiązany do przestrzegania postanowień Polityki Ochrony Danych Osobowych obowiązującej w Uczelni, niezależnie od miejsca wykonywania pracy.
2. Pracownik podczas pracy zdalnej może przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
3. Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność.
4. Na pracowniku ciąży obowiązek dbałości o dobro zakładu pracy w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.
5. Pracownik zobowiązany jest natychmiastowo powiadomić Inspektora Ochrony Danych (rodo@ue.poznan.pl) oraz bezpośredniego przełożonego o jakimkolwiek incydencie związanym z wyciekiem danych, zarówno w formie elektronicznej, jak i papierowej, jak również o kradzieży lub zaginięciu powierzonego mu sprzętu.
6. Pracownik ponosi odpowiedzialność za bezpieczeństwo i dostęp do powierzonego mu sprzętu oraz za prawidłową jego eksploatację.
7. Pracownik zobowiązany jest do zabezpieczenia miejsca pracy w celu ochrony przetwarzanych informacji oraz powierzonego sprzętu przed dostępem osób postronnych lub zniszczeniem. W szczególności, pracownik zobowiązany jest do ochrony danych osobowych oraz innych danych stanowiących tajemnicę służbową przed osobami postronnymi, w tym także osobami wspólnie z nim mieszkającymi.
8. Niedopuszczalne jest przetwarzanie w ramach pracy zdalnej informacji niejawnych podlegających ochronie na podstawie ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych.
9. Informacje, niezależnie od nośnika, na którym zostały zapisane, przeznaczone do użytku służbowego (stanowiące własność UEP bądź sporządzane przez pracowników UEP) mogą być wykorzystywane wyłącznie do celów związanych z wykonywaniem obowiązków służbowych. Należy zabezpieczyć dostęp do tych informacji przez osoby nieuprawnione, w tym dzieci i domowników.
10. Usługi, sprzęt i oprogramowanie (w szczególności komputery stacjonarne i przenośne, telefon, dostęp do Internetu), będące własnością bądź dostarczane przez UEP, mogą być wykorzystywane wyłącznie do celów służbowych. Sposób korzystania z tych usług i urządzeń może być rejestrowany oraz monitorowany i kontrolowany.
11. Na laptopie służbowym oraz na telefonie służbowym nie może być instalowane żadne nielegalne oprogramowanie lub niewymagane oprogramowanie do pracy zdalnej w powierzonym zakresie.
12. Zabronione jest:
    1) przechowywanie na dyskach twardych komputerów oraz na dyskach sieciowych plików niezwiązanych z wykonywanymi obowiązkami służbowymi, w szczególności zawierających treści erotyczne, pornograficzne, rasistowskie;
    2) przechowywanie w środkach przetwarzania informacji oprogramowania, utworów muzycznych i wideo oraz innych plików, których używanie może powodować naruszenie praw własności intelektualnej.

13. Pracownik ponosi konsekwencje przechowywania i wykorzystywania nielegalnego oprogramowania oraz materiałów i plików, o których mowa w ust. 12 pkt 1 i 2 w powierzonych mu środkach przetwarzania informacji (np. komputerze).
14. Wynoszenie dokumentacji papierowej z siedziby Pracodawcy powinno być ograniczone do niezbędnego minimum i może odbyć się wyłącznie za zgodą przełożonego. Pracodawca może zezwolić pracownikom na korzystanie z dokumentacji papierowej zawierającej dane osobowe w trakcie pracy zdalnej tylko w wyjątkowych sytuacjach. Generalną zasadą jest praca w obiegu elektronicznym.
15. Drukowanie dokumentów na potrzeby pracy należy ograniczyć do niezbędnego minimum. Dokumenty zawierające dane osobowe powinny być drukowane w siedzibie UEP.
16. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej – dokumenty i ich kopie powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach, należy zabezpieczyć dostęp do nich osób nieuprawnionych, w tym dzieci i domowników.
17. Po zakończeniu pracy pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.
18. Pracownik nie może korzystać z laptopa służbowego w miejscach publicznych.