

REGULAMIN PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH W PRACY ZDALNEJ w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi

§ 1

Pracodawca określając zasady ochrony danych osobowych w ramach pracy zdalnej, kieruje się wytycznymi art. 32 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 (dalej: RODO), który nakazuje wdrożenie odpowiednich środków technicznych i do ryzyka związanego z przetwarzaniem danych, które mają gwarantować odpowiedni poziom bezpieczeństwa przetwarzania danych, oraz wymogiem § 20 ust. 2 pkt 8 Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów Teleinformatycznych wskazującym na obowiązek ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

§ 2

Biorąc pod uwagę specyfikę pracy zdalnej oraz ograniczone możliwości wpływania na warunki organizacyjno – techniczne tego miejsca, Pracodawca przed wydaniem polecenia pracy zdalnej odbiera od Pracownika oświadczenie potwierdzające przygotowanie miejsca wykonywania pracy zdalnej w sposób gwarantujący odpowiednie zabezpieczenie danych osobowych (**Załącznik Nr 1**).

§ 3

Pracownik wykonuje pracę zdalną wyłącznie z wykorzystaniem powierzonego przez pracodawcę sprzętu służbowego. Przekazanie sprzętu następuje w formie protokołu udostępnienia sprzętu informatycznego na czas wykonywania pracy zdalnej wraz z oświadczeniem pracownika.

Wzór dokumentu stanowi (**Załącznik Nr 2**).

§ 4

Pracodawca w sytuacjach wyjątkowych, podyktowanych brakiem możliwości zabezpieczenia na potrzeby pracy zdalnej sprzętu informatycznego/mobilnego, może na wniosek pracownika wyrazić zgodę na wykorzystanie do pracy zdalnej sprzętu prywatnego.

Wzór wniosku stanowi (**Załącznik Nr 3**).

§ 5

Pracownik w związku z wykonywaniem pracy zdalnej, zobowiązany jest do przestrzegania polityk, zasad i procedur ochrony danych osobowych obowiązujących u Pracodawcy.

§ 6

Pracownik wykonując prace zdalnie otrzymuje dostęp do danych osobowych w zakresie niezbędnym do realizacji powierzonych mu obowiązków służbowych. Dostęp do danych osobowych możliwy jest po nadaniu pracownikowi upoważnienia do ich przetwarzania i trwa do momentu ustania wykonywania przez pracownika pracy zdalnej, lub do momentu cofnięcia upoważnienia przez Pracodawcę.

Wzór upoważnienia stanowi (**Załącznik Nr 4**).

Część integralną upoważnienia stanowi zbiór wytycznych i zasad dotyczących bezpiecznego przetwarzania danych w pracy zdalnej, które to wytyczne Pracownik zobowiązuje się przestrzegać potwierdzając ten fakt stosownym oświadczeniem.

§ 7

Nie jest dopuszczalne wykorzystywanie danych osobowych przetwarzanych w ramach pracy zdalnej w innym celu niż wykonywanie obowiązków pracowniczych.

§ 8

Podstawową formą dostępu do danych w związku z wykonywaniem pracy zdalnej, jest forma elektroniczna. Dostęp do danych osobowych przetwarzanych elektronicznie odbywa się w sposób zdalny i następuje poprzez:

- 1) dostęp do skrzynki pocztowej pracownika w domenie pracodawcy,
- 2) udostępnienie pracownikowi elektronicznych kopii dokumentów na zaszyfowanym nośniku służbowym (np. pendrive),
- 3) komunikacja za pomocą komunikatora internetowego Teams.

§ 9

Komunikacja służbowa odbywa się w sposób zapewniający bezpieczeństwo informacji i danych osobowych, wyłącznie poprzez wskazane przez pracodawcę narzędzia i połączenia zdalne. Przenoszenie służbowych danych na inne urządzenia niż wskazane przez Pracodawcę, w tym prywatne komputery i urządzenia mobilne, bez zgody Pracodawcy jest zabronione.

