

**Zarządzenie Nr 56/2023**  
**Burmistrza Miasta i Gminy Olsztyn**  
**z dnia 9.05.2023 r.**

**w sprawie zmiany Zarządzenia nr 58 Burmistrza Miasta i Gminy Olsztyn z dnia 12 maja 2022 r. w sprawie wprowadzenia Polityki Bezpieczeństwa przetwarzania danych osobowych Urzędu Miasta i Gminy Olsztyn**

na podstawie:

- Art. 24 ust. 1 i 2 Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 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 nazywanego ogólnym Rozporządzeniem o ochronie danych osobowych (RODO) (Dz.U.UE.L.2016.119.1 z późn. zm.);
- § 20 ust. 2 pkt 8 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247 t.j.)

zarządzam co następuje:

§ 1.

§ 1 Zarządzenia otrzymuje brzmienie:

„1. Wprowadzam **Politykę Bezpieczeństwa przetwarzania danych osobowych Urzędu Miasta i Gminy Olsztyn** stanowiącą załącznik nr 1 do niniejszego zarządzenia, której integralną częścią są :

- a) Załącznik 1 - Instrukcja zabezpieczenia systemu informatycznego,
- b) Załącznik 2 - Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w systemie informatycznym,
- c) Załącznik 3 - Wzór rejestru czynności przetwarzania,
- d) Załącznik 4 - Wzór rejestru kategorii czynności przetwarzania,
- e) Załącznik 5 - Instrukcja niszczenia nośników danych osobowych,
- f) Załącznik 6 - Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń.
- g) Załącznik 7 – Dokumentacja systemu informatycznego wspierającego zadania publiczne
- h) Załącznik 8 – Zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.”

§ 2.

Zarządzenie wchodzi w życie z dniem ogłoszenia.

**Burmistrz**  
*Tomasz Kucharski*



## **ZASADY GWARANTUJĄCE BEZPIECZNĄ PRACĘ PRZY PRZETWARZANIU MOBILNYM I PRACY NA ODLEGŁOŚĆ**

Celem niniejszej procedury jest zapewnienie bezpiecznego procesu przetwarzania danych osobowych w pracy poza siedzibą Urzędu zgodnie z Art. 24 ust. 1 i 2 Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 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 nazywanego ogólnym Rozporządzeniem o ochronie danych osobowych (RODO) (Dz.U.UE.L.2016.119.1 z późn. zm.); oraz § 20 ust. 2 pkt 8 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247 t.j.)

### **§ 1.**

#### **Postanowienia ogólne**

1. Pracownik może wykonywać pracę poza siedzibą Urzędu po złożeniu wniosku i wyrażeniu zgody przez pracodawcę lub wydaniu przez pracodawcę polecenia w postaci papierowej lub elektronicznej.
2. Pracownik, który wykonuje pracę poza siedzibą jednostki zobowiązany jest w jej trakcie do przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych oraz innymi przepisami regulującymi pracę Urzędu Miasta i Gminy Olsztyn, zwłaszcza z polityką bezpieczeństwa przetwarzania danych osobowych, w tym instrukcją zarządzania systemami informatycznymi.
3. W ramach pracy poza siedzibą Urzędu pracownik zobowiązany jest do przetwarzania udostępnionych mu danych osobowych jedynie w celach służbowych, określonych w zakresie obowiązków.
4. Zabronione jest wykorzystywanie przez pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.
5. Wykonywanie pracy poza siedzibą jednostki odbywa się na służbowym sprzęcie komputerowym.

### **§ 2.**

#### **Przygotowanie i weryfikacja zabezpieczeń komputera, przed rozpoczęciem pracy poza siedzibą Urzędu:**

1. Informatyk, w razie potrzeby, zakłada konto VPN i nadaje uprawnienia, zgodnie z wnioskiem o pracę poza siedzibą Urzędu.
2. Informatyk szyfruje dane znajdujące się na komputerze, wykorzystywanym do pracy mobilnej (poza siedzibą Urzędu).
3. Informatyk weryfikuje, czy właściwie wykonywana jest kopia danych komputera, wykorzystywanego do pracy mobilnej tj. zgodnie z paragrafem 3 Instrukcji Zabezpieczenia Systemu Informatycznego Urzędu Miasta i Gminy Olsztyn.
4. Informatyk weryfikuje status aktualizacji systemu antywirusowego komputera.

### **§ 3.**

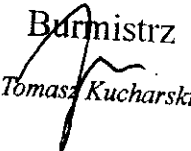
#### **Bezpieczne przetwarzanie danych osobowych zawartych w dokumentacji papierowej podczas pracy poza siedzibą Urzędu**

1. Dokumentacja papierowa zawierająca dane osobowe udostępniana jest pracownikowi w zakresie niezbędnym do realizacji obowiązków służbowych, za pisemną zgodą kierownika referatu.

2. Po otrzymaniu zgody pracownik sporządza kopie dokumentów niezbędnych do realizacji jego obowiązków służbowych.
3. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
4. Po wykonaniu kopii dokumentów pracownik przygotowuje zestawienie określające jakie dokumenty, w jakiej liczbie zostały skopiowane, następnie przekazuje je kierownikowi referatu.
5. Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia w taki sposób, aby były niewidoczne dla osób trzecich, na przykład w teczce wykonanej z nieprzezroczystego materiału.
7. Praca z dokumentami nie może być wykonywana w miejscach publicznych, na przykład w kawiarni, galerii handlowej itp.
8. Podczas pracy poza siedzibą Urzędu pracownik zobowiązany jest przechowywać udostępnione kopie dokumentów papierowych tylko przez okres niezbędny do wykonania określonego zadania podczas pracy (zasada ograniczenia przetwarzania). Po tym czasie zobowiązany jest niezwłocznie zwrócić je kierownikowi.
9. Po weryfikacji kompletności dokumentów zwróconych przez pracownika, kierownik niszczy kopie dokumentów.
10. Zabrania się pracownikowi samodzielnego niszczenia dokumentacji uzyskanej od kierownika lub samodzielnie wytworzonej.

#### **§ 4. Obowiązki pracownika**

1. W okresie wykonywania pracy poza siedzibą Urzędu, z wykorzystaniem sprzętu informatycznego, Pracownik, w razie potrzeby wykorzystania zasobów systemów informatycznych Urzędu, ma obowiązek wykorzystać szyfrowane połączenie VPN.
2. Pracownik zobowiązuje się do zabezpieczenia dostępu do sprzętu służbowego oraz posiadanych danych i informacji przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi, oraz przed zniszczeniem lub modyfikacją.
3. Wykonywanie pracy na odległość, nie zwalnia pracownika z obowiązku przestrzegania postanowień Polityki Bezpieczeństwa Urzędu Miasta i Gminy Olsztyn, przyjętej u Pracodawcy wraz z dokumentami powiązanymi.
4. Zalecane jest blokowanie komputera w razie oddalenia się od miejsca pracy, wykonywanej poza siedzibą Urzędu.
5. Po zakończeniu pracy, należy każdorazowo wylogować się z systemów informatycznych Urzędu wykorzystywanych do pracy oraz z systemu VPN, jeżeli takowe były wykorzystywane.
6. Zalecane jest podłączenie sprzętu komputerowego do zabezpieczonej, domowej sieci WiFi. Zabronione jest korzystanie z otwartych sieci WiFi (np. WiFi hotelowe, w galeriach handlowych czy hot-spoty w kawiarniach)
7. Praca poza siedzibą urzędu wykonywana jest w godzinach zgodnych z rozkładem czasu pracy danego pracownika.

**Burmistrz**  
  
*Tomasz Kucharski*