

Zarządzenie Nr WG.0050.469.2020
Wójta Gminy Ożarówce

z dnia 28 października 2020 roku

w sprawie wprowadzenia Regulaminu bezpieczeństwa danych osobowych podczas wykonywania pracy zdalnej w Urzędzie Gminy Ożarówce

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2020 r., poz. 713) w związku z art. 3 ustawy z 20 marca 2020r.o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t.j. Dz. U. z 2020 r., poz. 1842)

zarządzam, co następuje:

§ 1.

Wprowadza się Regulamin bezpieczeństwa danych osobowych podczas wykonywania pracy zdalnej w Urzędzie Gminy Ożarówce, który stanowi załącznik do niniejszego Zarządzenia.

§ 2.

Zobowiązuje się wszystkich pracowników Urzędu Gminy Ożarówce do zapoznania się z Regulaminem bezpieczeństwa danych osobowych podczas wykonywania pracy zdalnej w Urzędzie Gminy Ożarówce oraz do jego przestrzegania.

§ 3.

Wykonanie Zarządzenia powierza się pracownikom Urzędu Gminy Ożarówce.

§ 4.

Nadzór nad wykonaniem Zarządzenia powierza się Kierownikom poszczególnych komórek organizacyjnych Urzędu Gminy Ożarówce.

§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia.

Regulaminu bezpieczeństwa danych osobowych podczas wykonywania pracy zdalnej w Urzędzie Gminy Ożarówice

§ 1. Wprowadzenie

Niniejszy Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych podczas wykonywania pracy zdalnej na polecenie pracodawcy zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

§ 2. Warunki podjęcia pracy zdalnej

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy, zasady kontaktowania się z pracownikiem, określa kierownik komórki organizacyjnej.
4. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym Regulaminie.
5. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodne z niniejszym Regulaminem, warunki świadczenia tej pracy.
6. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.

§ 3. Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej

1. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych.
3. Każdy pracownik dopuszczony do pracy zdalnej zobowiązany jest do jej wykonywania wyłącznie w miejscu zamieszkania.
4. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
5. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera lub smartfona.

6. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z kierownikiem komórki organizacyjnej, co oznacza, że pracownik jest dostępny i realizuje swoje zadania w ustalonych godzinach.
7. Pracownik jest zobowiązany do wykonywania pracy zgodnie z zakresem obowiązków oraz przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych mu zadań.
8. Pracownik jest zobowiązany do zachowania w tajemnicy danych osobowych, do których ma dostęp.
9. Pracownik jest zobowiązany do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
10. Zabrania się przekazywania przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować.
11. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się podstawą prawną do dostępu do takich danych.
12. Odchodząc od komputera należy upewnić się, że urządzenie zostało zablokowane.

§ 4. Bezpieczeństwo pracy zdalnej

1. Internet

- 1) Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy lub prywatnych.
- 2) W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
 - a) korzystanie z internetu powinno wymagać uwierzytelnienia poprzez hasło,
 - b) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
- 3) Niedozwolone jest korzystanie z publicznej sieci WiFi.
- 4) Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela informatyk urzędu.

2. Urządzenia służące do pracy zdalnej

- 1) Praca zdalna może być realizowana z wykorzystaniem sprzętu służbowego lub prywatnego.
- 2) Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą wyłącznie do wykonywania obowiązków służbowych.
- 3) Zabronione jest udostępnianie urządzeń służbowych wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
- 4) Na sprzęcie służbowym zabronione jest samodzielne instalowanie dodatkowych aplikacji lub oprogramowania.
- 5) Pracownik ponosi odpowiedzialność za szkody spowodowane przez samowolną instalację oprogramowania.
- 6) Pracownik odpowiada za przechowywanie i wykorzystywanie, na powierzonym mu sprzęcie służbowym, materiałów i plików niezwiązanych z wykonywaniem obowiązków służbowych, mogących powodować naruszenie prawa własności intelektualnej.

- 7) Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
- 8) Urządzenie służbowe jest wydawane pracownikowi za protokołem.
- 9) Minimalne wymagania w zakresie bezpieczeństwa urządzeń służbowych:
 - a) na urządzeniu jest legalne i aktualne oprogramowanie,
 - b) zostały włączone automatyczne aktualizacje,
 - c) została włączona zapor systemowa,
 - d) został zainstalowany i działa w tle program antywirusowy,
 - e) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika,
 - f) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip),
 - g) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności.
- 10) Pracownik odpowiada za zabezpieczenie sprzętu IT przed zniszczeniem, uszkodzeniem, utratą oraz kradzieżą.
- 11) Pracownik zobowiązany jest do zabezpieczenia dostępu do sprzętu IT, nośników (pendrive) oraz danych osobowych na nich zawartych przed osobami postronnymi oraz domownikami.
- 12) Pracownik zobowiązany jest do bezpiecznego przewożenia sprzętu IT (bagażnik samochodu, torba na laptop).
- 13) Dane osobowe przechowywane na nośnikach (pendrive) poza siedzibą pracodawcy muszą być zaszyfrowane.
- 14) Zakazane jest kopiowanie/zapisywanie danych osobowych związanych z wykonywaniem zadań służbowych na niezabezpieczone prywatne nośniki zewnętrzne.

