

## **REGULAMIN OCHRONY DANYCH OSOBOWYCH W PRACY ZDALNEJ**

### **I. Wprowadzenie**

1. Niniejszy regulamin określa zasady ochrony danych osobowych podczas pracy zdalnej i jest wprowadzany w związku z przepisami rozporządzenia PEiR (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. 119, s. 1 ze zm.) – dalej RODO oraz ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2022 r. poz. 1510 z późn. zm.).
2. W Regulaminie pod określeniem "pracownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stałe wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji. Pod określeniem "pracodawca" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi.
3. Pracodawca/administrator – należy przez to rozumieć pracodawcę/pracownika wykonującego pracę zdalną.

### **II. Warunki podjęcia pracy zdalnej**

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa pracodawca w odrębnym regulaminie i/lub porozumieniu z pracownikiem.
4. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady ochrony danych osobowych podczas pracy zdalnej określone w niniejszym Regulaminie.
5. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki techniczne oraz lokalowe, ochrony danych osobowych w miejscu wykonywania pracy zdalnej.
6. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie z jego instrukcjami.
7. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.
8. Pracodawca, przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie dla pracowników wykonujących pracę zdalną. W imieniu pracodawcy szkolenie w zakresie zasad ochrony danych osobowych w pracy zdalnej wykonuje Inspektor Ochrony Danych. Szkolenie może mieć postać materiału wideo udostępnionego pracownikowi przed przystąpieniem do wykonywania pracy zdalnej.

9. Pracownik po zapoznaniu się z niniejszym regulaminem oraz po szkoleniu przeprowadzonym przez Inspektora Ochrony Danych podpisuje oświadczenie o znajomości zasad pracy zdalnej i zobowiązanie do ich przestrzegania. Wzór oświadczenia stanowi **załącznik nr 4** do niniejszego regulaminu i jest przechowywany w aktach osobowych pracownika.
10. Pracownik wykonujący pracę zdalną, uzyskuje dostęp do danych osobowych, których przetwarzanie jest niezbędne do wykonywania obowiązków pracowniczych. Dostęp do danych osobowych możliwy jest po nadaniu pracownikowi upoważnienia do ich przetwarzania w trybie zdalnym i trwa do momentu ustania wykonywania pracy w trybie zdalnym – wzór upoważnienia stanowi **załącznik nr 1** do niniejszego regulaminu.

### 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 w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz smartfona, a także zabezpieczenie dokumentacji papierowej w trakcie wykonywania pracy i po jej zakończeniu.
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.
6. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych jest realizowane w sposób zapewniający poufność informacji przekazywanych w trakcie spotkania/ rozmowy.

### IV. Bezpieczeństwo pracy zdalnej

#### A. Internet

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy.
2. Jeżeli pracodawca udostępnia pracownikowi modem internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik korzysta z tych urządzeń do połączeń z Internetem. Korzystanie z domowej sieci internetowej odbywa się za zgodą i wiedzą pracodawcy.
3. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
  - 1) korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło,
  - 2) hasło dostępu powinno składać się z co najmniej 12 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,
  - 3) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny,
  - 4) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej,
  - 5) został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.

4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela pracownik Ośrodka Pomocy Społecznej w Międzychodzie, zatrudniony na stanowisku: koordynator d.s. komputeryzacji pomocy społecznej.

