

ZARZĄDZENIE NR 49/2023
BURMISTRZA MIASTA PUCK

z dnia 7 kwietnia 2023 r.

**zmieniające Zarządzenie nr 97/2019 w sprawie wprowadzenia Polityki
Bezpieczeństwa w Urzędzie Miasta Puck**

Na podstawie art. 31 i art. 33 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. 2023 r. poz. 40) Burmistrz Miasta Puck zarządza, co następuje:

§ 1. Zmienia się zarządzenie nr 97/2019 Burmistrza Miasta Puck z dnia 10 czerwca 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miasta Puck w ten sposób, że w rozdziale 9 załącznika do zarządzenia, dodaje się punkt 7a o treści: "7a. Wprowadza się „Regulamin ochrony danych osobowych podczas świadczenia okazjonalnej pracy zdalnej” oraz dodaje się załącznik Nr 17 o treści załączonej do niniejszego zarządzenia."

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta
Puck Hanna Pruchniewska

**Regulamin ochrony danych osobowych podczas
świadczenia okazjonalnej pracy zdalnej**

I. Wprowadzenie

1. Niniejszy regulamin określa zasady ochrony danych osobowych podczas świadczenia okazjonalnej pracy zdalnej i jest wprowadzany w związku z przepisami rozporządzenia PEiR (UE) nr 2016/679 z 27.04.2016 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 – dalej RODO oraz ustawy z dnia 26 czerwca 1974 r. Kodeks pracy oraz Zarządzenia Burmistrza Miasta Puck Nr 41/2023 w sprawie wykonywania pracy zdalnej przez pracowników Urzędu Miasta Puck.

2. W Regulaminie pod określeniem "pracownik" należy rozumieć osoby zatrudnione w ramach stosunku pracy. Pod określeniem "pracodawca" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi.

II. Warunki podjęcia pracy zdalnej

1. O możliwości podjęcia okazjonalnej pracy zdalnej przez pracownika decyduje pracodawca.

2. Pracownik może zgłosić pracodawcy chęć podjęcia okazjonalnej pracy zdalnej za pomocą wniosku stanowiącego Załącznik nr 1 do Zarządzenia Nr 41/2023 Burmistrza Miasta Puck w sprawie wykonywania pracy zdalnej przez pracowników Urzędu Miasta Puck.

3. Warunki i zasady okazjonalnej pracy zdalnej, określa pracodawca w odrębnym regulaminie.

4. W przypadku podjęcia okazjonalnej pracy zdalnej pracownika obowiązują zasady ochrony danych osobowych podczas pracy zdalnej określone w niniejszym Regulaminie.

5. Pracownik podejmując okazjonalną pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki techniczne i lokalowe oraz ochrony danych osobowych w miejscu wykonywania pracy zdalnej.

6. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie z jego instrukcjami.

7. Pracownik zobowiązany jest natychmiastowo powiadomić informatyka (tel. 58 673 05 36) oraz 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.

8. Pracownik podczas okazjonalnej pracy zdalnej może przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.

9. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.

III. Miejsce świadczenia okazjonalnej pracy zdalnej

1. Pracownik musi zapewnić właściwe warunki umożliwiające mu świadczenie skutecznej okazjonalnej pracy zdalnej z zachowaniem właściwego poziomu bezpieczeństwa informacji.

2. Pracownik wykonuje okazjonalną pracę zdalną pod adresem, który wskazał pracodawcy. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, jak kawiarnie, restauracje, galerie handlowe itp., gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.

3. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz smartfona, a także zapewnienie pracy

4. Odchodząc od komputera lub kończąc korzystanie ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.

5. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych jest realizowane w sposób zapewniający poufność informacji przekazywanych w trakcie spotkania/ rozmowy.

IV. Bezpieczeństwo okazjonalnej pracy zdalnej Internet

1. Pracownik wykonuje okazjonalną pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy lub odpowiednio zabezpieczonych urządzeń prywatnych

2. Jeżeli pracodawca udostępnia pracownikowi modem internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik korzysta z tych urządzeń do połączeń z Internetem. Korzystanie z domowej sieci internetowej odbywa się za zgodą i wiedzą pracodawcy.

3. 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, np. poprzez hasło,
- b) Sieć powinna być zaszyfrowana w standardzie minimum WPA, hasło powinno składać się z dużych i małych liter oraz cyfr i znaków specjalnych.
- c) Jeśli to możliwe, należy zmienić login i hasło do panelu administracyjnego routera na własny.
- d) Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.

