Załącznik nr 1 do Zarządzenia nr 45
Dyrektora WSSE w Gorzowie Wlkp.
z dnia 21 grudnia 2023 r.

Procedura ochrony danych osobowych podczas wykonywania pracy zdalnej.

I. Informacje ogólne:

Pracownik wykonujący pracę poza Wojewódzką Stacją Sanitarno-Epidemiologiczną w Gorzowie Wlkp. (praca zdalna) jest zobowiązany do przestrzegania zasad ochrony danych osobowych określonych w dokumentacji RODO Wojewódzkiej Stacji Sanitarno-Epidemiologicznej w Gorzowie Wlkp., w tym:

- INSTRUKCJI PRZETWARZANIA DANYCH OSOBOWYCH (PO/WSSE-02/I-01)
- INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM (PO/WSSE-02/I-02)
- Procedury: ZACHOWANIE POUFNOŚCI INFORMACJI ORAZ OCHRONA PRAW WŁASNOŚCI KLIENTA (PO/WSSE – 02)
- Regulaminu Ochrony Danych Osobowych w Wojewódzkiej Stacji Sanitarno-Epidemiologicznej w Gorzowie Wlkp.

II. Warunki pracy zdalnej:

1. Pracodawca zapewnia pracownikowi wsparcie w ustanowieniu bezpiecznego dostępu do infrastruktury IT organizacji poprzez np. użycie zdalnego pulpitu/VPN/innych aplikacji.
2. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.

III. Zasady pracy ze sprzętem komputerowym.

1. Podczas pracy zdalnej pracownik powinien tak zorganizować stanowisko pracy by osoby nieupoważnione (w tym członkowie rodziny) nie mieli wglądu w ekran monitora.
2. Pracownik nie może udostępniać innym osobom danych służących do uwierzytelnienia do systemów i/lub usług.
3. Zabrania się udostępniania informacji poufnych innym osobom (także członkom rodziny).
4. Zabrania się używania do połączenia internetowego publicznej sieci wi-fi.
5. Każdorazowo - podczas przerw w pracy i odejściu od komputera lub zakończeniu pracy danego dnia należy wylogować się z systemów oraz wyłączyć zdalne połączenie.

IV. Zasady postępowania z dokumentami w formie papierowej.

1. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich zabrania do domu na czas wykonywania pracy zdalnej lub wykonania niezbędnych kopii.
2. Podczas przewożenia dokumentów do miejsca wykonywania pracy zdalnej należy zachować szczególną ostrożność, aby nie doszło do ich zagubienia lub kradzieży.

Trzeba zapewnić bezpieczne przewożenie dokumentacji papierowej np. w teczkach, aktówkach, plecakach.

3. Dokumentacja w miejscu wykonywania pracy zdalnej powinna być zabezpieczona przed dostępem nieupoważnionych osób tam przebywających, np. w szafie, biurku zamykanym na klucz.
4. Zabrania się poza miejscem wykonywania pracy zdalnej, pozostawiania dokumentów w miejscach dostępnych dla osób nieupoważnionych.
5. Po zakończeniu pracy dokumenty należy zwrócić pracodawcy lub zniszczyć je w niszczarce.

V. Zasady korzystania z poczty elektronicznej.

1. Komunikacja powinna odbywać się za pomocą elektronicznej poczty służbowej.
2. Pliki zawierające dane osobowe przed wysłaniem ich do odbiorców, powinny być zabezpieczone hasłem, które należy przekazać odbiorcy telefonicznie, SMS lub inną drogą komunikacji.
3. W przypadku zabezpieczenia plików hasłem, należy stosować się do obowiązującej w WSSE „Polityki haseł".
4. Przy wysłaniu wiadomości należy upewnić się, że jest ona kierowana do odpowiedniego odbiorcy.
5. Nie należy otwierać załączników poczty pochodzącej z nieznanych, nietypowych źródeł lub podszywających się pod rzeczywistych nadawców.
6. Zakazane jest otwieranie hiper-linków, gdyż grozi to zainfekowaniem komputera.
7. Nie wolno wprowadzać loginów i haseł do formularzy zawartych w poczcie.
8. Należy zgłaszać służbom IT wszystkie przypadki podejrzanych e-maili, plików w e-mailach, prób wyłudzeń haseł dostępowych, kontaktów podejrzanych osób o próby uzyskania nieuprawnionego dostępu do danych.
9. W przypadku wysyłania informacji do odbiorców, z zastrzeżeniem ich poufności lub gdy ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji Ukrytej kopii (UDW/BCC), tzn. adresy należy wpisać w ww. pole.

VI. Obowiązek zachowania poufności i ochrony danych osobowych przez pracownika.

1. Pracownik wykonujący pracę zdalną jest zobowiązany do zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Pracownik jest zobowiązany do zachowania w tajemnicy danych osobowych, do których ma dostęp.
3. Pracownik jest zobowiązany do niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań.
4. Pracownik jest zobowiązany do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
5. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować.

6. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się podstawą prawną do dostępu do takich danych. W przypadkach wątpliwych należy skontaktować się z bezpośrednim przełożonym lub Inspektorem Ochrony Danych.

VII. Postępowanie w przypadku naruszenia ochrony danych osobowych.

1. Każdy pracownik zobowiązany jest do powiadomienia pracodawcy, bezpośredniego przełożonego lub Inspektora Ochrony Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do incydentów wymagających powiadomienia należą:
   a) zdarzenia losowe zewnętrzne (utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata/zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, nieświadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),
   d) telefoniczne próby wyłudzenia danych osobowych,
   e) kradzież, zagubienie komputerów, CD, DVD, dysków przenośnych, pendrive z danymi osobowymi,
   f) e-maile zachęcające do ujawnienia identyfikatora oraz hasła.
3. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji należy niezwłocznie zgłosić zdarzenie do pracodawcy, służbom IT oraz Inspektorowi Ochrony Danych.

Ja niżej podpisana/podpisany oświadczam, że zapoznałam/zapoznałem się z procedurą ochrony danych osobowych podczas wykonywania pracy zdalnej i zobowiązuję się przestrzegać zasad w niej zapisanych.

……..
Data/podpis pracownika