Załącznik do Zarządzenia Nr 4623/2023
Prezydenta Miasta Radomia
z dnia 28 czerwca 2023r.

Procedura bezpiecznego przetwarzania danych osobowych w pracy zdalnej Urzędu Miejskiego w Radomiu

I. WSTĘP

Ustanawia się poniższą procedurę bezpiecznego przetwarzania danych osobowych w pracy zdalnej Urzędu Miejskiego w Radomiu. Celem procedury jest ustalenie jednolitych zasad i zapewnienie bezpiecznego procesu przetwarzania danych osobowych w pracy zdalnej.

II. DOKUMENTY POWIĄZANE

- Polityka bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Miejskim w Radomiu.
- Instrukcja Zarządzania Systemem Informatycznym w tym do przetwarzania danych osobowych w Urzędzie Miejskim w Radomiu.
- Rejestr naruszeń ochrony danych.

III. WARUNKI KONIECZNE DO WYKONYWANIA PRACY ZDALNEJ

Pracownik jest zobowiązany do świadczenia pracy zdalnej we wskazanym miejscu po uzgodnieniu z pracodawcą poprzez zawarcie umowy o pracę lub w trakcie zatrudnienia (w formie zmiany warunków umowy o pracę niewymagającej formy pisemnej lub polecenia pracy zdalnej w szczególnych przypadkach) oraz po podpisaniu oświadczenia stanowiącego załącznik nr 1.

Pracownik wykonujący pracę zdalną zobowiązany jest w jej trakcie przetwarzać dane osobowe zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych oraz z „Polityką Bezpieczeństwa Informacji i Ochrony Danych Osobowych w Urzędzie Miejskim w Radomiu" i „Instrukcją zarządzania systemem informatycznym w tym do przetwarzania danych osobowych w Urzędzie Miejskim w Radomiu".

W ramach pracy zdalnej pracownik zobowiązany jest do przetwarzania udostępnionych mu danych osobowych jedynie w celach służbowych, określonych w umowie o pracę lub w poleceniu pracy zdalnej.

Zabronione jest wykorzystywanie przez pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.

1. **Bezpieczeństwo obszaru przetwarzania**
    a. Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych osobowych przetwarzanych przez niego w ramach pracy zdalnej.
    b. Pracownik zobowiązany jest do zachowania poufności informacji, w szczególności podczas służbowych rozmów telefonicznych lub wideokonferencji.
    c. Pracownik zobowiązany jest do zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.
    d. Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu.
    e. Pracownik zobowiązany jest do stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy.
    f. Pracownik zobowiązany jest po zakończeniu pracy na sprzęcie elektronicznym każdorazowo wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu i zabezpieczyć przed dostępem osób niepowołanych.

2. **Bezpieczeństwo sieci wykorzystywanej do pracy zdalnej**
    a. Sprzęt komputerowy powinien być podłączony do zabezpieczonej sieci. Zabronione jest korzystanie z otwartych sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych lub hot-spot w kawiarniach i tym podobnych.
    b. Dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem, którym nie jest hasło domyślne, zdefiniowane podczas pierwszej konfiguracji urządzenia.
    c. Oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.

3. **Bezpieczeństwo logowania**
    a. Dostęp do sprzętu lub programu wykorzystywanego do pracy zdalnej powinien być możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła.
    b. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być odpowiednio długie i złożone. Nie powinno być ono zbudowane za pomocą ciągu znajdujących się obok siebie znaków na klawiaturze lub oparte na prostych skojarzeniach związanych z użytkownikiem, na przykład numer telefonu, data urodzenia, imiona lub nazwiska.

c. Zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach nie gwarantujących ich poufności.
d. Zabronione jest domyślne zapamiętywanie hasła dostępu do konta użytkownika systemu na sprzęcie oraz programów wykorzystywanych w pracy zdalnej.

4. Bezpieczne korzystanie z programów i platform wykorzystywanych w pracy zdalnej (w tym wideokonferencji)

a. W przypadku korzystania z programów z funkcją wideokonferencji zaleca się wyłączenie opcji nagrywania i przechowywania.
b. W trakcie korzystania z programów lub platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych (zasada minimalizacji danych).
c. Zabronione jest korzystanie z prywatnego adresu e-mail do celów służbowych.
d. Zabrania się udostępniania dokumentów służbowych, za pomocą publicznego czatu lub innych komunikatorów.
e. Zabrania się udostępniania w mediach społecznościowych linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej.
f. Zaleca się udostępnianie linków do konferencji i innych aktywności realizowanych w ramach pracy zdalnej, na przykład poprzez wskazany adres e-mail.