§ 10

Pracownik zobowiązany jest do zachowania w tajemnicy otrzymanych od pracodawcy danych dostępowych, w tym loginu i hasła oraz zabezpiecza je przed dostępem osób nieuprawnionych, w tym domowników. Zasady dotyczące zmiany hasła, jego budowy i przechowywania określają wewnętrzne procedury obowiązujące u Pracodawcy.

§ 11

Pracownik korzystając z przydzielonego mu dostępu do danych przetwarzanych elektronicznie jest zobowiązany do pracy w ramach przydzielonego mu konta w systemie informatycznym. Nie jest dopuszczalne udostępnianie konta, loginu, hasła osobom nieuprawnionym, w tym innym pracownikom lub domownikom, ani też korzystanie z konta, loginu, hasła innego pracownika.

§ 12

Pracownik nie powinien przysyłać plików z danymi osobowymi za pomocą poczty elektronicznej w celu pracy z danymi osobowymi), tj. na potrzeby wykonywania pracy zdalnej, jeżeli możliwy jest dostęp do danych w systemie informatycznym lub za pomocą połączenia zdalnego VPN.

§ 13

Jeżeli pracownik przesyła załączniki zawierające dane osobowe w wiadomościach mailowych, muszą być one zaszyfrowane odpowiednim programem (np. Zip).

Hasło do odszyfrowania załącznika nie może być przesyłane do adresata w treści tej samej wiadomości. Pracownik przekazuje hasło wykorzystując inną formę komunikacji tj. telefonicznie, SMS-em.

Instrukcja szyfrowania załączników do wiadomości mailowych za pomocą programu 7-ZIP, szyfrowania nośników danych za pomocą narzędzia BitLocker, oraz korzystania z przeglądarki internetowej w formie incognito (tryb prywatny) stanowi (**Załącznik Nr 6**).

§ 14

Pracodawca jedynie w uzasadnionych przypadkach podyktowanych okolicznościami uniemożliwiającymi dostęp do danych w wersji elektronicznej, wyraża zgodę pracownikowi na wynoszenie dokumentów papierowych.

Aby zminimalizować ryzyko utraty, zniszczenia lub naruszenia integralności dokumentów, pracownik w pierwszej kolejności otrzymuje kopie tych dokumentów.

Wynoszenie przez pracownika kopii dokumentów nie zwalnia go od stosowania tych samych reguł i procedur bezpieczeństwa, co w odniesieniu do dokumentacji oryginalnej.

§ 15

Pracodawca w sytuacji, w której dokumenty wynoszone będą w oryginale, może wprowadzić obowiązek ewidencjonowania wydanych pracownikowi dokumentów zawierających dane osobowe, w celu kontroli poprawności zwrotu wyniesionej dokumentacji.

Pracownik zobowiązany jest do niezwłocznego zwrotu dokumentów po wykonaniu pracy, do której te dokumenty były mu niezbędne.

§ 16

W przypadku wystąpienia incydentu mogącego naruszyć bezpieczeństwo danych osobowych oraz spowodować ryzyko naruszenia poufności, integralności lub dostępności danych, pracownik zobowiązany jest niezwłocznie, najpóźniej do godziny od ustalenia incydentu zawiadomić o tym fakcie Pracodawcę lub Inspektora Ochrony Danych.

§ 17

Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. Pracownik niezwłocznie zgłasza Pracodawcy lub wyznaczonej przez Pracodawcę osobie realizującej wsparcie techniczne, wszelkie uzasadnione potrzeby w tym zakresie.

W przypadku sprzętu informatycznego/mobilnego zgłoszenie należy przesłać do służb IT.

§ 18

Pracodawca realizuje wobec pracownika obowiązek informacyjny z art. 13 RODO, informując go o zasadach przetwarzania danych w związku z poleceniem pracy zdalnej, przy pierwszej czynności związanej z decyzją o przejściu pracownika na tryb pracy zdalnej.