4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela informatyk Urzędu Miasta Puck. Urządzenia służące do pracy zdalnej

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.

2. Praca zdalna jest realizowana z wykorzystaniem służbowego sprzętu, jak i prywatnego komputera stacjonarnego lub laptopa. Zabronione jest używanie nieodpowiednio zabezpieczonego prywatnego sprzętu lub prywatnych kont pocztowych do przetwarzania danych osobowych. Sprawy służbowe mogą być załatwiane tylko i wyłącznie przy użyciu laptopa służbowego, zabezpieczonego komputera prywatnego lub telefonu służbowego.

3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy oraz zgodę na korzystanie z odpowiednio zabezpieczonego prywatnego sprzętu do celów służbowych.

4. Urządzenie służbowe jest wydawane pracownikowi za protokołem.

5. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt do informatyka Urzędu Miasta Puck.

6. Informatyk odnotowuje, które urządzenia są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.

7. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie informatyka udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez informatyka narzędzia), w celu dokonania jego zdalnego przeglądu.

8. Przegląd urządzeń prywatnych, na których wykorzystanie pracodawca wyraził zgodę, jest obowiązkowy.

9. Minimalne wymagania w zakresie bezpieczeństwa:

- a) Na urządzeniu jest legalne i aktualne oprogramowanie (system operacyjny, program antywirusowy);
- 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, kod PIN lub token;
- f) Wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;
- g) Został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
- h) Zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności;
- i) Jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami;

10. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:

- a) Zaszyfrowany dysk
- b) Wyłączone porty pamięci zewnętrznych
- c) Oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy. Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik wykorzystuje tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.

2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, uprzednio należy je zabezpieczyć hasłem.

3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, należy przysyłać je w załączniku zabezpieczonym hasłem.

4. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska czy adresy e-mail.

5. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.

6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.

7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą, o ile nie będzie wykorzystywane do zabezpieczania plików w komunikacji z innymi odbiorcami.

8. 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.

9. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.

10. 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/BCC), tzn. adresy wpisać w to pole.

11. Masowe wysyłki wiadomości e-mail należy realizować poprzez specjalne oprogramowanie udostępnione w tym celu przez pracodawcę.

12. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików. Zasady korzystania z dokumentów w formie papierowej

1. Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.

2. Obowiązuje ogólny zakaz wynoszenia dokumentów lub ich kopii poza siedzibę pracodawcy.

3. Jeżeli do świadczenia okazjonalnej pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy pisemną prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.

4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.

5. Zabronione jest wynoszenie poza siedzibę pracodawcy oryginałów dokumentów.

6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.

7. Informacja jest przekazywana pracodawcy.

8. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić

9. Praca z dokumentami nie może być wykonywana w miejscu publicznym (np. kawiarnia, restauracja, galeria handlowa, komunikacja publiczna itp.)

10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, lub osobie upoważnionej przez pracodawcę który weryfikuje ich kompletność.

11. Pracownik zapewnia zabezpieczenie dokumentów w miejscu wykonywania pracy zdalnej, poprzez przechowywanie w szafie zamykanej na klucz, do której tylko on ma dostęp.

12. Po dostarczeniu kopii dokumentów do Urzędu Miasta Puck, należy je niezwłocznie zniszczyć, jeżeli nie będą już potrzebne.

V. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do informatyka Urzędu Miasta Puck.

2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, informatyka, a także inspektora ochrony danych.

VI. Działania niedozwolone

1. Niedozwolone jest:

- a) Udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
- b) Przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
- c) Przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
- d) Korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę;
- e) Odmówienie pracownikowi działu IT przeglądu urządzenia;
- f) Niszczenie dokumentów w domu;
- g) Udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
- h) Dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
- i) Samodzielne zniszczenie dokumentów w domu;
- j) Logowanie się na konto innego użytkownika;
- k) Zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;
- l) Zabranie oryginałów dokumentów; ł) Niezwrócenie dokumentów;
- m) Niepotwierdzenie z pracodawcą zakresu zwróconych danych. Oświadczam, że zapoznałam/em się z Regulaminem ochrony danych podczas wykonywania okazjonalnej pracy zdalnej na rzecz Urzędu Miasta Puck i jest on dla mnie zrozumiały Data
i podpis Pracownika