

ZARZĄDZENIE NR 16/2020

z dnia 13.03.2020 r.

w zapobieganiu rozprzestrzenianiu się wirusa SARS–COV-2 wśród pracowników Starostwa Powiatowego w Środzie Śląskiej

Na podstawie art. 3 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. z 2020 r., poz. 374), zarządzam co następuje:

§ 1

Niniejsze Zarządzenie określa zasady pracy pracowników Starostwa Powiatowego w Środzie Śląskiej (zwanym dalej Jednostką) świadczonej poza miejscem jej stałego wykonywania ("praca zdalna").

§ 2

1. Zaleca się ograniczenie do minimum bezpośrednich kontaktów pracowników Starostwa Powiatowego w Środzie Śląskiej w miejscu pracy.
2. W celu zapewnienia sprawnej komunikacji zaleca się wykorzystywanie poczty elektronicznej i kontaktów telefonicznych.

§ 3

Czas trwania pracy wykonywanej zdalnie następuje do odwołania stanu zagrożenia epidemicznego lub epidemii.

§ 4

O sposobie i rodzaju wykonywanych obowiązków w tym trybie pracy zdalnej i sposobie jej rozliczenia decyduje Kierownik Jednostki.

§ 5

1. Niniejsze Zarządzenie stanowi udokumentowane polecenie do przetwarzania danych osobowych w zakresie niezbędnym do należytego wykonywania obowiązków w ramach pracy zdalnej.
2. Pracownicy Jednostki są uprawnieni i zobowiązani do przetwarzania danych osobowych na potrzeby należytego wykonywania obowiązków w ramach pracy zdalnej.
3. Pracownicy Jednostki są zobowiązani do należytego zabezpieczenia danych osobowych, które przetwarzają w związku z wykonywaniem obowiązków w ramach pracy zdalnej oraz uniemożliwić dostęp do tych danych osobom nieuprawnionym (m.in. domownikom).
4. Pracownicy Jednostki są zobowiązani do ewidencjonowania pobierania (wypożyczania) oraz zdawania wszelkich dokumentów, urządzeń, nośników w tym zawierających dane osobowe, które będą przetwarzane poza siedzibą Administratora Danych Osobowych. Ewidencje w postaci protokołów zdawczo-odbiorczych prowadzi Kierownik Jednostki/ osoba upoważniona.

§ 6

1. Decyzje w zakresie nieuregulowanym niniejszym zarządzeniem podejmuje Kierownik Jednostki.
2. Zarządzenie wchodzi w życie z dniem podpisania i obowiązuje do odwołania, w zależności od rozwoju sytuacji epidemiologicznej i decyzji Rządu RP.

STAROSTA

Krzysztof Szalankiewicz

.....
Podpis osoby zarządzającej

PROTOKÓŁ WYDANIA DOKUMENTÓW LUB URZĄDZEŃ



Odbierający (imię i nazwisko, stanowisko):

.....

Dokumenty podlegające zwrotowi:

1. od do
2. od do
3. od do
4. od do
5. od do
6. Inne dokumenty:

.....

Urządzenia podlegające zwrotowi

1. Komputer stacjonarny
2. Laptop.....
3. Drukarki.....

Odbiorca zobowiązuje się w terminie do lub na polecenie służbowe do zwrotu wydanych dokumentów i urządzeń.

Dokumenty/urządzenia* odebrano dnia:

.....

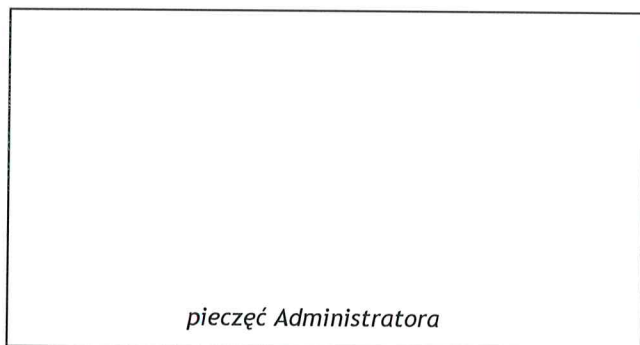
podpis Odbierającego

.....

podpis Wydającego

**niepotrzebne skreślić*

PROTOKÓŁ ODBIORU DOKUMENTÓW LUB URZĄDZEŃ



Odbierający (imię i nazwisko, stanowisko):

.....

Dokumenty podlegające zwrotowi:

1. od do
2. od do
3. od do
4. od do
5. od do

Urządzenia podlegające zwrotowi

1. Komputer stacjonarny
2. Laptop.....
3. Drukarka

Dokumenty/urządzenia* zdano dnia:

Uwagi

.....

