Załącznik nr 3
do zarządzenia nr 0050.1846.2023.VIII
Prezydenta Miasta Jeleniej Góry
z dnia 28 kwietnia 2023 r.

Zasady ochrony danych osobowych podczas pracy zdalnej w trybie okazjonalnym w Urzędzie Miasta Jelenia Góra

Ochrona danych osobowych podczas pracy zdalnej

1. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
2. Podczas wykonywania pracy zdalnej Pracownik zobowiązany jest do przestrzegania przepisów prawa w zakresie ochrony danych osobowych oraz wszystkich procedur wewnętrznych obowiązujących w Urzędzie.
3. Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność.
4. Pracownik zobowiązany jest natychmiastowo powiadomić Inspektora Ochrony Danych Osobowych telefonicznie pod nr tel. 75 75 49 860 lub mailowo iodo_um@jeleniagora.pl oraz bezpośredniego przełożonego o jakimkolwiek incydencie związanym z wyciekiem danych, zarówno w formie elektronicznej jak i papierowej oraz o kradzieży lub zaginięciu powierzonego mu sprzętu.

Praca z danymi w obiegu elektronicznym

1. Instalowanie jakiegokolwiek oprogramowania na laptopie służbowym jest możliwe tylko przez pracowników Referatu Informatyki lub za ich zgodą i zgodnie z ich wytycznymi.
2. Na laptopie służbowym nie może być instalowane żadne nielegalne oprogramowanie.
3. Pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich, a w szczególności domowników i dzieci.
4. Pracownik nie może nagrywać ani przechowywać żadnych danych ani informacji na zewnętrznych nośnikach danych.
5. Zabronione jest używanie prywatnego sprzętu lub prywatnych kont pocztowych do przetwarzania danych osobowych. Sprawy służbowe mogą być załatwiane tylko i wyłącznie przy użyciu laptopa służbowego.
6. Pracownik nie może przechowywać na służbowym laptopie plików niezwiązanych z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.
7. Pracownik odpowiada za ochronę powierzonego mu sprzętu służbowego, nie może korzystać z laptopa służbowego w miejscach publicznych.
8. Laptop służbowy chroniony jest hasłem oraz dodatkowo jest szyfrowany.
9. Pracownik nie może łączyć się z wewnętrznymi systemami Urzędu i dyskami sieciowymi z innego sprzętu niż sprzęt służbowy. Łącząc się z zasobami sieciowymi urzędu Pracownik jest zobowiązany korzystać z bezpiecznego połączenia za pomocą sieci VPN.
10. Hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową.
11. Przy wysyłaniu wiadomości e-mail Pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.
12. Pracownik nie może przesyłać treści podejrzanych, naruszających prawa własności intelektualnej, zabronionych prawnie.
13. W przypadku wiadomości zawierających informacje poufne lub o charakterze tajemnicy przedsiębiorstwa konieczne jest szyfrowanie wiadomości z weryfikacją hasła oraz przesłanie hasła do odbiorcy innym kanałem komunikacji niż poczta email.
14. W przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z Referatem Informatyki.

Praca z dokumentami papierowymi

1. Wynoszenie dokumentacji papierowej z siedziby Urzędu powinno być ograniczone do niezbędnego minimum. Bezpośredni przełożony może zezwolić pracownikom na korzystanie z dokumentacji papierowej zawierającej dane osobowe w trakcie pracy zdalnej tylko w wyjątkowych sytuacjach. Generalną zasadą jest praca w obiegu elektronicznym.
2. W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą Urzędu **należy wykonać kopię dokumentów**, na której Pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.
3. Drukowanie dokumentów na potrzeby pracy zdanej należy ograniczyć do niezbędnego minimum.
4. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.
5. Wydawane kopie dokumentów na potrzeby pracy zdalnej podlegają ewidencji przez bezpośredniego przełożonego.
6. Wynoszenie dokumentów powinno mieć miejsce w zabezpieczonej aktówce i w taki sposób, aby były niewidocznie dla osób trzecich.
7. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej - dokumenty powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach, należy zabezpieczyć dostęp do nich osób nieuprawnionych, w tym dzieci i domowników.
8. Po powrocie z pracy zdalnej zwrot kopii dokumentów podlega odnotowaniu w prowadzonej ewidencji, po czym Pracownik powinien wykonane kopie zniszczyć.
9. Po zakończeniu pracy Pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.

Prezydent Miasta Jeleniej Góry

Jerzy Łużniak