5. Bezpieczne przechowywanie danych

a. Sprzęt komputerowy i inne urządzenia mobilne wykorzystywane w pracy tj.: laptop, telefon lub tablet powinny być zabezpieczone przed dostępem osób trzecich np. hasłem.
b. Zewnętrzne karty pamięci, a także inne nośniki danych, takie jak pendrive lub dyski zewnętrzne, wykorzystywane w celach służbowych w pracy zdalnej powinny być zabezpieczone hasłem przed dostępem osób trzecich.
c. Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych (np. Dysk Google), komunikatorach (np. Messenger) lub innych usługach dostępnych w sieci.

6. Ochrona przed cyberatakami

a. Sprzęt wykorzystywany do pracy zdalnej musi być wyposażony w uruchomione i zaktualizowane oprogramowanie antywirusowe.
b. Systemy, w tym system operacyjny i oprogramowanie wykorzystywane do pracy zdalnej musi być regularnie aktualizowany.
c. Komputer wykorzystywany do pracy zdalnej musi mieć uruchomioną zaporę sieciową.

7. Zachowanie bezpieczeństwa podczas pracy zdalnej

a. Zabrania się samodzielnej lub z wykorzystaniem wsparcia podmiotów zewnętrznych naprawy sprzętu służbowego wykorzystywanego do pracy zdalnej. W celu naprawy uszkodzonego sprzętu służbowego należy bezzwłocznie zwrócić go pracodawcy.

b. Zabrania się drukowania dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów czy osób trzecich.
c. Komunikacja z przełożonym lub innymi współpracownikami powinna być prowadzona za pośrednictwem wdrożonych w Urzędzie Miejskim w Radomiu rozwiązań teleinformatycznych.
d. Pracownik zobowiązany jest do weryfikowania nadawców wiadomości e -mail. W przypadku wątpliwości co do tożsamości nadawcy zabronione jest otwieranie załączników do wiadomości e-mail oraz hiperłączy znajdujących się w tekście.
e. Podczas wysyłania korespondencji zbiorczej pracownik zobowiązany jest do korzystania z opcji „kopia ukryta" dzięki której odbiorcy wiadomości nie zobaczą wzajemnie swoich adresów e-mail.
f. Pracownik zobowiązany jest do szyfrowania załączników zawierających dane osobowe dołączone do wiadomości e-mailowych np. poprzez archiwizację z hasłem i przekazywania hasła zawsze inną formą, na przykład telefonicznie.
g. Zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne konta e-mail.
h. Zabrania się włączać opcję autouzupełniania formularzy w opcjach przeglądarki internetowej.
i. Pracownik zobowiązany jest do stworzenia oddzielnego konta użytkownika systemu w pracy na prywatnym sprzęcie komputerowym, wykorzystywanym do pracy zdalnej. Konto użytkownika powinno posiadać ograniczone uprawnienia i być chronione silnym hasłem oraz nieudostępniane osobom trzecim.
j. Za legalność oprogramowania, w tym programu antywirusowego odpowiada właściciel sprzętu.
k. Po zakończeniu okresu pracy poza miejscem jej stałego wykonywania pracownik jest zobowiązany bezzwłocznie przekazać pracodawcy wszystkie dane związane z wykonywanymi zadaniami służbowymi zapisane na prywatnym sprzęcie (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje), a następnie usunąć je w sposób trwały.

IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ

Pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych, zobowiązany jest:

- do niezwłocznego poinformowania o tym pracodawcy – administratora danych i inspektora ochrony danych;
- zabezpieczenia dostępu do miejsca lub urządzeń celem zapobieżenia dalszym zagrożeniom, które mogłyby skutkować utratą danych osobowych;

- powstrzymania się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować brak możliwości identyfikacji naruszenia;
- współpracy w celu identyfikacji zagrożeń oraz zminimalizowanie jego ewentualnych negatywnych skutków, zastosowania działań naprawczych oraz zaradczych tak, aby zminimalizować wystąpienie podobnych naruszeń w przyszłości.

Zakres przekazanych niezbędnych informacji dotyczących naruszenia zawiera załącznik nr 2.

