ZARZĄDZENIE NR 27/2024
WÓJTA GMINA KOBYLANKA
z dnia 12 lutego 2024 r.

w sprawie wprowadzenia podstawowych zasad realizacji pracy w formie okazjonalnej pracy zdalnej oraz Procedur ochrony danych osobowych w ramach okazjonalnej pracy zdalnej

Na podstawie art. 67^{20} , art. 67^{33} oraz art. 67^{26} Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2022 r., poz. 1510, 1700, 2140, z 2023 r., poz. 240, 641), zarządza się co następuje:

§ 1. Wprowadza się podstawowe zasady realizacji pracy w formie okazjonalnej pracy zdalnej oraz procedury ochrony danych osobowych w ramach okazjonalnej pracy zdalnej w Urzędzie Gminy Kobylanka w brzmieniu określonym w załączniku do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podjęcia.

Wójt Gminy

Julita Pilecka

PODSTAWOWE ZASADY REALIZACJI PRACY W FORMIE OKAZJONALNEJ PRACY ZDALNEJ

§ 1
POSTANOWIENIA OGÓLNE

1. Praca zdalna okazjonalna może być wykonywana w przypadku:
    - stanu wyższej konieczności, który to stan wynika z oceny Pracodawcy lub jest wynikiem ustanowionych przepisów prawa lokalnego lub powszechnie obowiązującego albo,
    - w sytuacji wystąpienia szczególnych i incydentalnych okoliczności uzasadniających wykonywanie okazjonalnej pracy zdalnej,
    - pozytywnie rozpatrzonego przez Pracodawcę wniosku złożonego przez Pracownika, zawierającego uzasadnienie dla udzielenia możliwości realizacji pracy w sposób zdalny (załącznik nr 1).
2. Praca w formie zdalnej okazjonalnej jest możliwa wyłącznie w sytuacji, w której umożliwia pracownikowi realizację podstawowych obowiązków pracowniczych wynikających z powierzonego jemu zakresu czynności w czasie, w którym będzie trwała.
3. Pracodawca może odmówić udzielenia okazjonalnej pracy zdalnej ze względu na organizację, charakter i rodzaj wykonywanej pracy przez pracownika.
4. Wykonywanie okazjonalnej pracy zdalnej nie stanowi podstawy do nabycia ryczałtu rekompensującego koszty pracy zdalnej.
5. Strony mogą ustalić zasady wykorzystywania przez pracownika wykonującego pracę zdalną materiałów i narzędzi pracy, w tym urządzeń technicznych, niezbędnych do wykonywania pracy zdalnej, niezapewnionych przez pracodawcę. Pracownik jest zobowiązany do wykonywania pracy zgodnie z treścią umowy łączącej go z Pracodawcą oraz zakresem obowiązków.
6. Pracodawca ma prawo kontrolowania wykonywania okazjonalnej pracy zdalnej oraz żądania od Pracownika informacji o jej wynikach. Kontrola może odbywać się przy wykorzystaniu środków porozumiewania się na odległość jak również bezpośrednio w miejscu świadczenia okazjonalnej pracy zdalnej. Kontrola przeprowadzana w miejscu świadczenia pracy w porozumieniu z Pracownikiem, w godzinach pracy Pracownika, nie może naruszać jego prywatności ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z przeznaczeniem.
7. W przypadku stwierdzenia uchybień lub nieprawidłowości podczas kontroli okazjonalnej pracy zdalnej w zakresie bezpieczeństwa i higieny pracy, nieprawidłowości organizacji stanowiska pracy lub w przestrzeganiu wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym danych osobowych oraz procedur przyjętych przez Pracodawcę, zobowiąże on Pracownika do niezwłocznego usunięcia stwierdzonych uchybień. W przypadku braku możliwości usunięcia uchybień kontynuowanie pracy w formie zdalnej zostanie uznane za niemożliwe.

8. Przy pracy zdalnej okazjonalnej nie znajdują zastosowania art. 67^{19} – 67^{24} oraz art. 67^{31} Kodeksu Pracy.

§ 2
PRZETWARZANIE INFORMACJI

1. Niniejsze zasady zostały przygotowane dla potrzeb związanych z ochroną informacji przy wykonywaniu pracy w formie zdalnej i określają podstawowe wymogi obowiązujące Pracownika podczas wykonywania pracy w formule zdalnej.
2. Świadczenie obowiązku pracy w formule zdalnej nie zwalnia pracownika z obowiązku przestrzegania wymogów w zakresie bezpieczeństwa przetwarzania informacji określonych w wewnętrznych dokumentach obowiązujących u Pracodawcy. W związku ze świadczeniem pracy zdalnej Pracownik powinien przestrzegać wewnętrznych dokumentów funkcjonujących u Pracodawcy odnoszących się do przetwarzania danych osobowych, tj. Polityki ochrony danych osobowych, Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym. Niniejsze zasady stosuje się jako uzupełnienie ww. aktów wewnętrznych.
3. Pracodawca ma prawo przeprowadzać kontrolę przestrzegania przez Pracownika wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych, na zasadach określonych w aktach wewnętrznych wymienionych w §1 ust.2 oraz niniejszych zasadach.