§ 19

Nieprzestrzeganie zasad ochrony danych może być kwalifikowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

§ 20

Przed przystąpieniem do wykonywania pracy zdalnej Pracownik zapoznaje z treścią niniejszego Regulaminu, co potwierdza pisemnym lub elektronicznym oświadczeniem i zobowiązaniem do jego przestrzegania. Wzór oświadczenia stanowi (**Załącznik Nr 5**) do niniejszego Regulaminu.

§ 21

W przypadku wykonywania przez pracownika pracy zdalnej z wykorzystaniem sprzętu prywatnego obowiązuje (**Załącznik Nr 7**) do niniejszego Regulaminu.

§ 22

W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie mają wewnętrzne procedury obowiązujące u Pracodawcy oraz przepisy z zakresu ochrony danych osobowych oraz z zakresu prawa pracy.

Oświadczenie pracownika

Oświadczam, że dysponuję warunkami organizacyjno-technicznymi umożliwiającymi mi prawidłowe zabezpieczenie danych osobowych w miejscu wskazanym do wykonywania pracy zdalnej. Znam i będę stosował(a) zalecenia przetwarzania i ochrony danych osobowych w pracy zdalnej obowiązujące u Pracodawcy, w tym wytyczne i procedury zawarte w Regulaminie przetwarzania i ochrony danych osobowych w pracy zdalnej w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi. Jednocześnie informuję, iż otrzymałam(em) do stosowania instrukcję szyfrowania załączników, szyfrowania nośników danych za pomocą narzędzia BitLocker, oraz korzystania z przeglądarki internetowej w formie incognito (tryb prywatny) - Instrukcja Administratora Danych i zobowiązuję się do przestrzegania zasad tam zawartych.

.....
(Data i podpis pracownika)

Protokół
udostępnienia sprzętu elektronicznego do celów służbowych

Z dniemudostępniam Pani/Panu

zatrudnionemu na stanowisku

niżej wymieniony sprzęt elektroniczny:

LP	Typ sprzętu	Model	Numer seryjny
1	np. Smartfon		
2	Laptop		

Uwagi: Wyżej wymieniony sprzęt w dniu przekazania był nowy i w pełni sprawny

Pracodawca zobowiązuje się dostarczyć wszelkich niezbędnych materiałów eksploatacyjnych dla danego sprzętu, niezbędnych do wykonania, przez pracownika, czynności służbowych.

(podpis pracodawcy / osoby wydającej
sprzęt, upoważnionej przez pracodawcę)

(data i podpis pracownika)

**Oświadczenie pracownika o odpowiedzialności za używanie służbowego sprzętu
informatycznego / mobilnego w celu wykonywania pracy zdalnej**

1. Pracownik, zwany dalej również Użytkownikiem, oświadcza, że otrzymał sprawny technicznie sprzęt informatyczny/mobilny zgodnie z protokołem przekazania.
2. Komputer posiada zainstalowane oprogramowanie niezbędne do wykonywania czynności

