Zarządzenie Nr 39/2023
Burmistrza Miasta Świeradów – Zdrój
z dnia 15.05.2023 r.

w sprawie: wprowadzenia procedury ochrony danych osobowych podczas pracy zdalnej w Urzędzie Miasta Świeradów-Zdrój

Na podstawie art. 67^{26} ustawy z dnia z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2022 r. poz. 1510 ze zm.), art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2023 r. poz. 40 ze zm.), art. 24 i 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4 maja 2016 r., s. 1, Dz. Urz. UE L127 z dnia 23 maja 2018 r., s. 2)

zarządzam, co następuje:

§ 1.

Wprowadza się procedurę ochrony danych osobowych podczas pracy zdalnej w Urzędzie Miasta Świeradów-Zdrój, stanowiący załącznik do niniejszego zarządzenia.

§ 2.

Wykonanie zarządzenia powierzam Sekretarzowi Gminy

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta Świeradów-Zdrój
(-)Roland Marciniak

Załącznik nr 1
do Zarządzenia nr 39/2023 Burmistrza Miasta Świeradów-Zdrój
z dnia 15.05.2023 r.

PROCEDURA

OCHRONA DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ W URZĘDZIE MIASTA ŚWIERADÓW-ZDRÓJ

I. Postanowienia ogólne

1. **Praca zdalna** – praca wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość.
2. **Pracodawca** – Urząd Miasta z siedzibą przy ul. 11 Listopada 35, 59-850 Świeradów-Zdrój
3. **Administrator Danych Osobowych „ADO" –** Burmistrz Miasta Świeradów-Zdrój
4. **Inspektor Ochrony Danych** - osoba wyznaczona przez Administratora Danych Osobowych zwanego dalej „IOD".

II. Warunki miejsca świadczenia pracy zdalnej

1. Pracownik zapewnia właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, jak kawiarnie, restauracje, galerie handlowe, 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 z dokumentami w sposób uniemożliwiający wgląd do ich treści.
4. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
5. Odchodząc od komputera lub kończąc korzystanie ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.

III. Bezpieczeństwo pracy zdalnej

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych otrzymanych od pracodawcy albo na komputerze prywatnym.

2. Pracownik przed przystąpieniem do pracy upewnia się, że wszystkie urządzenia, z jakich korzysta, posiadają niezbędne aktualizacje systemu operacyjnego (IOS , Android lub Windows), oprogramowania oraz systemu antywirusowego.

3. Pracownik używa przede wszystkim służbowego konta e-mail. W przypadku korzystania z prywatnego e-maila, pracownik upewnia się, że treść i załączniki wiadomości są właściwie szyfrowane. Należy unikać używania danych osobowych lub poufnych informacji w temacie wiadomości.

4. Pracownik każdorazowo dokładnie sprawdza nadawcę e-maila oraz nie otwiera wiadomości od nieznanych adresatów, a zwłaszcza załączników oraz nie klika w link zawarty w takiej wiadomości.

5. Jeżeli pracodawca udostępnia pracownikowi modem internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik powinien korzystać w pierwszej kolejności z tych urządzeń.

6. 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) hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,

    c) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny,

    d) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej,

    e) został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny,

    f) porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela ADO bądź Administrator Systemu Informatycznego (ASI)/Informatyk.

7. W celu zapewnienia bezpiecznej pracy, pracownik zobowiązuje się do:

    a) zabezpieczenia stacji roboczej poprzez aktualne oprogramowanie antywirusowe,

    b) posiadania indywidualnego loginu dostępu do systemu,

    c) zabezpieczenia komputera hasłem o dużej złożoności hasła konta Administratora komputera i konta użytkownika, oraz pracowania na koncie z adekwatnym poziomem uprawnień,

    d) nieodchodzenia od komputera przed jego uprzednim zablokowaniem,

    e) nie zapisywania haseł na kartkach w szczególności nie zapisywanie ich w plikach na komputerze prywatnym a także nie udostępniania ich w jakikolwiek sposób innym osobom,

    f) nieudostępniania sprzętu innym osobom,

g) nieinstalowania oprogramowania niebezpiecznego i pochodzącego z niewiadomych źródeł,

