Załącznik Nr 3 do regulaminu wykonywania pracy zdalnej okazjonalnej w Zespole Ośrodków Wsparcia w Lublinie

# Instrukcja ochrony danych osobowych w pracy zdalnej w Zespole Ośrodków Wsparcia w Lublinie

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja:

1. Administrator - Dyrektor Zespołu Ośrodków Wsparcia w Lublinie,
2. Inspektor Ochrony Danych Zespołu Ośrodków Wsparcia w Lublinie,
3. Administrator Systemu Informatycznego Zespołu Ośrodków Wsparcia w Lublinie.

Zakres dostępu do dokumentu – odczyt:

1. Administrator - Dyrektor Zespołu Ośrodków Wsparcia w Lublinie,
2. Kierownictwo Jednostki Organizacyjnej Zespołu Ośrodków Wsparcia w Lublinie,
3. Inspektor ochrony danych Zespołu Ośrodków Wsparcia w Lublinie,
4. Pracownicy Zespołu Ośrodków Wsparcia w Lublinie,
5. Administratorzy Systemów Informatycznych Zespołu Ośrodków Wsparcia w Lublinie,
6. Podmioty trzecie zarządzające systemem informatycznym Zespołu Ośrodków Wsparcia w Lublinie, upoważnione przez Kierownictwo tej Jednostki w zakresie adekwatnym do realizowanych przez nie zadań ,
7. Podmioty trzecie, które mają dostęp do danych osobowych zgromadzonych w Jednostkach Organizacyjnych ZOW Lublin na mocy zawartych umów w zakresie adekwatnym do realizowanych przez nie zadań,
8. Podmioty i instytucje upoważnione na podstawie przepisów prawa.

Załącznik Nr 3 do regulaminu wykonywania pracy zdalnej okazjonalnej w Zespole Ośrodków Wsparcia w Lublinie

## I. Zasady Ogólne

1. Niniejsza Instrukcja określa zasady bezpieczeństwa informacji i danych osobowych w trakcie pracy zdalnej.
2. Pracodawca, przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie dla pracowników wykonujących pracę zdalną.
3. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność. 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 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.

## II. Praca z danymi w obiegu elektronicznym

1. Zgodnie z regulaminem wykonywania pracy zdalnej okazjonalnej w Zespole Ośrodków Wsparcia w Lublinie dopuszcza się pracę zdalną przy użyciu prywatnego urządzenia komputerowego pracownika w przypadku uzyskania pisemnej zgody Pracodawcy.
2. Pracownik może wykorzystywać sprzęty mobilny wyłącznie zgodnie z zasadami określonymi w niniejszej Instrukcji.
3. Sprzęt mobilny bez względu na miejsce użytkowania powinien być należycie zabezpieczony przed nieuprawnionym dostępem, kradzieżą, zniszczeniem oraz innym działaniami, które mogą wpłynąć na jego bezpieczeństwo.
4. Pracownik odpowiada za zabezpieczenie sprzętu przed dostępem osób trzecich, a w szczególności zakazuje się udostępniania laptopa osobom trzecim, w tym także członkom rodziny w trakcie pracy zdalnej.
5. Na laptopie ani na telefonie wykorzystywanym do pracy zdalnej nie powinno być instalowane żadne nielegalne oprogramowanie.
6. Pracownik nie może przechowywać żadnych danych ani informacji na innych nośnikach niż te dopuszczone przez Pracodawcę do pracy zdalnej.
7. Zabronione jest używanie prywatnych kont pocztowych do przetwarzania danych osobowych. Sprawy służbowe mogą być załatwiane tylko i wyłącznie przy użyciu zweryfikowanego przez ASI laptopa oraz telefonu.
8. W przypadku konieczności użycia komputera przenośnego w miejscu publicznym, należy zachować szczególną ostrożność w celu zapobieżenia wyciekom informacji
9. Komputery oraz inne urządzenia mobilne powinny być zabezpieczone hasłem oraz posiadać szyfrowaną partycję służącą do przechowywania danych. Dane te powinny być zaszyfrowane w sposób uniemożliwiający ich bezpośrednie odczytanie przez osoby trzecie w przypadku utraty urządzenia.
10. W razie zgubienia lub kradzieży sprzętu komputerowego, użytkownik zobowiązany jest do natychmiastowego zgłoszenia incydentu bezpieczeństwa bezpośredniemu przełożonemu.

11. Hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową.
12. Przy wysyłaniu wiadomości e-mail Pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.
13. Pracownik nie może przesyłać treści podejrzanych, naruszających prawa własności intelektualnej, zabronionych prawnie.
14. W przypadku wiadomości zawierających informacje poufne lub o charakterze tajemnicy przedsiębiorstwa konieczne jest szyfrowanie wiadomości z podwójną weryfikacją hasłem.
15. W przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z ASI.

## III. Praca z dokumentami papierowymi

1. Wynoszenie dokumentacji papierowej z siedziby Pracodawcy powinno być ograniczone do niezbędnego minimum. Pracodawca może zezwolić Pracownikowi na korzystanie z dokumentacji papierowej zawierającej dane osobowe w trakcie pracy zdalnej tylko w wyjątkowych sytuacjach. Generalną zasadą jest praca w obiegu elektronicznym.
2. W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą zakładu pracy w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której Pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.
3. Drukowanie dokumentów na potrzeby pracy należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.
4. Wydawane oryginały dokumentów na potrzeby pracy zdalnej podlegają ewidencji przez przełożonego.
5. Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce i w taki sposób, aby były niewidocznie dla osób trzecich.
6. 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.
7. Po wykorzystaniu oryginałów dokumentów powinny one zostać niezwłocznie zwrócone. Zwrot dokumentów podlega odnotowaniu w prowadzonej ewidencji.
8. Po wykorzystaniu kopii dokumentacji powinny one zostać w całości zniszczone przez Pracownika. W przypadku nieposiadania niszczarki w miejscu pracy Pracownika powinien on wykonane kopie zniszczyć niezwłocznie w siedzibie zakładu pracy.
9. Po zakończeniu pracy Pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.