- służbowych oraz został zabezpieczony przed nieautoryzowanym uruchomieniem (wprowadzony został proces uwierzytelniania dostępu do zasobów komputera).
3. Pracownik zobowiązuje się w okresie obowiązywania polecenia wykonywania pracy zdalnej - używać powierzony sprzęt komputerowy sprzęt mobilny wyłącznie do celów służbowych związanych z wykonywaniem pracy zdalnej, zgodnie z procedurami i regulaminami dotyczącymi zasad użytkowania sprzętu informatycznego wdrożonymi do stosowania u pracodawcy.
 4. Pracodawca udostępnia komputer przenośny / sprzęt mobilny w celu umożliwienia wykonywania pracy zdalnej w miejscu wskazanym przez pracownika, przy zachowaniu przez pracownika szczególnej staranności podczas użytkowania i przenoszenia komputera/sprzętu mobilnego. Za bezpieczeństwo komputera/sprzętu mobilnego odpowiada pracownik.
 5. Pracownik zobowiązuje się niezwłocznie powiadomić pracodawcę w formie pisemnej lub elektronicznej o:
 - a) zaistnieniu zmiany stanu technicznego komputera/sprzętu mobilnego, uniemożliwiającego jego poprawną eksploatację,
 - b) kradzieży lub zaginięcia komputera/urządzenia mobilnego,
 - c) zaistnieniu innych niż wymienione w punktach a) i b) okoliczności, uniemożliwiających używanie sprzętu do celów służbowych,
 - d) incydencie mogącym naruszyć ochronę przetwarzanych danych osobowych, w tym wystąpienia ryzyka naruszenia poufności, integralności lub dostępności danych.
 6. Samowolne otwieranie (demontaż) komputera, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych części/elementów jest zabronione.
 7. Pracownik zobowiązuje się do korzystania wyłącznie z oprogramowania już zainstalowanego, udostępnionego przez pracodawcę.
 8. Pracownik nie ma prawa kopiować oprogramowania zainstalowanego na komputerze/urządzeniach mobilnych na swoje własne potrzeby ani na potrzeby osób trzecich.
 9. Instalowanie jakiegokolwiek oprogramowania na komputerze/ urządzeniu mobilnym może być dokonane wyłącznie przez osobę upoważnioną.
 10. Pracownik ma prawo zapisywania dokumentów elektronicznych wyłącznie na dysku udostępnionego komputera służbowego oraz na dysku komputera w zakładzie pracy udostępnionego zdalnie za pomocą łącza VPN.
 11. Pracownik nie ma prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną, odpowiedzialną za konfigurację systemu operacyjnego.
 12. W przypadku naruszenia któregoś z powyższych postanowień osoba upoważniona przez pracodawcę ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.
 13. Pracodawca lub upoważniony przez niego Informatyk lub inne osoby wyznaczone przez pracodawcę mają prawo monitorować i kontrolować pracę na komputerze, z zachowaniem przepisów prawa i po uprzednim poinformowaniu pracownika.
 14. Użytkownik nie ma prawa podłączać komputera służbowego do publicznych sieci Wi-Fi oraz do zewnętrznych ogólnodostępnych innych form pośredniczących w dostępie do Internetu.
 15. Pracownik wykonujący prace zdalnie może korzystać z nośników zewnętrznych, w tym dysków

USB, pendrive itp., wyłącznie za wiedzą i zgodą Pracodawcy oraz z wykorzystaniem wyłącznie nośników zaszyfrowanych.

16. Pracownik oświadcza, że zobowiązuje się przestrzegać zasad ochrony danych osobowych podczas wykorzystywania udostępnionego sprzętu, w tym zobowiązuje się do:
- a) dołożenia wszelkich starań przy wykonywaniu powierzonych obowiązków w celu ochrony danych osobowych,
 - b) zachowaniu w tajemnicy loginu i hasła do systemu operacyjnego komputera służbowego oraz do właściwego zabezpieczenia loginu i hasła przed dostępem osób nieuprawnionych,
 - c) przetwarzania danych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi Pracodawcy,
 - d) do zabezpieczenia przetwarzanych danych przed ich:
 - udostępnieniem osobom nieupoważnionym,
 - zabraniem przez osobę nieuprawnioną,
 - przetwarzaniem z naruszeniem przepisów prawa,
 - nieuprawnioną zmianą lub zniszczeniem,
 - utratą,
 - uszkodzeniem,
 - e) należytego dbania o powierzony sprzęt, w szczególności o jego sprawność i czystość.
17. Pracownik akceptuje, że niewłaściwe korzystanie z systemów, sieci i zasobów komputerowych może prowadzić do zawieszenia praw dostępu, do postępowania dyscyplinarnego i/lub prawnego.
18. Na polecenie Pracodawcy, wraz z zakończeniem polecenia wykonywania pracy zdalnej - Pracownik zobowiązany jest do zwrotu technicznie sprawnego komputera wraz z wszelkimi danymi służbowymi bez prawa ich skopiowania w jakiegokolwiek formie.