.....
podpis Zdającego

.....
podpis Odbierającego

**niepotrzebne skreślić*

Oświadczenie pracownika w związku z podjęciem pracy zdalnej (home office)

Ja

(imię i nazwisko pracownika)

pracujący/a na umowę o pracę/umowę cywilnoprawną w

STAROSTWIE POWIATOWYM W ŚRODZIE ŚLĄSKIEJ
(nazwa i miejsce pracy)

oświadczam, że:

1. Jestem upoważniony/a przez Pracodawcę (Administradora Danych Osobowych) do przetwarzania danych osobowych oraz zobligowany do zachowania tajemnicy.
2. Zapoznałem się z Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym/ lub Instrukcją Informatyczną/ lub Regulaminem Użytkowania Systemów Teleinformatycznych u Pracodawcy.
3. Nie dopuszczę do komputera, telefonu, dokumentów papierowych i innych nośników przekazanych mi przez Pracodawcę oraz informacji w nich zawartych, w tym danych osobowych, domowników oraz innych osób trzecich.
4. Zachowam dane Pracodawcy w poufności. Wszelkie notatki będę przechowywał/a zabezpieczone, tak by osoby trzecie nie miały do nich dostępu.
5. Zapiszę wszystkie dane na komputerze w katalogu wskazanym przez Pracodawcę lub na odpowiednio zabezpieczonym nośniku zewnętrznym udostępnionym przez Pracodawcę.
6. Nie będę kopiować/zapisywać danych służbowych na niezabezpieczone/ prywatne dyski zewnętrzne i inne nośniki zewnętrzne.
7. Mam świadomość, że dokumenty papierowe, komputer, telefon i inne nośniki przekazane mi przez Pracodawcę służą wyłącznie do pracy służbowej – nie zainstaluję dodatkowego oprogramowania bez nadzoru działu IT, nie będę korzystać ze służbowego sprzętu w innych celach niż te związane z pracą.
8. Komputer, dokumenty papierowe oraz inne nośniki udostępnione przez Pracodawcę zabezpieczę w odpowiedni sposób przed dostępem osób nieupoważnionych, zgodnie z przekazanymi mi w tym zakresie wytycznymi.
9. Będę przestrzegać zasad korzystania z komputera, telefonu i innych nośników przekazanych mi przez Pracodawcę zgodnie z obowiązującymi w tym zakresie procedurami, w tym w szczególności zgodnie z wytycznymi i regulaminami.
10. Zobowiązuję się zwrócić powierzone mi dokumenty, urządzenia oraz nośniki wraz z kompletnymi danymi na każde żądanie Pracodawcy.

.....
(miejsce i data)

.....
(podpis pracownika)

KLAUZULA INFORMACYJNA
dot. ograniczania możliwości rozprzestrzeniania się wirusów
w tym koronawirusa SARS-Cov-2 wywołującego chorobę
o nazwie COVID-19, innych chorób zakaźnych
W

Treść informacji:

Zgodnie z art. 13 ust. 1 i 2 RODO informujemy, że:

1.	Administratorem Danych Osobowych jest STAROSTWO POWIATOWE W ŚRODZIE ŚLĄSKIEJ, UL. WROCŁAWSKA 2, 55-300 ŚRODA ŚLĄSKA;
2.	Kontakt z Inspektorem Ochrony Danych możliwy jest na adres email: rodo.hr.consulting@gmail.com ;
3.	Dane osobowe będą przetwarzane wyłącznie w celu przeciwdziałania, zwalczania, a w szczególności zapobieganiu rozprzestrzeniania się wirusa COVID-19 oraz innych chorób zakaźnych na podstawie art. 6 ust. 1 lit. d RODO;
4.	Dane będą przechowywane przez okres niezbędny do konkretnego przetwarzania danych, wynikający z przepisów prawa;
5.	Dane mogą być przekazane służbom Głównego Inspektoratu Sanitarnego lub innym służbom kryzysowym. Pracodawca może pozyskiwać dodatkowe dane osobowe (np. informacje o miejscu przebywania podczas urlopu lub w związku z pomiarem temperatury);
6.	Podanie danych osobowych umożliwiających Pani/Pana identyfikację jest obowiązkiem wynikającym z przepisu prawa; jeśli administrator tych danych nie będzie posiadał, nie będzie możliwe zrealizowanie celu przetwarzania;
7.	Przysługuje Pani/Panu: 1. prawo dostępu do swoich danych; 2. prawo do sprostowania (poprawiania) swoich danych; 3. prawo do ograniczenia przetwarzania;
8.	Przysługuje Pani/Panu prawo do wniesienia skargi do Prezesa UODO (na adres: Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa);
9.	Dane osobowe przeze mnie udostępnione nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym decyzji będących wynikiem profilowania;