3. Zarządzanie uprawnieniami

- 1) Każdy użytkownik programów i systemu operacyjnego zobowiązany jest do pracy na własnym koncie.
- 2) Zabronione jest udostępnianie konta innemu użytkownikowi.
- 3) Użytkownik przed tymczasowym odejściem od komputera musi włączyć wygaszacz ekranu zabezpieczony hasłem (np. z użyciem kombinacji klawiszy WINDOWS + L) lub wylogować się z systemu bądź z programu.
- 4) Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, na których znajdują się dane osobowe.

4. Zabezpieczanie przekazywanych informacji

- 1) Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
- 2) Należy korzystać wyłącznie ze służbowej poczty elektronicznej.
- 3) Jeżeli niezbędne jest przesłanie informacji zawierających dane osobowe, powinno się je zabezpieczyć hasłem.

- 4) Jeżeli informacje zawierające dane osobowe będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
- 5) Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska i adres.
- 6) Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji (telefon, sms).
- 7) Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
- 8) Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
- 9) Rekomendowane metody zabezpieczania hasłem:
 - a) nadanie hasła do pliku, w którym są dane osobowe,
 - b) zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.
- 10) Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
- 11) W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji ukrytej kopii (UDW).
- 12) Nie wolno otwierać załączników poczty pochodzącej z nietypowych domen.
- 13) Nie wolno „klikać” na hiperlinki w podejrzanym poczcie, gdyż grozi to zainfekowaniem komputera.

5. Zasady korzystania z dokumentów w formie papierowej

- 1) Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.
- 2) Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.

§ 5. Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik zobowiązany jest do powiadomienia kierownika komórki organizacyjnej lub pracodawcy, Inspektora Ochrony Danych lub Administratora Systemów Informatycznych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do incydentów wymagających powiadomienia, należą:
 - 1) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twarde dyski, oprogramowania, pomyłki użytkowników, utrata/zagubienie danych),
 - 2) umyślne incydenty (włamanie do systemu informatycznego, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, nieświadome zniszczenie danych, działanie wirusów i innego szkodliwego oprogramowania),
 - 3) kradzież, zagubienie komputera lub pendrive z danymi osobowymi.

§ 6. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu służbowego lub oprogramowania należy niezwłocznie zgłosić informatykowi urzędu

2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie kierownikowi komórki organizacyjnej, który o zaistniałej sytuacji informuje pracodawcę, a także Inspektora Ochrony Danych i Administratora Systemów Informatycznych.

§ 7. Postanowienia końcowe

1. Pracownik świadczy pracę zdalną wyłącznie po przekazaniu przez pracodawcę pisemnego polecenia wykonywania pracy zdalnej.
2. Praca zdalna posiada zadaniowy charakter pracy.
3. Czas wykonywania pracy zdalnej określony jest w poleceniu pracodawcy. Zmiana okresu pracy zdalnej może być zmieniona przez pracodawcę, a pracownik zostanie o tym powiadomiony.
4. Przed przystąpieniem do pracy zdalnej pracownik zapoznaje się z treścią niniejszego Regulaminu, co potwierdza pisemnym oświadczeniem.

Wzór oświadczenia stanowi załącznik do Regulaminu.

.....
(imię i nazwisko pracownika)

**Oświadczenie o poufności przy wykonywaniu pracy zdalnej oraz zapoznaniu się
z Regulaminem bezpieczeństwa danych osobowych podczas wykonywania
pracy zdalnej w Urzędzie Gminy Ożarówce**

Oświadczam, iż zapoznałam/em się z zasadami wykonywania pracy zdalnej powierzonej mi przez pracodawcę zgodnie z „Regulaminem bezpieczeństwa danych osobowych podczas wykonywania pracy zdalnej w Urzędzie Gminy Ożarówce”.

W szczególności zobowiązuję się do:

- przetwarzania informacji wyłącznie w zakresie i celu przewidzianym w powierzonych przez pracodawcę zadaniach,
- zachowania w tajemnicy informacji, do których mam lub będę mieć dostęp w związku z wykonywaniem zadań podczas pracy zdalnej,
- zachowania w tajemnicy sposobów zabezpieczenia sprzętu IT i systemów informatycznych wykorzystywanych do pracy zdalnej,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych,
- niedopuszczania do komputera lub telefonu i innych nośników przekazanych mi przez pracodawcę oraz informacji w nich zawartych, w tym danych osobowych, domowników oraz innych osób trzecich,
- wykonywania pracy zdalnej wyłącznie w miejscu zamieszkania.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez pracodawcę za naruszenie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

.....
Podpis pracownika