Załącznik Nr 1

Do Zarządzenia Nr ŚDS.021.9.2023

Procedura ochrony danych osobowych

przetwarzanych podczas pracy zdalnej w Środowiskowym Domu Samopomocy w Solcu Kujawskim

Niniejsza Procedura określa zasady bezpieczeństwa informacji i danych osobowych w trakcie pracy zdalnej.

1. Pracodawca, przeprowadza instruktaż i szkolenie w tym zakresie dla Pracowników wykonujących pracę zdalną.
2. Pracownicy podczas pracy zdalnej mogą 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. Na Pracowniku ciąży obowiązek dbałości o dobro zakładu pracy w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.
4. Pracownik w miarę możliwości zobowiązany jest do zmiany domyślnego hasła do domowego routera oraz korzystania z VPN przy kontaktach służbowych.
5. Prowadząc służbowe rozmowy telefoniczne Pracownik zobowiązany jest do zachowania poufności poprzez unikanie rozmów w obecności osób postronnych oraz w miejscach, w których rozmowa może być słyszalna przez osoby postronne.
6. Pracownik zobowiązany jest natychmiast powiadomić ASI oraz bezpośredniego przełożonego o jakimkolwiek incydencie związanym z naruszeniem ochrony danych osobowych, wyciekiem danych jak również z zagubieniem dokumentacji papierowej lub nośnika danych zawierających dane osobowe lub poufne informacje.
7. Pracownik zobowiązany jest natychmiast powiadomić ASI oraz bezpośredniego przełożonego o kradzieży lub utracie powierzonego mu sprzętu w celu natychmiastowego odłączenia go od zasobów sieciowych Pracodawcy.

Praca z danymi w obiegu elektronicznym

1. Instalowanie jakiegokolwiek oprogramowania na laptopie służbowym jest możliwe tylko przez ASI za zgodą i zgodnie z jego wytycznymi.
2. Na laptopie służbowym ani na telefonie służbowym nie może być instalowane żadne nielegalne oprogramowanie.
3. Pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich, a w szczególności domowników i dzieci.
4. Pracownik nie może udostępniać sprzętu służbowego do użytku osobom trzecim, a w szczególności domownikom i dzieciom.

5. Pracownik nie może przechowywać żadnych danych ani informacji na innych nośnikach niż udostępnione mu przez Pracodawcę.
6. Zabronione jest zapisywanie informacji i danych na dyskach komputerów prywatnych.
7. Sprawy służbowe mogą być załatwiane tylko i wyłącznie przy użyciu laptopa służbowego oraz telefonu służbowego.
8. Za zgodą Pracodawcy do połączenia z siecią Pracodawcy Pracownik może używać prywatnego sprzętu (laptopa, komputera). Uprawnienia do podłączenia urządzenia niebędącego własnością Pracodawcy nadawane przez ASI są jedynie na czas niezbędny do wykonania czynności, dla których urządzenie to ma być podłączone do sieci Pracodawcy.
9. Do komunikacji służbowej Pracownik może wykorzystywać jedynie służbową skrzynkę pocztową.
10. Zabronione jest uruchamianie przekierowań wiadomości ze służbowej skrzynki mailowej na prywatną.
11. Zabronione jest korzystanie do celów służbowych z komunikatorów dostępnych w sieciach i usługach społecznościowych.
12. Pracownik nie może korzystać ze sprzętu służbowego w celach prywatnych.
13. Pracownik nie może przechowywać na laptopie ani telefonie służbowym plików niezwiązanych z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.
14. Pracownik nie może bez uzgodnienia z ASI instalować na telefonie służbowym ani na laptopie służbowym prywatnych aplikacji lub oprogramowania.
15. Pracownik odpowiada za ochronę powierzonego mu sprzętu służbowego, nie może korzystać z laptopa służbowego w miejscach publicznych.
16. Laptop służbowy oraz telefon służbowy chronione są hasłem, a laptopy dodatkowo są szyfrowane.
17. Pracownik nie może łączyć się z systemami i dyskami sieciowymi z innego sprzętu niż sprzęt służbowy.
18. Hasła do poczty elektronicznej oraz do używanych programów i aplikacji nie powinny być zapisywane przez przeglądarkę internetową.
19. Przy wysyłaniu wiadomości e-mail Pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.
20. Pracownik zobowiązany jest do zwracania szczególnej uwagi na otrzymywane wiadomości, w tym do czytania dokładnie treści, zwracania uwagi na adres nadawcy oraz linki w wiadomościach.
21. Pracownik nie może przesyłać treści podejrzanych, naruszających prawa własności intelektualnej, zabronionych prawnie.
22. W przypadku wiadomości zawierających dane osobowe lub inne informacje poufne Pracownik zobowiązany jest umieścić je w zaszyfrowanym załączniku do wiadomości.
23. Pracownik jest zobowiązany do ochrony zawartości ekranu komputerowego przed dostępem osób postronnych.

24. W przypadku zauważenia problemów z funkcjonowaniem sprzętu służbowego Pracownik natychmiast powinien je zgłosić do ASI. W przypadku potrzeby konserwacji lub aktualizacji oprogramowania na służbowym laptopie Pracownik ma obowiązek dostarczyć sprzęt do ASI. W przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z ASI.

Praca z dokumentami papierowymi

1. Wynoszenie dokumentacji papierowej z siedziby Pracodawcy powinno być ograniczone do niezbędnego minimum. Pracodawca może zezwolić na korzystanie z dokumentacji papierowej zawierającej dane osobowe oraz informacje poufne 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 Pracodawcy w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której Pracownik będzie pracował. Kopie dokumentów z danymi osobowymi oraz informacjami poufnymi podlegają takiej samej ochronie jak oryginały.
3. Drukowanie dokumentów na potrzeby pracy zdalnej należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy 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, służącej do przewożenia dokumentów 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 powinien odbywać się na takich samych zasadach jak wynoszenie dokumentów – z zabezpieczonej aktówce. Zwrot dokumentów podlega odnotowaniu w prowadzonej ewidencji.
8. Po wykorzystaniu kopii dokumentacji powinny one zostać w całości zniszczone. W przypadku nieposiadania niszczarki o minimalnej klasie niszczenia P-3 w miejscu pracy zdalnej Pracownik powinien on wykonane kopie zniszczyć niezwłocznie w siedzibie zakładu pracy.
9. Po zakończeniu pracy zdalnej Pracownik powinien bezwzględnie przestrzegać zasady czystego biurka oraz innych zasad opisanych w Polityce Bezpieczeństwa Danych Osobowych.

Postanowienia końcowe

1. Procedura wchodzi w życie z dniem 7 kwietnia 2023 roku
2. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy obowiązujące w zakresie ochrony danych osobowych.
3. Oświadczenie pracownika dot. procedury ochrony danych osobowych