h) w przypadku konieczności zapisania danych służbowych na komputerze należy przestrzegać zasad bezpiecznego przechowywania danych na komputerze, w tym szyfrowanie danych, i trwałego ich usuwania, z zastosowaniem stosownego oprogramowania (np. Eraser),

i) zadbania o bezpieczeństwo urządzeń w sieci domowej (np. silne hasło do sieci WiFi oraz aktualizacje oprogramowania urządzeń),

j) korzystania ze stabilnego i wydajnego łącza internetowego,

k) korzystania z bezpiecznych kanałów dostępności do Internetu (np. unikanie „otwartych" kanałów dostępowych WiFi),

l) korzystania z aktualnej przeglądarki internetowej. Zalecana jest praca w przeglądarce w tzw. trybie incognito,

m) nie wykonywania jednocześnie działań służbowych oraz prywatnych na tym samym komputerze; nie wykonywania pracy służbowej z własną aktywnością osobistą na przykład na portalach społecznościowych np. Facebooku,

n) unikania przeglądania stron potencjalnie niebezpiecznych,

o) nieużywania prywatnych skrzynek pocztowych czy grup na portalach społecznościowych do komunikacji firmowej,

p) w przypadku wykonywania pracy zdalnej w sposób inny niż z wykorzystaniem pulpitu zdalnego (np. w drodze dostępu do aplikacji służbowych za pomocą strony internetowej – poczty służbowej) – niezapisywania jakichkolwiek danych pracodawcy poza aplikacjami, w których taki zapis jest elementem ich funkcjonowania (np. zapisanie się wysłanego e-maila w katalogu wysłane). W szczególności zapisywania jakichkolwiek danych pracodawcy na dyskach prywatnego komputera, prywatnych nośnikach zewnętrznych lub na prywatnym koncie w usłudze chmurowej (np. Google Drive, iCloud, Microsoft Onedrive, Dropbox),

q) stosowanie się do wytycznych wydanych przez pracodawcę.

8. W przypadku utraty urządzenia, na którym pracuje, pracownik niezwłocznie informuje o tym fakcie ADO oraz Inspektora Ochrony Danych Osobowych.

IV. Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę, w tym służbową skrzynkę pocztową e-mail.

2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone i zaszyfrowane hasłem.

3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione 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.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
8. Rekomendowane metody zabezpieczania hasłem, tj.:
   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. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.
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.

V. Zakres obowiązywania procedury ochrony danych osobowych podczas wykonywania pracy zdalnej

1. Procedura ochrony danych osobowych podczas pracy zdalnej obowiązuje w strukturze organizacyjnej całego podmiotu jakim jest Urząd Miasta.

VI. Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy obowiązujące w zakresie ochrony danych osobowych.

Wykaz załączników:

- Oświadczenie pracownika w związku z podjęciem pracy zdalnej

Załącznik nr 1 – Oświadczenie pracownika w związku z podjęciem pracy zdalnej

Świeradów-Zdrój, dn. ……...

…….

(imię i nazwisko pracownika)

Oświadczenie pracownika w związku z podjęciem pracy zdalnej

Pouczony o odpowiedzialności, oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w tym z postanowieniami Rozporządzenia ogólnego o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz procedurami wewnętrznymi obowiązującymi w tym zakresie w tym również z **Procedurą ochrony danych osobowych podczas pracy zdalnej w Urzędzie Miasta Świeradów-Zdrój.**

Oświadczam, iż zapoznałem/-am się z zasadami ochrony danych osobowych poza miejscem pracy i zobowiązuję się do ich przestrzegania.

Dodatkowo, w związku z ochroną danych osobowych podczas wykonywania pracy zdalnej zobowiązuje się do zabezpieczania dostępu do sprzętu służbowego oraz posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi, oraz zniszczeniem.

Zobowiązuję się przestrzegać wszelkich wewnątrzzakładowych procedur dotyczących ochrony danych osobowych w Urzędzie Miasta Świeradów-Zdrój również podczas wykonywania pracy zdalnej w miejscu zamieszkania lub innym miejscu uzgodnionym z Pracodawcą oraz jestem zobowiązany/-a do wykonywania pracy zgodnie z treścią umowy łączącej mnie z Pracodawcą.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie przepisów Ustawy o ochronie danych osobowych oraz Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 roku.

…….

(podpis oświadczającego)