PREZYDENT MIASTA

(-) Radosław Witkowski

Załącznik nr 1

…… Radom, dnia ……r.

(imię i nazwisko)

……

(stanowisko)

O Ś W I A D C Z E N I E

Ja niżej podpisana(y), **oświadczam**, że wszelki sprzęt komputerowy oraz oprogramowanie będące własnością Urzędu Miejskiego w Radomiu, a udostępniony mi w celu świadczenia pracy zdalnej będę wykorzystywał(a) wyłącznie dla realizacji zadań służbowych, określonych w umowie o pracę lub innej umowie cywilnoprawnej. Oświadczam również, że prywatny sprzęt komputerowy wykorzystywany do pracy zdalnej posiada odpowiednie zabezpieczenia w postaci oprogramowania antywirusowego oraz stosownych haseł dostępu. Oświadczam, że zapoznałam(em) się, rozumiem i będę przestrzegać obowiązków wynikających z przepisów Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2019, poz. 1781), z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia27 kwietnia 2016r. oraz dokumentów przyjętych przez Urząd Miejski w Radomiu w związku z przetwarzaniem danych osobowych, a w szczególności: **Polityki bezpieczeństwa Informacji i ochrony danych osobowych; Instrukcji zarządzania systemem informatycznym w tym do przetwarzania danych osobowych, wprowadzonych Zarządzeniem Prezydenta Miasta Radomia Nr 3715/2022 z dnia 12 lipca 2022r.**

Zobowiązuję się do podejmowania działań zmierzających do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem oraz unikaniem tych zachowań, które mogłyby poziom bezpieczeństwa danych osobowych obniżyć.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w trakcie wykonywania pracy zdalnej, również po jej ustaniu.

Zobowiązuję się również do użytkowania powierzonego mi sprzętu komputerowego w sposób należyty, tak aby nie wyrządzić w nim szkody oraz zgodnie z zasadami określonymi w **„Instrukcji zarządzania systemem informatycznym, w tym do przetwarzania danych osobowych"** obowiązującej w Urzędzie Miejskim w Radomiu.

Urząd Miejski w Radomiu zastrzega sobie prawo monitorowania sposobu użycia sprzętu komputerowego oraz oprogramowania, będącego własnością Urzędu Miejskiego

w Radomiu, a udostępnionego w celu świadczenia pracy zdalnej.

Potwierdzam, że zdaję sobie sprawę z tego, że w razie naruszenia zasad, grozi mi odpowiedzialność materialna na podstawie art. 114 K.P., a także odpowiedzialność dyscyplinarna włączając utratę zatrudnienia - zgodnie z art. 52 K.P. (Dz.U. z 2022r., poz. 1510 t.j. z późn. zm ustawy z dnia 26 czerwca 1974r. - Kodeks Pracy), odpowiedzialność karna na podstawie art. 278 i 293 K.K. w związku z art. 291 i 292 (ustawy z dnia 6 czerwca 1997r. Kodeks Karny Dz.U. z 2022r., poz. 1138 t.j. z późn. zm) oraz odpowiedzialność karna i cywilna przewidziana w art. 116 i następnych (ustawy z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022r., poz.2509 t.j. z późn. zm) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnienie oprogramowania.

…… (podpis pracownika)

Załącznik nr 2

Zgłoszenie naruszenia ochrony danych

1. Imię i nazwisko osoby zgłaszającej:
   .....
2. Data i czas zaistnienia/ rozpoczęcia naruszenia
   .....
3. Naruszenie ochrony danych dotyczyło:
   a) zgubienia lub kradzieży nośnika/urządzenia;
   b) nieuprawnione uzyskanie dostępu do informacji;
   c) nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń;
   d) złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych;
   e) uzyskanie poufnych informacji poprzez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej;
   f) nieprawidłowa anonimizacja danych osobowych w dokumencie;
   g) nieprawidłowe usunięcie/ zniszczenie danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez administratora;
   h) niezamierzona publikacja;
   i) dane osobowe wysłane do niewłaściwego odbiorcy;
   j) ujawnienie danych niewłaściwej osobie;
   k) ustne ujawnienia danych osobowych;
   l) inne: .....
4. Szczegółowy opis kategorii osób i danych osobowych (np.: imię, nazwisko, data urodzenia, miejsce zamieszkanie, dane dotyczące zdrowia):

   .....
   .....

5. Opis okoliczności naruszenia

   .....
   .....
   .....