# ZARZĄDZENIE NR 100/2023 BURMISTRZA KONSTANTYNOWA ŁÓDZKIEGO z dnia 18 maja 2023 roku

**w sprawie wprowadzenia Procedury ochrony danych osobowych podczas pracy zdalnej**

Na podstawie art. (artykułu) 31 oraz art. 33 ust. (ustęp) 1 i ust. 3 ustawy z dnia 8 marca 1990 r. (roku) o samorządzie gminnym (tekst jednolity Dziennik Ustaw z 2023 r. poz. (pozycja) 40), 6726 ustawy z dnia 26 czerwca 1974 r. Kodeksu pracy tekst jednolity Dziennik Ustaw z 2022 r. poz. 1510 z późn. zm.) , **Burmistrz Konstantynowa Łódzkiego zarządza, co następuje:**

1. Wprowadzam Procedurę ochrony danych osobowych podczas pracy zdalnej.
2. Zobowiązuję pracowników do zapoznania się z Procedurą przed rozpoczęciem pracy zdalnej.
3. Zarządzenie wchodzi w życie z dniem podpisania.

**BURMISTRZ KONSTANTYNOWA ŁÓDZKIEGO**

**Robert Jakubowski**

**Procedura ochrony danych osobowych w pracy zdalnej**

**1.** Niniejsza Procedura określa zasady bezpieczeństwa informacji i danych osobowych w trakcie pracy zdalnej.

**2.** Pracodawca, przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie dla pracowników wykonujących pracę zdalną.

**3.** Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.

**4.** Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność. Na pracowniku ciąży obowiązek dbałości o dobro zakładu pracy w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.

**5.** Pracownik zobowiązany jest natychmiastowo powiadomić Dział IT 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.

**Praca z danymi w obiegu elektronicznym**

**6.** Instalowanie jakiegokolwiek oprogramowania na laptopie służbowym jest możliwe tylko przez pracowników Działu IT lub za ich zgodą i zgodnie z ich wytycznymi.

**7.** Na laptopie służbowym ani na telefonie służbowym nie może być instalowane żadne nielegalne oprogramowanie.

**8.** Pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich, a w szczególności domowników i dzieci.

**9.** Pracownik nie może przechowywać żadnych danych ani informacji na innych nośnikach niż udostępnione mu przez Pracodawcę.

**10.** 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 oraz telefonu służbowego.

**11.** Pracownik nie może przechowywać na laptopie ani telefonie służbowym plików niezwiązanych z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.

**12.** Pracownik nie może bez uzgodnienia z Działem IT instalować na telefonie służbowym ani na laptopie służbowym prywatnych aplikacji lub oprogramowania.

**13.** Pracownik odpowiada za ochronę powierzonego mu sprzętu służbowego, nie może korzystać z laptopa służbowego w miejscach publicznych.

**14.** Laptop służbowy oraz telefon służbowy chronione są hasłem, a laptopy dodatkowo są szyfrowane.

**15.** Pracownik nie może łączyć się z firmowymi systemami i dyskami sieciowymi z innego sprzętu niż sprzęt służbowy. Łącząc się z zasobami sieciowymi Pracodawcy Pracownik jest zobowiązany korzystać z bezpiecznego połączenia za pomocą sieci VPN.

**16.** Hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową.

**17.** Przy wysyłaniu wiadomości e-mail Pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.

**18.** Pracownik nie może przesyłać treści podejrzanych, naruszających prawa własności intelektualnej, zabronionych prawnie.

**19.** W przypadku wiadomości zawierających informacje poufne lub o charakterze tajemnicy przedsiębiorstwa konieczne jest szyfrowanie wiadomości z podwójną weryfikacją hasłem.

**20.** W przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z Działem IT.

**21.** Zasady bezpiecznego odbywania videokonferencji określa zał. nr 1.

**Praca z dokumentami papierowymi**

**22.** Wynoszenie dokumentacji papierowej z siedziby Pracodawcy powinno być ograniczone do niezbędnego minimum. Pracodawca 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.

