Załącznik Nr 5

do Zarządzenia Nr 21

Mazowieckiego Kuratora Oświaty

z dnia 08 maja 2024 r.

**PROCEDURA**

**ochrony danych osobowych pracy zdalnej
pracowników Kuratorium Oświaty w Warszawie**

**I. Wprowadzenie**

1. Niniejsza procedura określa zasady ochrony danych osobowych podczas pracy zdalnej i jest wprowadzana w związku z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27.04.2016 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 (Dz. Urz. UE L z 2016 r. Nr 119, s. 1 ze zm.) – dalej RODO oraz ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U.
z 2023 r. poz. 1465).
2. Procedura ma zastosowanie do pracy zdalnej wykonywanej całkowicie, częściowo oraz pracy zdalnej okazjonalnej.

**II. Warunki podjęcia pracy zdalnej**

1. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady ochrony danych osobowych podczas pracy zdalnej określone w niniejszej Procedurze.
2. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszą Procedurą, warunki techniczne oraz lokalowe, ochrony danych osobowych w miejscu wykonywania pracy zdalnej.
3. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub dostępu do Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie
z jego instrukcjami.

**III. Miejsce świadczenia pracy zdalnej**

1. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Pracownik wykonuje pracę zdalną pod adresem, który wskazał pracodawcy. 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 pod wskazanym adresem należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera.
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 należy upewnić się, że urządzenie zostało zablokowane.
6. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych jest realizowane w sposób zapewniający poufność informacji przekazywanych w trakcie spotkania/rozmowy.

**IV. Urządzenia służące do pracy zdalnej**

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy. Wyjątek może stanowić jedynie prywatny telefon pracownika i Internet.
2. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
3. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
4. Minimalne wymagania w zakresie bezpieczeństwa:
5. na urządzeniu są zainstalowane legalne i aktualne: system operacyjny
i oprogramowanie,
6. zostały włączone automatyczne aktualizacje,
7. została włączona zapora systemowa,
8. został zainstalowany i działa w tle program antywirusowy,
9. zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika,
10. wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,
11. został zainstalowany program umożliwiający tworzenie plików zabezpieczonych hasłem (np. 7-zip),
12. zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności,
13. jeżeli urządzenie daje taką możliwość, pracę należy wykonywać na koncie
z ograniczonymi uprawnieniami.

**Internet i sieć lokalna**

1. Niedozwolone jest wykonywanie pracy zdalnej w miejscach publicznych.
2. Niedozwolone jest wykonywanie pracy zdalnej z nieznanych, obcych lub otwartych sieciach.
3. 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 po uzgodnieniu z Pracodawcą limitu danych komórkowych do wykorzystania.
4. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, a w szczególności:
5. korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło,
6. hasło dostępu powinno składać się z co najmniej 12 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,
7. jeśli to możliwe, należy zmienić login i hasło do panelu administracyjnego routera na własne,
8. dostęp do panelu administracyjnego routera powinien być możliwy wyłącznie
z urządzeń znajdujących się w sieci lokalnej (domowej) lub dla serwisu dostawcy łącza internetowego.
9. Dostęp zdalny do informatycznych zasobów w sieci lokalnej Kuratorium Oświaty jest możliwy wyłącznie za pośrednictwem szyfrowanych połączeń VPN.

**V. Zabezpieczanie przechowywanych i przekazywanych informacji**

1. Dane osobowe w trakcie przechowywania na urządzeniu powinny być szyfrowane
z wykorzystaniem narzędzi do szyfrowania dysków.
2. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska, czy adresy e-mail.
3. Jeżeli niezbędne jest przesłanie informacji o charakterze poufnym, w szczególności zawierające dane osobowe, powinny zostać one zabezpieczone hasłem.
4. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
5. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
8. Rekomendowane metody zabezpieczania hasłem:
9. nadanie hasła do pliku, w którym są dane osobowe,
10. zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.
11. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą
w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
12. 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 kopi, tzn. adresy wpisać w to pole.
13. Pracownik może także przekazywać pliki z informacjami chronionymi
z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych.
14. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików.

**Zasady korzystania z dokumentów w formie papierowej**

1. Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.
2. Obowiązuje całkowity zakaz zabierania takich dokumentów lub ich kopii poza siedzibę pracodawcy oraz wykonywania ich wydruków w miejscu wykonywania pracy zdalnej.

**VI. Szczególne sytuacje**

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do pracowników odpowiedzialnych za techniczne utrzymanie
i konfigurację tego sprzętu.
2. W przypadku zagubienia lub kradzieży sprzętu, lub innych nośników informacji, należy niezwłocznie zgłosić takie zdarzenie do bezpośredniego przełożonego oraz do wydziału odpowiedzialnego za techniczne utrzymanie sprzętu i do Inspektora ochrony danych.

**VII. Działania niedozwolone**

Niedozwolone jest:

* udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
* przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
* przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
* korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę;
* odmówienie przeglądu urządzenia pracownikowi odpowiedzialnemu za techniczne utrzymanie sprzętu;
* udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
* dzielenie się informacjami zawierającymi dane osobowe z innymi osobami,
w szczególności domownikami;
* logowanie się na konto innego użytkownika.

………………………………………….. …………………….

 Imię i nazwisko pracownika Miejscowość, data

…………………………………………

 Wydział/delegatura/stanowisko

**OŚWIADCZENIE**

Oświadczam, że zapoznałem się z Procedurą ochrony danych osobowych pracy zdalnej pracowników Kuratorium Oświaty w Warszawie i zobowiązuję się do jej przestrzegania oraz przetwarzania danych osobowych zgodnie z zawartymi w niej zapisami.

…………………………………………

 Podpis pracownika