.....
(data i podpis pracownika)

Zwrot udostępnionego sprzętu elektronicznego

Uwagi:

Data zwrotu:

(podpis osoby odbierającej sprzęt,
upoważnionej przez pracodawcę)

(data i podpis pracownika)

Świadoma/świadom odpowiedzialności cywilnej jak i karnej oraz art. 107 ustawy z dn. 10 maja 2018 r. o ochronie danych osobowych oświadczam, iż zdałam/em udostępniony sprzęt elektroniczny i nie jestem w posiadaniu żadnych dokumentów i innych materiałów zawierających informacje poufne, w szczególności dane osobowe, jakie

sporządziłam/em, zebrałam/em, opracowałam/em lub otrzymałam/em w czasie wykonywania pracy, włączając w to kopie, odpisy, a także zapisy na innych nośnikach.

Załącznik Nr 3
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

Oświadczenie
o wyrażeniu zgody na wykorzystywanie prywatnego sprzętu informatycznego
w celu wykonywania pracy zdalnej

Oświadczam, że posiadam niezbędny sprzęt informatyczny wraz z niezbędnym do pracy zdalnej oprogramowaniem i wyrażam zgodę na bezpłatne jego wykorzystywanie w celu wykonywania pracy zdalnej na rzecz **Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, ul. Reymonta 80, 41-250 Czeladź, tel. 32 265 15 57, email: sp1@sp1.czeladz.pl**

Wykorzystywany przeze mnie do pracy zdalnej sprzęt prywatny umożliwia poszanowanie i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

.....
(data, podpis pracownika)

U p o w a ż n i e n i e
do przetwarzania danych w ramach pracy zdalnej

Na podstawie art. 29 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 (RODO), Dz. Urz. UE L z 2016 r. nr 119/1, w związku z przepisami Kodeksu pracy

u p o w a ż n i a m

Panią/Pana

Stanowisko:

do przetwarzania danych osobowych poza siedzibą **Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**, w zakresie niezbędnym do wykonywania obowiązków służbowych wynikających z powierzonego Pani/Panu zakresu czynności w ramach pracy zdalnej.

Upoważnienie obejmuje następujący sposób przetwarzania:

[X] - elektronicznie

[] - papierowo

upoważnienie obowiązuje od dnia **do** zakończenia wykonywania przez Panią/Pana pracy zdalnej.

Upoważnienie do przetwarzania danych obejmuje wyłącznie miejsce wykonywania pracy zdanej określone w porozumieniu Pani/Pana z pracodawcą tj. Pani/Pana miejsce zamieszkania, W przypadku wyrażenia przez Pracodawcę zgody na wnoszenie dokumentacji papierowej, upoważnienie obejmuje również możliwość przemieszczania się z dokumentacją papierową z miejsca wykonywania pracy zdalnej do siedziby pracodawcy tj. **Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**. Jednocześnie w związku z wykonywaniem pracy zdalnej zobowiązuję Panią/ Pana do przestrzegania następujących zasad i procedur dotyczących przetwarzania danych osobowych:

- 1) dane zarówno w wersji papierowej jak i elektronicznej należy zabezpieczać przed dostępem osób trzecich. Nie należy udostępniać urządzeń na których wykonywana jest praca zdalna domownikom, współlokatorom lub innym osobom postronnym;
- 2) zabronione jest przemieszczanie się z dokumentacją służbową w inne miejsca, aniżeli miejsce uzgodnione z pracodawcą na potrzeby wykonywania pracy zdalnej tj. miejsce zamieszkania pracownika, z uwzględnieniem drogi dostarczenia dokumentacji z miejsca wykonywania pracy zdalnej do siedziby pracodawcy