## **B. Urządzenia służące do pracy zdalnej**

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
2. Praca zdalna jest realizowana z wykorzystaniem służbowego sprzętu, jak komputer stacjonarny, laptop, smartfon, tablet, itp.
3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
4. Pracownik jest uprawniony także do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
5. Jeżeli z jakiś względów pracownik nie może wykonywać pracy zdalnej z wykorzystaniem służbowego sprzętu, zgłasza to pracodawcy, który może wydać zgodę na pracę z wykorzystaniem prywatnych urządzeń.
6. Urządzenie służbowe jest wydawane pracownikowi za protokołem, którego wzór stanowi załącznik nr 2 do niniejszego regulaminu. Protokół sporządza i przechowuje koordynator d.s. komputeryzacji pomocy społecznej.
7. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt koordynatorowi d.s. komputeryzacji pomocy społecznej.
8. Koordynator d.s. komputeryzacji pomocy społecznej odnotowuje, które urządzenia są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
9. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie koordynatora d.s. komputeryzacji pomocy społecznej udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez koordynatora narzędzia), w celu dokonania jego zdalnego przeglądu.
10. Przegląd urządzeń prywatnych, na których wykorzystanie pracodawca wyraził zgodę, jest obowiązkowy.
11. Minimalne wymagania w zakresie bezpieczeństwa:
  - 1) na urządzeniu jest legalne i aktualne oprogramowanie,
  - 2) zostały włączone automatyczne aktualizacje,
  - 3) została włączona zapor systemowa,
  - 4) został zainstalowany i działa w tle program antywirusowy,
  - 5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token,
  - 6) wyłączono autouzupętnianie i zapamiętywanie hasła w przeglądarce internetowej,
  - 7) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip),
  - 8) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności,
  - 9) jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami.

12. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:
- 1) zaszyfrowany dysk,
  - 2) wyłączone porty pamięci zewnętrznych,
  - 3) oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.

### **C. Zabezpieczanie przekazywanych informacji**

1. Do pracy zdalnej pracownik wykorzystuje tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, uprzednio należy je zabezpieczyć hasłem.
3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty elektronicznej e-mail, należy przesyłać je 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 i niesłownikowe.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą, o ile nie będzie wykorzystywane do zabezpieczania plików w komunikacji z innymi odbiorcami.
8. Rekomendowane metody zabezpieczania hasłem:
  - 1) nadanie hasła do pliku, w którym są dane osobowe,
  - 2) 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.

### **D. Zasady korzystania z dokumentów w formie papierowej**

1. Zgodnie z obowiązującymi 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 ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.
3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.

4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości elektronicznej e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
5. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
6. Po skopiowaniu dokumentów pracownik przygotowuje ich pisemne zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane. Wzór pisemnego zestawienia skopiowanych dokumentów stanowi **załącznik nr 3** do niniejszego regulaminu.
7. Informacja jest przekazywana pracodawcy i przechowywana na stanowisku bezpośredniego przełożonego.
8. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
9. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.).
10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność zgodnie z wcześniejszym pisemnym zestawieniem.
11. Pracownik zapewnia zabezpieczenie dokumentów w miejscu wykonywania pracy zdalnej, poprzez przechowywanie w szafie zamykanej na klucz, do której tylko on ma dostęp.

#### V. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać koordynatorowi d.s. komputeryzacji pomocy społecznej.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, koordynatora d.s. komputeryzacji pomocy społecznej, a także inspektora ochrony danych.
3. Szczegółowy sposób postępowania w przypadku zauważenia incydentu ochrony danych określa dokumentacja ochrony danych osobowych obowiązująca w zakładzie pracy.

#### VI. Działania niedozwolone

Niedozwolone jest:

- 1) udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług,
- 2) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail,
- 3) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki,
- 4) korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę,
- 5) odmówienie koordynatorowi d.s. komputeryzacji pomocy społecznej przeglądu urządzenia,
- 6) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom,
- 7) dzielenie się informacjami poufnymi z innymi osobami, w szczególności z domownikami,
- 8) samodzielne zniszczenie dokumentów w domu,

- 9) logowanie się na konto innego użytkownika,
- 10) zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy,
- 11) zabranie oryginałów dokumentów,
- 12) niezwrócenie dokumentów,
- 13) niepotwierdzenie z pracodawcą zakresu zwróconych danych.