§ 3
ZABEZPIECZENIA I OBOWIĄZKI ORGANIZACYJNE

1. Pracownik wykonuje pracę zdalną w miejscu zamieszkania lub w innym miejscu uzgodnionym z Pracodawcą.
2. Pracownik zobowiązuje się do dbania o bezpieczeństwo organizacyjne oraz techniczne w związku ze świadczeniem pracy zdalnej, poprzez:
    - stworzenie bezpiecznego i ergonomicznego stanowiska pracy,
    - zapewnienie okoliczności, w których lokalizacja stanowiska pracy będzie znajdowała się w tzw. strefie bezpiecznej, do której nie będą miały dostępu osoby trzecie w trakcie realizacji pracy zdalnej,
    - stosowanie zasady „czystego biurka” i „czystego ekranu”,
    - zabezpieczanie po zakończonej pracy przed dostępem powierzonych jemu służbowych urządzeń takich jak komputer, telefon, pendrive, a także nośników papierowych zawierających dane osobowe lub inne informacje klasyfikowane jako chronione przed osobami postronnymi, w tym domownikami.

3. W przypadku przekazania urządzeń technicznych przez Pracodawcę Pracownik zobowiązuje się do zabezpieczania powierzonych urządzeń, o których mowa w § 1 ust.5 oraz nośników informacji (niezależnie od ich postaci – papierowe i elektroniczne), zawierających dane osobowe lub inne informacje chronione przed zniszczeniem, utratą, w tym zagubieniem.
4. Pracownik nie może użytkować sprzętu ani nośników papierowych lub elektronicznych zawierających dane osobowe lub inne informacje poufne Pracodawcy w miejscach publicznych, takich jak: restauracje, bary, parki, centra handlowe, sklepy, parkingi (nawet w zamkniętym pojeździe), środki komunikacji publicznej, biblioteki
5. W przypadku zmiany warunków lokalowych i technicznych uniemożliwiających wykonywanie pracy zdalnej lub zachowanie warunków określonych w Polityce ochrony danych osobowych i Polityce Bezpieczeństwa Informacji, Pracownik informuje o tym niezwłocznie Pracodawcę.
6. W przypadku przekazania urządzeń technicznych przez Pracodawcę, Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. Pracownik niezwłocznie zgłasza Pracodawcy wszelkie uzasadnione potrzeby w tym zakresie.
7. W przypadku przekazania urządzeń technicznych przez Pracodawcę, Pracownik jest zobowiązany korzystać z powierzonego mu przez Pracodawcę Sprzętu wyłącznie w celach służbowych.

§ 4
ZABEZPIECZENIA I OBOWIĄZKI TECHNICZNE

1. W przypadku przekazania urządzeń technicznych przez Pracodawcę, Pracownik jest zobowiązany wykonywać pracę zdalną, wykorzystując sprzęt powierzony mu przez Pracodawcę.
2. Pracownik nie może dokonywać modyfikacji w powierzonym sprzęcie, w szczególności poprzez instalację nowego oprogramowania lub dezinstalację oprogramowania już istniejącego.
3. Jeśli pojawią się jakiekolwiek problemy z przekazanym sprzętem (związane z fizycznym działaniem lub oprogramowaniem), lub jeśli Pracownik zauważy nietypowe lub podejrzane działania powinien o tym natychmiast powiadomić Pracodawcę.
4. Pracownik zobowiązany jest do używania jedynie zaufanego dostępu do sieci bez możliwości korzystania z otwartych sieci publicznych.
5. Jeśli pracownik korzysta z połączenia WIFI, sieć WIFI powinna być zabezpieczona hasłem.
6. Pracownik jest zobowiązany do korzystania ze służbowej skrzynki pocztowej (e-mail) wyłącznie w celach służbowych. Pracownik nie może korzystać z prywatnej skrzynki pocztowej (e-mail) w celach służbowych.