- tj. **Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi** (dostarczenie dokumentacji/odbiór dokumentacji);
- 3) zabronione jest przekazywanie dokumentacji papierowej osobom trzecim, celem jej dostarczenia do zakładu pracy bez wcześniejszego powiadomienia o tym fakcie pracodawcy oraz otrzymania od niego zgody;
 - 4) przenosząc (transportując) dokumentację zawierającą dane osobowe pomiędzy zakładem pracy, a miejscem wykonywania pracy zdalnej, należy zastosować odpowiednie środki bezpieczeństwa, polegające w szczególności na przenoszeniu/przewożeniu dokumentów w zamkniętej teczce, i w żadnym wypadku nie wolno pozostawiać dokumentacji bez nadzoru w miejscach publicznych, ogólnodostępnych;
 - 5) dokumenty niepotrzebne zawierające dane osobowe należy przechowywać do momentu bezpiecznego zniszczenia w niszczarce – zabrania się ręcznego targania dokumentów i wyrzucania dokumentów służbowych do kosza na śmieci;
 - 6) Wymiana danych między zakładem pracy tj. siedzibą pracodawcy, a miejscem wykonywania pracy zdalnej opiera się głównie na komunikacji elektronicznej i wymaga przestrzegania następujących zasad:
 - a) **poczta elektroniczna:**
 - Komunikacja możliwa jest wyłącznie za pomocą poczty służbowej. Zabronione jest korzystanie z poczty prywatnej w celach służbowych.
 - Przesyłając dane osobowe pocztą elektroniczną należy każdorazowo wykorzystywać mechanizmy kryptograficzne (szyfrowanie załączników z danymi).
 - W przypadku zabezpieczenia plików (załączników z danymi) hasłem, obowiązuje zasada zastosowania przynajmniej 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym kanałem komunikacji np. telefonicznie lub SMS-em.
 - Należy zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
 - Bez weryfikacji wiarygodności nadawcy, nie należy korzystać z hiperlinków w wiadomościach e-mail.
 - Nie należy otwierać załączników (plików) w poczty elektronicznej nawet od znanych nam nadawców bez uważnej weryfikacji tegoż nadawcy.
 - Przy korzystaniu z poczty elektronicznej, Pracownik ma obowiązek przestrzegać tajemnicy pracodawcy, prawa własności przemysłowej i prawa autorskiego.
 - b) **zewnętrzne nośniki danych (pendrive, dysk zewnętrzny)**
 - Dozwolone jest używanie wyłącznie zaszyfrowanych służbowych nośników zewnętrznych dopuszczonych przez Administratora do pracy zdalnej.
 - W przypadku kradzieży lub zgubienia służbowego nośnika danych, należy natychmiast powiadomić o tym Pracodawcę lub Inspektora ochrony danych oraz Administratora IT, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
 - c) **zasady korzystania z komputera służbowego**
 - Zasady użytkowania sprzętu informatycznego udostępnionego pracownikowi na czas wykonywania pracy zdalnej oraz odpowiedzialność za używanie służbowego

sprzętu określone zostały w „Oświadczeniu o odpowiedzialności za używanie służbowego sprzętu informatycznego w celu wykonywania pracy zdalnej”.

Na podstawie niniejszego upoważnienia jest Pan/Pani zobowiązany/a do przetwarzania danych osobowych wyłącznie we wskazanym zakresie oraz zgodnie z przepisami RODO i obowiązującymi u Pracodawcy procedurami oraz polityką ochrony danych. Informuję, jednocześnie, iż podpisane przez Panią/Pana oświadczenie do zachowania w tajemnicy danych osobowych oraz sposób ich zabezpieczenia, obowiązuje nie tylko w stosunku do przetwarzania danych w siedzibie pracodawcy, ale w każdym miejscu wykonywania obowiązków służbowych, również w przypadku wykonywania pracy zdalnej, oraz rozciąga się na okres po ustaniu zatrudnienia.

Wystawił:.....
(data i podpis Administratora Danych Osobowych)

Oświadczenie pracownika

Oświadczam, iż o niniejszym upoważnieniu i jego zakresie zostałem/am poinformowany/a w dniu oraz że rozumiem jego treść i zobowiązuję się do przestrzegania zawartych w nim postanowień i wytycznych oraz postanowień i wytycznych zawartych w Regulaminie.