## **VII. Procedura przeprowadzania kontroli przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych, w związku z pracą zdalną**

1. Każda osoba wykonująca pracę zdalną jest zobowiązana do zapewniania ochrony informacji przetwarzanych w związku z wykonywanymi zadaniami, w tym do przestrzegania procedur ochrony danych osobowych obowiązujących u pracodawcy oraz zasad zapewniania bezpieczeństwa i ochrony informacji podczas pracy zdalnej, które zostały określone w niniejszym regulaminie.
2. Pracodawca jest uprawniony do przeprowadzenia kontroli przestrzegania obowiązków, o których mowa w ust. 1, na zasadach określonych w regulaminie i/lub porozumieniu o pracę zdalną, z pracownikiem podlegającym kontroli (dalej: „Porozumienie”).
3. W powiadomieniu o przeprowadzeniu kontroli, pracodawca przekazuje informacje w zakresie:
  - 1) daty i godziny przeprowadzenia kontroli,
  - 2) sposobu przeprowadzenia kontroli,
  - 3) zakresu kontroli,
  - 4) osób uprawnionych do przeprowadzenia kontroli.
4. Kontrola odbywa się po uprzednim poinformowaniu pracownika, przy czym informacja musi zostać przekazana z wyprzedzeniem, zgodnie z terminem określonym w Porozumieniu.
5. Zakresem kontroli mogą być objęte:
  - 1) pomieszczenia, w których wykonywana jest praca zdalna,
  - 2) sposób zapewniania poufności w miejscu wykonywania pracy (środki techniczne oraz organizacyjne),
  - 3) sposób zabezpieczenia nośników danych,
  - 4) sposób postępowania ze zbędnymi danymi,
  - 5) stosowanie wewnętrznych procedur w zakresie blokowania ekranu, nieudostępniania urządzeń służbowych innym osobom, polityki czystego biurka, polityki czystego monitora,
  - 6) bezpieczeństwo sieciowe,
  - 7) wykorzystywane narzędzia pracy i środki komunikacji elektronicznej,
  - 8) znajomość procedur postępowania w przypadku naruszenia ochrony danych,
  - 9) zapisywanie danych elektronicznych w wyznaczonych przez pracodawcę lokalizacjach,
  - 10) szyfrowanie danych przekazywanych drogą elektroniczną w związku z wykonywaną pracą zdalną,
  - 11) inne obowiązki pracownika wynikające z obowiązujących zasad ochrony informacji.
6. Pracownik zapewnia, aby w momencie kontroli, w kontrolowanych pomieszczeniach, nie przebywały inne osoby.

7. Kontrola może zostać przeprowadzona w miejscu świadczenia pracy zdalnej, które wskazał pracownik w Porozumieniu lub poprzez elektroniczne środki porozumienia się na odległość.
8. Pracodawca dostosowuje sposób przeprowadzania kontroli do miejsca wykonywania pracy zdalnej i jej rodzaju.
9. Wykonywanie czynności kontrolnych nie może naruszać prywatności pracownika wykonującego pracę zdalną i innych osób, ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem.
10. Kontrola w miejscu wykonywania pracy jest realizowana przez uprawnionych pracowników i obejmuje:
  - 1) wstęp do pomieszczeń, w których wykonywana jest praca zdalna,
  - 2) weryfikację, czy przestrzegane są procedury ochrony danych osobowych obowiązujące u pracodawcy oraz zasady zapewniania bezpieczeństwa i ochrony informacji podczas pracy zdalnej, które zostały określone w niniejszym regulaminie,
  - 3) dokumentowanie fotograficzne stanu faktycznego, przy czym zdjęcia nie mogą obejmować osób fizycznych.
11. Kontrola poprzez elektroniczne środki porozumienia się na odległość, jest realizowana poprzez komunikator internetowy i obejmuje:
  - 1) zdalne połączenie przez wskazany przez pracodawcę komunikator, z obowiązkiem włączenia kamery,
  - 2) weryfikację, czy przestrzegane są procedury ochrony danych osobowych obowiązujące u pracodawcy oraz zasady zapewniania bezpieczeństwa i ochrony informacji podczas pracy zdalnej, które zostały określone w Regulaminie pracy zdalnej,
  - 3) dokumentowanie stanu faktycznego poprzez włączenie nagrywania lub wykonanie zrzutów ekranu.
12. Dokumentowanie stanu faktycznego jest uprawnieniem pracodawcy, z którego może, ale nie musi skorzystać.
13. Pracodawca może także dokonać kontroli na podstawie przekazanego przez pracownika nagrania lub zdjęć, z miejsca wykonywania pracy zdalnej.
14. Kontrola obejmuje wyłącznie pomieszczenia wskazane przez pracownika, jako służące do realizowania pracy zdalnej.
15. Z kontroli jest sporządzany raport.
16. W przypadku stwierdzenia uchybień w zapewnianiu ochrony informacji podczas pracy zdalnej, pracownik jest zobowiązany do ich usunięcia w terminie wskazanym przez pracodawcę.
17. W przypadku rażącego naruszenia zasad ochrony danych osobowych, pracodawca może cofnąć zgodę na wykonywanie pracy zdalnej przez pracownika.