7. Korzystając z poczty email lub dostępów do systemów online w chmurze na swoim sprzęcie nie należy pozwalać przeglądarce na zapamiętywanie danych logowania.
8. Zabrania się kopiowania lub przenoszenia jakichkolwiek danych osobowych przetwarzanych przez Pracodawcę lub innych informacji poufnych Pracodawcy na prywatne komputery, urządzenia mobilne i innego rodzaju sprzęt.
9. Wszystkie informacje, materiały i dokumenty wytworzone lub używane przez Pracownika w ramach pracy zdalnej muszą być przechowywane na serwerze Pracodawcy. Jeżeli Pracodawca przewiduje korzystanie z przechowywania plików w chmurze, Pracownik powinien korzystać z takiego rozwiązania.
10. Jeżeli Pracownik nie pracuje w chmurze ani nie korzysta z dostępu do serwerów Pracodawcy, to jest zobowiązany do zadbania o to, aby przechowywane dane zostały bezpiecznie zarchiwizowane na powierzonym przez Pracodawcę sprzęcie .
11. Należy dokonywać niezbędnych aktualizacji sprzętu, systemu operacyjnego lub stosowanych na nich zabezpieczeń wg zaleceń Administratora Systemu Informatycznego.
12. Pracownik zobowiązany jest zwracać szczególną uwagę na poprawność adresu odbiorcy pliku, dokumentu lub innych danych. Przed wysłaniem wiadomości e-mail należy przynajmniej jednokrotnie zweryfikować poprawność adresu. Przy rozsyłaniu korespondencji e-mail wielu adresatom należy używać funkcji UDW, pozwalającej na ukrycie adresów e-mail adresatów.
13. Pracownik zobowiązany jest zwracać szczególną uwagę podczas używania poczty email na adres nadawcy. Każdą podejrzaną dyspozycję powinien sprawdzić innym kanałem komunikacji.
14. W sytuacji, gdy Pracownik przekazuje za pośrednictwem komunikacji elektronicznej pliki zawierające dane osobowe, powinny one zostać zaszyfrowane odpowiednim oprogramowaniem, a klucz do tych plików powinien zostać przekazany adresatowi inną drogą (np. SMS).
15. Nie należy otwierać podejrzanych załączników lub klikać w nieznane linki przesłane drogą elektroniczną za pośrednictwem maila. Wszystkie podejrzane sytuacje powinien zgłosić niezwłocznie do Administratora Systemu Informatycznego.
16. Pracownik zobowiązany jest do przestrzegania następujących zasad:
    - stosowania haseł dostępu do sprzętu. Zabronione jest dezaktywowanie haseł oraz wyłączanie opcji uwierzytelniania dwuskładnikowego tam, gdzie jest ona wymagana przez Pracodawcę,
    - niemodyfikowania konfiguracji dotyczącej ochrony antywirusowej,

- weryfikacji, czy ewentualne logowanie się do aplikacji odbywa się za pomocą szyfrowanego połączenia SSL/TLS (z kłódką oraz adresem www rozpoczynającego się frazą „https.”),
- blokować komputer podczas każdej przerwy w pracy,
- po skończonej pracy zamykać komputer (nie „usypiać” czy „hibernować”)

17. Pracownik jest zobowiązany przestrzegać prawa własności intelektualnej osób trzecich, w tym prawa własności przemysłowej i prawa autorskiego, jak również innych przepisów powszechnie obowiązującego prawa.
18. Pracownik nie ma prawa korzystać ze sprzętu w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym, niestosownym, mając na uwadze powszechnie obowiązujące zasady postępowania.

Wniosek o wykonywanie okazjonalnej pracy zdalnej

Na podstawie art. 67^{33} Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2022 r. poz. 1510, 1700, 2140, z 2023 r. poz. 240.) składam wniosek o dopuszczenie do wykonywania przeze mnie okazjonalnej pracy zdalnej w dniu …….. w związku ……
……

Wnoszę o uzgodnienie miejsca wykonywania OPZ pod adresem:

……

(adres zamieszkania)

Oświadczam, że na stanowisku pracy zdalnej w ww. miejscu są zapewnione bezpieczne i higieniczne warunki tej pracy.

Oświadczam, że zapoznałem się z przygotowaną przez Pracodawcę:

1. Oceną ryzyka zawodowego,
2. Informacją zawierającą zasady bezpiecznego i higienicznego wykonywania pracy zdalnej,
3. Informacją określającą procedury ochrony danych osobowych,

oraz zobowiązuję się do przestrzegania informacji, procedur, wskazówek i wniosków wynikających z tych dokumentów.
Zasady kontroli wykonywania pracy zdalnej, kontrola w zakresie bezpieczeństwa i higieny pracy lub kontrola przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych ustaliłem z pracodawcą w dniu…….. i zobowiązuję się do ich stosowania w czasie wykonywania okazjonalnej pracy zdalnej.

……

Podpis pracownika