**23.** W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą zakładu pracy w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której Pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.

**24.** Drukowanie dokumentów na potrzeby pracy należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.

**25.** Wydawane oryginały dokumentów na potrzeby pracy zdalnej podlegają ewidencji przez przełożonego.

**26.** Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce i w taki sposób, aby były niewidocznie dla osób trzecich.

**27.** Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej - dokumenty i ich kopie powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach, należy zabezpieczyć dostęp do nich osób nieuprawnionych, w tym dzieci i domowników.

**28.** Po wykorzystaniu oryginałów dokumentów powinny one zostać niezwłocznie zwrócone. Zwrot dokumentów podlega odnotowaniu w prowadzonej ewidencji.

**29.** Po wykorzystaniu kopii dokumentacji powinny one zostać w całości zniszczone przez Pracownika. W przypadku nieposiadania niszczarki w miejscu pracy Pracownika powinien on wykonane kopie zniszczyć niezwłocznie w siedzibie zakładu pracy.

**30.** Po zakończeniu pracy Pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.

**Załącznik nr 1**

**Zasady bezpiecznego prowadzenia wideokonferencji2**

|  |  |
| --- | --- |
| **Zasady bezpiecznego prowadzenia wideokonferencji** | |
| **Etapy wideokonferencji** | **Wytyczne** |
| Przed rozpoczęciem wideokonferencji | 1. Zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego chcesz skorzystać.  2. Sprawdź, czy Twoje rozmowy będą nagrywane i przechowywane.  3. Zweryfikuj, do jakich celów będą wykorzystywane Twoje dane osobowe.  4. Sprawdź, o jakie uprawnienia do danych jesteś proszony - lista kontaktów, lokalizacja itp.  5. Do zainstalowania aplikacji na komputerze użyj oficjalnej strony aplikacji, z której chcesz korzystać; w przypadku urządzeń mobilnych wybierz oficjalny sklep - Google Play lub App Store.  6. Upewnij się, że osoby postronne nie mają dostępu do Twojego ekranu.  7. Sprawdź, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie.  8. Korzystaj z aplikacji webowych, nie desktopowych.  9. Zabezpiecz sieć Wi-Fi silnym hasłem.  10. Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli.  11. Przy podłączeniu się do telekonferencji korzystaj z kodów dostępu/PIN-ów.  12. Przeskanuj program do telekonferencji systemem antywirusowym. |
| W trakcie korzystania z wideokonferencji | 1. Ogranicz ilość podawania danych osobowych - użyj pseudonimu i służbowego adresu e-mail.  2. Użyj innego hasła, niż używane przez Ciebie w innych usługach.  3. Nie udostępniaj linków do konferencji w mediach społecznościowych.  4. Włącz, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line.  5. Zarządzaj opcjami udostępniania ekranu.  6. W celu wykonywania rozmów służbowych wykorzystuj dostęp do sieci za pomocą szyfrowanego połączenia VPN.  7. Nie udostępniaj dokumentów służbowych za pomocą czatu, który może być publiczny.  8. Jeżeli to możliwe, korzystaj z opcji zamazywania tła (tak żeby rozmówcy nie widzieli Twojego otoczenia).  9. Korzystaj z opcji "poczekalnia", tak abyś mógł kontrolować osoby uczestniczące w telekonferencji; unikniesz przypadkowych lub niechcianych osób.  10. Logując się do telekonferencji, wyłącz mikrofon i kamerę (włączysz je, jak będzie to potrzebne). |
| Po skorzystaniu z wideokonferencji | 1. Wyłącz mikrofon i kamerę.  2. Upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację.  3. Sprawdź, czy program do telekonferencji nie działa w tle. |

2 Opracowano na podstawie: *https://uodo.gov.pl/pl/138/1525 (dostęp: 21.07.2022 r.).*