#### **VIII. Klauzula informacyjna dla pracownika wykonującego pracę zdalną**

1. Administratorem Pani/Pana danych osobowych jest Ośrodek Pomocy Społecznej w Międzychodzie, reprezentowany przez Dyrektora, dalej: Administrator.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się za pośrednictwem adresu e-mail: [pukaczewski@hotmail.com](mailto:pukaczewski@hotmail.com).

3. Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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), zwanego dalej RODO, w związku z przepisami ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy i przepisami wykonawczymi w celu wypełnienia obowiązku administratora w zakresie realizacji praw i obowiązków pracodawcy wynikających z Kodeksu pracy, w tym w zakresie umożliwienia pracownikowi wykonywania pracy zdalnej, jej ewidencji i kontroli. W przypadku wykonywania pracy zdalnej na podstawie wniosku pracownika posiadającego orzeczenie o niepełnosprawności albo orzeczenie o znacznym stopniu niepełnosprawności albo pracownika sprawującego opiekę nad innym członkiem najbliższej rodziny lub inną osobą pozostającą we wspólnym gospodarstwie domowym posiadającym takie orzeczenie, dane osobowe będą przetwarzane na podstawie art. 9 ust. 2 lit. b) RODO.
4. Podane przez Panią/Pana dane osobowe będą udostępniane wyłącznie podmiotom uprawnionym do ich przetwarzania na podstawie przepisów prawa. Dane osobowe będą udostępnione podmiotom zapewniającym, na podstawie umów zawartych przez administratora, obsługę działalności administratora (np. dostawcy usług informatycznych, poczty elektronicznej, systemów kadrowych, systemów monitorowania i ewidencji czasu pracy).
5. Dane osobowe będą przechowywane przez czas trwania stosunku pracy (np. w zakresie związanym z komunikacją służbową) albo przez czas trwania stosunku pracy i niezbędnej archiwizacji (w odniesieniu do danych osobowych niezbędnych do wypełnienia obowiązków pracodawcy, ewidencji czasu pracy zdalnej, kontroli pracy zdalnej).
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia w przypadkach przewidzianych przepisami prawa oraz ograniczenia przetwarzania.
7. Posiada Pani/Pan prawo wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych, jeżeli uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
8. Podanie danych osobowych jest dobrowolne, ale niezbędne do weryfikacji gotowości do świadczenia pracy zdalnej, wniosku o świadczenie pracy zdalnej a następnie zawarcia umowy dotyczącej wykonywania pracy zdalnej. Niepodanie danych osobowych oznacza brak możliwości zawarcia i wykonywania umowy.
9. Dane osobowe nie będą podlegały profilowaniu ani, na podstawie tych danych, nie będą podejmowane decyzje w sposób zautomatyzowany.



Międzychód, ..... r.

**UPOWAŻNIENIE**  
do przetwarzania danych osobowych

**I.**

Na podstawie art. 29 RODO z dniem ..... roku upoważniam Panią/Pana:

.....  
(imię i nazwisko wnioskującego)

zatrudnioną/zatrudnionego w: **Ośrodku Pomocy Społecznej w Międzychodzie**,  
(nazwa jednostki)

**do przetwarzania danych osobowych w sposób zdalny, tj. poza siedzibą administratora, w celach związanych z wykonywaniem obowiązków na stanowisku:**

.....  
(zajmowane stanowisko)

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych zgodnie z kategorią danych i formą ich przetwarzania określoną w odrębnym upoważnieniu do przetwarzania danych.