INFORMACJE DLA PRACOWNIKÓW, KTÓRYM ZLECONO PRACĘ ZDALNĄ

W związku z zleceniem pracy zdalnej należy pamiętać, że należy wdrożyć wszystkie możliwe środki, w celu zabezpieczenia powierzonych dokumentów, sprzętu i zawartych na nich danych osobowych. A przede wszystkim:

- Przestrzegaj zakazu prowadzenia rozmów w miejscach, które nie gwarantują zachowania poufności,
 - Stosuj zabezpieczenia wdrożone przez Twojego pracodawcę jak: używanie aktualizowane oprogramowania, blokowanie komputera, zabezpieczenia dokumentów papierowych, łącznie się z siecią firmy przy wykorzystaniu szyfrowanego połączenia VPN z zasobami firmowymi,
 - Nie drukuj dokumentów firmowych w ogólnodostępnych punktach ksero
 - Nie wrzucaj dokumentów firmowych do śmietnika – przechowuj je do momentu bezpiecznego zniszczenia
 - Nie udostępniaj dokumentów papierowych oraz urządzenia, na którym pracujesz, domownikom, współlokatorom lub innym osobom postronnym
 - Korzystaj tylko z domowej sieci bezprzewodowej lub z sieci przez Ciebie udostępnionych (hotspot z Twojego urządzenia mobilnego)
 - Nie dziel się informacjami służbowymi z na portalach społecznościowych
 - Pilnuj urządzenia oraz dokumentów papierowych, na których pracujesz, ponieważ mogą ulec zniszczeniu lub zostaną zgubione, a ważne informacje związane z Twoją pracą mogą zostać ujawnione nieuprawnionym osobom
 - Niedozwolone jest wysyłanie dokumentów oraz danych na prywatne skrzynki, jak i podawania klientom czy kontrahentom prywatnych adresów w celu wymiany korespondencji
 - Pamiętaj o zachowaniu zasady nie otwierania podejrzanej korespondencji mailowej, szczególnie jeżeli korespondencja zawiera pliki z rozszerzeniem .exe, korespondencji od firm finansowych, zawierającej faktury, korespondencji zawierającej w swej treści link, jeśli adresat, treść lub załączniki budzą twoje wątpliwości, nie otwieraj ich
-

**ZADANIA DO WYKONANIA W CELU ORGANIZACJI PRACY ZDALNEJ (home office)
dla ADMINISTRATORA DANYCH OSOBOWYCH**

w związku z wejściem w życie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych

/administracja, dział HR, kadry/

1. Przekaż informacje dla pracowników o pracy zdalnej.
2. Wydał pracownikom wzór oświadczenia dla pracownika o sprawowaniu opieki nad dzieckiem w wieku do 8 lat w związku z zamknięciem – z powodu COVID-19 – żłobków, klubów dziecięcych, przedszkoli oraz szkół.
3. Przygotuj klauzulę informacyjną w art. 13 RODO.
4. Zbierz od pracowników oświadczenia w związku z podjęciem pracy zdalnej.
5. Unikaj wynoszenia dokumentów papierowych poza Twoją organizację. W dzisiejszych czasach w większości przypadków można pracować na skanach, zdjęciach czy gotowych bazach danych. Jeśli nie będzie innej możliwości, zadbaj o to, żeby uniemożliwić dostęp do dokumentów osobom nieupoważnionym (w tym domownikom!)

/dział informatyczny, sektor IT/

1. Przyjmij i zakomunikuj pracownikom obowiązujące w Twojej firmie procedury odnoszące się do pracy zdalnej.
2. Wydadz zarządzenie dotyczące legalizacji pracy zdalnej w tym przetwarzania danych poza siedzibą Administratora w związku z przeciwdziałaniem zagrożeniu koronawirusem.
3. Wydadz pracownikom sprzęt, na którym mają pracować (m.in. laptopy, telefony komórkowe), pamiętając w szczególności o:
 - 1) zaszyfrowaniu dysków, kart pamięci lub innych elektronicznych nośników informacji,
 - 2) przyznaniu pracownikom adekwatnych do ich roli w organizacji praw dostępu (domyślnie jako użytkownicy),
 - 3) potwierdzeniu, że został zainstalowany system antywirusowy,
 - 4) włączeniu wszystkich funkcji bezpieczeństwa (np. hasła, automatyczne blokady ekranu, zdalne usuwanie zawartości sprzętu),
 - 5) włączeniu wszystkich automatycznych aktualizacji dla systemu operacyjnego, aplikacji oraz systemu antywirusowego.
4. Przekaż pracownikom informacje, w jaki sposób mogą kontaktować się z Tobą w przypadku problemów technicznych (podaj adres e-mail lub/i numer telefonu).
5. Poproś pracowników, aby zobowiązali się do korzystania z Internetu służbowego (np. hotspot WiFi z telefonu służbowego), a jeżeli nie jest to możliwe poproś ich o