.....
(data i podpis pracownika)

Oświadczenie pracownika

W związku z powierzeniem mi wykonywania pracy zdalnie na zasadach obowiązujących u Pracodawcy oświadczam, że zapoznałem/zapoznałam się z **Regulaminem przetwarzania i ochrony danych osobowych w pracy zdalnej w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi** i zobowiązuję się do jego przestrzegania i respektowania wszelkich zasad z niego wynikających.

.....
(data i podpis pracownika)

Procedura użytkowania prywatnego sprzętu informatycznego / mobilnego w celu wykonywania pracy zdalnej

1. Pracownik (dalej również Użytkownik) oświadcza, że dysponuje sprzętem informatycznym, który dobrowolnie udostępnia pracodawcy na cele wykonywania pracy zdalnej. Sprzęt komputerowy jest sprawny technicznie i jest podłączony do prywatnego Internetu pracownika.
2. Użytkownik na czas udostępnienia komputera prywatnego na potrzeby wykonywania pracy zdalnej nie będzie korzystał z zewnętrznych form pośredniczących w dostępie do Internetu, w tym z zewnętrznych publicznych sieci Wi-Fi.
3. Pracownik oświadcza, że komputer posiada zainstalowane oprogramowanie antywirusowe
4. Pracownik w godzinach pracy tj od 7 do 16 zobowiązuje się używać komputera prywatnego wyłącznie do wykonywania zadań służbowych w formie pracy zdalnej.
5. Pracownik zobowiązuje się w okresie obowiązywania polecenia wykonywania pracy zdalnej w godzinach wykonywania obowiązków służbowych na komputerze prywatnym zabezpieczyć sprzęt przed dostępem osób trzecich, w tym domowników/współlokatorów.
6. Przetwarzanie informacji służbowych, w tym szczególnie danych osobowych za pomocą komputera prywatnego wymaga przestrzegania przez pracownika zasad i procedur obowiązujących u pracodawcy, a dotyczących bezpiecznego przetwarzania danych w formie elektronicznej.
7. Pracownik zobowiązuje się niezwłocznie powiadomić pracodawcę w formie pisemnej lub elektronicznej o:
 - a) zaistnieniu zmiany stanu technicznego komputera prywatnego, uniemożliwiającego jego eksploatację,
 - b) zaistnieniu innych niż wymienione w punkcie a) okoliczności, uniemożliwiających używanie komputera prywatnego do celów służbowych.
8. Użytkownik oświadcza, że zobowiązuje się przestrzegać zasad ochrony danych na komputerze podczas wykonywania obowiązków służbowych, w tym zobowiązuje się do:
 - c) dołożenia wszelkich starań przy wykonywaniu powierzonych obowiązków w celu ochrony danych osobowych,
 - d) zachowaniu w tajemnicy loginu i hasła do łączenia się z zakładem pracy,
 - e) przetwarzania danych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi Pracodawcy,
 - f) do zabezpieczenia przetwarzanych danych przed ich:
 - udostępnieniem osobom nieupoważnionym,
 - zabranieniem przez osobę nieuprawnioną,

- przetwarzaniem z naruszeniem przepisów prawa,
 - nieuprawnioną zmianą lub zniszczeniem,
 - utratą,
 - uszkodzeniem,
- g) do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia.
9. Nieprzestrzeganie przez pracownika zapisów niniejszego regulaminu, będzie stanowić naruszenie obowiązków pracowniczych wynikających z Kodeksu pracy.

Oświadczam, że zapoznałem się z procedurą użytkowania prywatnego sprzętu informatycznego w celu wykonywania pracy zdalnej i zobowiązuję się do stosowania zapisów w niej zawartych.

.....
(data i podpis pracownika)

Klauzula informacyjna dla pracownika wykonującego pracę zdalną

1. Administratorem Pani/Pana danych osobowych jest **Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi, ul. Reymonta 80, 41-250 Czeladź, tel. 32 265 15 57** e-mail: **sp1@sp1.czeladz.pl**, dalej: Administrator.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się za pośrednictwem następujących danych kontaktowych: e-mail: **iodo@marwikpoland.pl**
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, na podstawie tych danych, nie będą podejmowane decyzje w sposób zautomatyzowany.

