Zarządzenie Nr 7/2026
Dyrektora Oświaty Miejskiej w Otwocku
z dnia 16 czerwca 2026 r.

w sprawie wprowadzenia procedur ochrony danych osobowych związanych z wykonywaniem pracy zdalnej dla pracowników jednostki Oświaty Miejskiej w Otwocku.

Na podstawie art. 67 (26) § 1 i 2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z2025 r., poz. 277 z późn. zm.), zarządzam, co następuje:

§ 1

Wprowadzam procedury ochrony danych osobowych związanych z wykonywaniem pracy zdalnej dla pracowników jednostki Oświaty Miejskiej w Otwocku w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.

§ 2

Zobowiązuje się wszystkich pracowników Oświaty Miejskiej w Otwocku do zapoznania się z treścią procedur o których mowa w § 1 niniejszego zarządzenia oraz do pisemnego potwierdzenia zapoznania się z jego treścią.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

p. o. Dyrektora
Oświaty Miejskiej w Otwocku
Hanna Skrzypczak

Załącznik nr 1
Do Zarządzenia Nr 7 /2026
Dyrektora Oświaty Miejskiej
z dnia 16.06. 2026 r.

Praca Zdalna w Oświacie Miejskiej w Otwocku

Art. 1. Postanowienia ogólne dotyczące pracy zdalnej

1. Praca zdalna to taka praca, która może być wykonywana całkowicie lub częściowo w miejscu wskazanym przez Użytkownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania Użytkownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość.
2. Użytkownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych oraz są zobowiązani zapewnić bezpieczeństwo tych danych, przestrzegając zasad wynikających z Polityki Ochrony Danych Osobowych oraz innych procedur przyjętych w tym zakresie w Jednostce.
3. Użytkownicy w trakcie pracy zdalnej zobowiązani są dbać o należyte bezpieczeństwo danych osobowych w szczególności o ich dostępność, poufność oraz integralność.
4. Użytkownicy zobowiązani są do zgłaszania bezpośredniemu przełożonemu każdego potencjalnego incydentu lub zdarzenia, skutkującego wystąpieniem naruszenia ochrony danych osobowych zgodnie z procedurą stanowiącą załącznik nr 14 do Polityki ochrony danych osobowych, tak aby AD mógł się wywiązać z obowiązków nałożonych na niego na mocy art. 33 RODO.

Art. 2. Praca na dokumentacji papierowej i elektronicznej w ramach wykonywania pracy zdalnej

1. Użytkownicy nie powinni wynosić oryginalnej dokumentacji stanowiącej własność Jednostki w postaci papierowej poza określony przez AD obszar przetwarzania danych bez pisemnej zgody bezpośredniego przełożonego lub innego upoważnionego przedstawiciela AD.
2. Jeżeli AD dopuszcza przy pracy zdalnej możliwość korzystania przez Użytkowników z dokumentacji papierowej, w tym również kopii dokumentów, wówczas AD zobowiązany jest:
   a. ewidencjonować wydane Użytkownikom dokumenty na potrzeby pracy zdalnej,
   b. poinformować Użytkowników o obowiązku ograniczonego przechowywania wydanych im dokumentów jedynie przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (ograniczenie przechowywania),
   c. zobowiązać Użytkowników do wykorzystywania podczas pracy zdalnej pozyskanych dokumentów zawierających dane osobowe wyłącznie w takim celu, w jakim byłyby one wykorzystywane w siedzibie AD,
   d. ograniczyć liczbę dokumentów wynoszonych poza obszar przetwarzania danych do tego, co niezbędne w stosunku do celu, w jakim te dane osobowe są przetwarzane przez Użytkownika w ramach wykonywania pracy zdalnej,
   e. zobowiązać Użytkownika do odpowiedniego zabezpieczenia danych osobowych podczas wykonywania pracy zdalnej, w szczególności przed dostępem osób nieuprawnionych.
3. Użytkownik zobowiązany jest do zwrotu kopii dokumentów.
4. Zwrot dokumentów podlega odnotowaniu w ewidencji, o której mowa w pkt 2 lit. a.
5. Praca zdalna na dokumentach papierowych przez Użytkownika będzie nieuzasadniona jeżeli AD:

a. wdrożył elektroniczny obieg dokumentów lub posiada możliwość szybkiego, sprawnego i bezpiecznego wdrożenia elektronicznego obiegu dokumentacji w zakresie związanym z obowiązkami Użytkownika,

b. Użytkownik posiada bezpieczny szyfrowany dostęp do niezbędnych do pracy dokumentów, w tym danych osobowych, przy pomocy środków komunikacji elektronicznej,

c. udostępnił Użytkownikowi odpowiednio zabezpieczone (m.in. zaszyfrowane) elektroniczne kopie niezbędnych dokumentów.