**II.**

Upoważnienie wygasa z chwilą pisemnego cofnięcia upoważnienia przez administratora.

.....  
Data i podpis Administratora

---

COFNIĘCIE UPOWAŻNIENIE  
do przetwarzania danych osobowych

I.

Na podstawie art. 29 RODO z dniem ..... roku cofam powyżej wydane upoważnienie **do przetwarzania danych osobowych w sposób zdalny, tj. poza siedzibą administratora.**

.....  
Data i podpis Administratora

**Potwierdzam odbiór upoważnienia**

.....

**PROTOKÓŁ ZDAWCZO – ODBIORCZY DOTYCZĄCY POWIERZENIA SPRZĘTU**

Sporządzony w dniu ..... w ..... pomiędzy:  
powierzającym sprzęt: .....

(specjalista d.s. komputeryzacji pomocy społecznej/inny upoważniony pracownik),

a

Użytkownikiem: .....

**§ 1**

**POWIERZENIE SPRZĘTU**

Użytkownik potwierdza, że otrzymał(a) do wyłącznego korzystania w celach służbowych:

1. Zestaw komputerowy składający się z następujących elementów:

- a) .....
- b) .....
- c) .....

liczba elementów w zestawie:.....  
*(słownie)*

parametry definiujące komputer i inny sprzęt - numery:

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

Na powyższym komputerze zainstalowane zostało następujące oprogramowanie (nazwa i numer seryjny lub numer licencji):

- a) .....
- b) .....
- c) .....
- d) .....
- e) .....

2. Telefon służbowy:

- a) model .....
- b) nr telefonu .....
- c) nr inwentarzowy .....

3. Dysk zewnętrzny:

a) model .....

b) nr inwentarzowy .....

.....  
Data i podpis powierzającego sprzęt

.....  
Data i podpis Użytkownika

---

**§ 2**  
**ZWROT POWIERZONEGO SPRZĘTU**

Użytkownik potwierdza, że zwraca powierzony sprzęt, a koordynator d.s. komputeryzacji pomocy społecznej/inny upoważniony pracownik, potwierdza odbiór powierzonego sprzętu bez uwag/z poniższymi uwagami\*

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

.....  
Data i podpis powierzającego sprzęt

.....  
Data i podpis Użytkownika

\*skreślić niepotrzebne

### ZESTAWIENIE SKOPIOWANYCH DOKUMENTÓW

Sporządzone w dniu ..... W .....  
pomiędzy:

Udostępniającym kopię: .....  
(pracodawca/bezpośredni przełożony)

a

Użytkownikiem kopii: .....

#### § 1

#### UDOSTĘPNIENIE KOPII

Użytkownik potwierdza, że wykonał kopie poniższych dokumentów do pracy poza siedzibą pracodawcy:

Lp.	Nazwa dokumentu	Ilość stron dokumentu	Ilość kopii

.....  
Data i podpis powierzającego dokumenty

.....  
Data i podpis Użytkownika



**§ 2**  
**ZWROT UDOSTĘPNIONYCH KOPII**

Użytkownik potwierdza, że zwraca udostępnione kopie, a przedstawiciel Pracodawcy potwierdza odbiór kopii bez uwag / z poniższymi uwagami\*

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

.....  
Data i podpis powierzającego dokumenty

.....  
Data i podpis Użytkownika

\*skreślić niepotrzebne

.....  
imię i nazwisko pracownika

**OŚWIADCZENIE**  
pracownika o zapoznaniu się z procedurą ochrony danych osobowych

Oświadczam, że zapoznano mnie z Regulaminem ochrony danych osobowych w pracy zdalnej, stanowiącego załącznik do Zarządzenia Nr 20/2023 z dnia 12.06.2023 r. Dyrektora Ośrodka Pomocy Społecznej w Międzychodzie w sprawie: wprowadzenia Regulaminu ochrony danych osobowych w pracy zdalnej w Ośrodku Pomocy Społecznej w Międzychodzie i zobowiązuję się do jej przestrzegania.

.....  
data, miejsce i podpis pracownika