Art. 3. Zasady bezpieczeństwa stosowane w ramach wykonywania pracy zdalnej

W ramach pracy zdalnej Użytkownicy mają obowiązek przestrzegać następujących zasad bezpiecznej pracy zdalnej:

1. prowadzenie rozmów i wideokonferencji służbowych powinno odbywać się w pomieszczeniach wewnętrznych bez dostępu osób nieupoważnionych przez AD do przekazywanych informacji (np. poprzez prowadzenie rozmów w odrębnym pokoju, a w przypadku wideokonferencji również w słuchawkach);
2. zakazane jest prowadzenie służbowych rozmów telefonicznych, w tym wideokonferencji, w miejscach narażonych na brak poufności informacji w szczególności np. na balkonach, tarasach czy innych otwartych przestrzeniach;
3. zakazane jest udostępnianie służbowych urządzeń osobom nieupoważnionym przez AD, w tym członkom rodziny Użytkownika;
4. zakazane jest niszczenie dokumentacji papierowej w miejscu pracy zdalnej – tego rodzaju czynności powinny odbywać się wyłącznie w siedzibie AD;
5. dokumentacja w formie papierowej oraz nośniki elektroniczne powinny być bezpiecznie przechowywane (np. szafa lub szuflada zamykana na klucz lub inne miejsca niedostępne dla pozostałych domowników Użytkownika);
6. zakazane jest udostępnianie osobom nieupoważnionym przez AD treści wyświetlanych na ekranie komputera, który jest wykorzystywany do pracy zdalnej – należy przestrzegać zasady „czystego ekranu", a także zadbać o odpowiednie ustawienie ekranu i/lub zastosowanie filtra prywatyzującego przekazanego przez AD,
7. przestrzeganie polityki „czystego biurka";
8. konta systemowe powinny być blokowane przed każdorazowym odejściem Użytkownika od stanowiska pracy;
9. wygaszacz ekranu powinien być uruchamiany automatycznie po upływie oznaczonego czasu w razie braku aktywności Użytkownika;
10. komputer służący do pracy zdalnej powinien być zabezpieczony przed dostępem osób nieupoważnionych przez AD z wykorzystaniem indywidualnego identyfikatora oraz hasła Użytkownika (podobne zasady obowiązują w zakresie telefonu wykorzystywanego do celów pracy zdalnej poprzez stosowanie PIN-u lub innej formy uwierzytelniania;
11. zakazane jest udostępnianie przez Użytkownika haseł osobom postronnym;
12. nośniki elektroniczne i urządzenia mobilne (w tym pendrive'y, karty pamięci, laptopy, telefony i tablety) powinny być szyfrowane;
13. dokumentacja i inne źródła danych osobowych nie mogą być wykorzystywane przez Użytkownika w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci publicznej, które nie zostały uprzednio autoryzowane przez AD;
14. zakazane jest utrwalanie danych na lokalnym dysku komputera – możliwość wykorzystania wyłącznie wskazanych przez AD zasobów sieciowych, z których wykonywane są regularnie kopie zapasowe;

15. stosowanie rozwiązań umożliwiających zdalne zarządzanie urządzeniami mobilnymi, w tym ich zdalne zlokalizowanie lub przywrócenie do stanu fabrycznego;
16. sprzęt informatyczny powinien zostać wyposażony w uruchomione oprogramowanie antywirusowe i zaporę sieciową;
17. użytkowana wersja systemu operacyjnego winna być wspierana przez producenta;
18. obowiązek aktualizowania systemu operacyjnego, z których korzysta Użytkownik, w tym systemu antywirusowego;
19. zakazane jest samodzielne pobieranie i instalacja oprogramowania bez wyraźnej zgody AD;
20. co do zasady zakazane jest korzystanie z uprawnień AD na komputerach służbowych wykorzystywanych do pracy zdalnej (chyba, że nie istnieje odmienna możliwość korzystania z urządzenia lub systemu teleinformatycznego);
21. zakazane jest naprawianie sprzętu informatycznego, na którym znajdują się dane osobowe AD z wykorzystaniem wsparcia podmiotów zewnętrznych bez uzyskania uprzedniej pisemnej zgody AD;
22. zakazane jest drukowanie dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów/osób trzecich;
23. użytkowanie sprzętu informatycznego powinno być zgodne z zasadami ostrożności z uwagi na konieczność uwzględnienia zagrożeń sieciowych typu phishing, na które sieć domowa może być bardziej podatna niż sieć AD.

Art. 4. Postanowienia końcowe

1. Obsługa informatyczna Jednostki lub inna osoba upoważniona przez AD prowadzi wykaz sprzętu (np. laptopy, smartfony) wydanego Użytkownikowi na potrzeby pracy zdalnej.
2. Obsługa informatyczna Jednostki zapewnia, aby sprzęt wydawany Użytkownikowi został wcześniej odpowiednio skonfigurowany, zabezpieczony przed ujawnieniem lub utratą danych, zgodnie z Instrukcją zarządzania systemami informatycznymi oraz innymi dokumentami dotyczącymi bezpieczeństwa sprzętu przyjętymi w Jednostce.
3. Obsługa informatyczna Jednostki przygotowuje dla Użytkowników pracujących zdalnie instrukcję dotyczącą instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych Użytkownikowi narzędzi pracy, w tym urządzeń technicznych.
4. Użytkownik jest zobowiązany stosować się do ustalonych przez AD zasad dotyczących instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych mu narzędzi pracy, w tym urządzeń technicznych.

Opracował:

Inspektor Ochrony Danych

Tomasz Szwed
Inspektor Ochrony Danych

/podpis/

ZATWIERDZIŁ:

DYREKTOR OŚWIATY MIEJSKIEJ W OTWOCKU

p. o. Dyrektora
Oświaty Miejskiej w Otwocku
Hanna Skrzypczak

/podpis/

Konsultacja:

Przedstawiciel pracowników:

Starszy specjalista
ds. administracyjno-kadrowych

mgr Izabela Gontarz