ZARZĄDZENIE NR 13/2022/2023

Dyrektora Szkoły Podstawowej nr 1 w Porębie
z dnia 27.03.2023r.

w sprawie nauczania wprowadzenia regulaminu przetwarzania i ochrony danych osobowych w pracy zdalnej w Szkole Podstawowej nr 1 im. Wojska Polskiego

§ 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.

§ 1

Wprowadza się regulaminu przetwarzania i ochrony danych osobowych w pracy zdalnej w Szkole Podstawowej nr 1 im. Wojska Polskiego, stanowiącej załącznik do niniejszego zarządzenia.

§ 2.

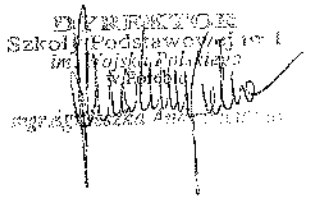
Zobowiązuje się pracowników Szkoły Podstawowej nr 1 w Porębie do zapoznania się i stosowania Procedury, o której mowa powyżej w § 1.

§ 3.

Zarządzenie podlega upublicznieniu poprzez wywieszenie na tablicy ogłoszeń w budynku Szkoły Podstawowej nr 1 w Porębie i na stronie BIP.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.



Załącznik do zarządzenia nr 12/2022/2023
Dyrektora Szkoły Podstawowej nr 1 w Porębie
z dnia 27.03.2023r.

REGULAMIN PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH W PRACY ZDALNEJ

w Szkole Podstawowej nr 1 im. Wojska Polskiego

§ 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 zdalne 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 zdalnie, 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) dostęp do systemu informatycznego przetwarzającego dane osobowe (w tym: dziennik elektroniczny),
3) dostęp do określonych zasobów w infrastrukturze IT pracodawcy przy użyciu szyfrowanego połączenia zdalnego VPN. Pracownik zobowiązuje się do zachowania w tajemnicy powierzonych mu danych dostępowych (danych uwierzytelniających) - Załącznik nr 5,
4) udostępnienie pracownikowi elektronicznych kopii dokumentów na zaszyfrowanym nośniku służbowym (np. pendrive),
5) komunikacja za pomocą komunikatora internetowego (m.in. MS Teams, Zoom, Webex),
6) korzystanie z usług chmurowych (nazwa *usługi np. OneDrive, Dysk Google*) w zakresie (zakres zadań).

§ 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 przesyłać 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 7**) do niniejszego Regulaminu.

§ 21

W przypadku wykonywania przez pracownika pracy zdalnej z wykorzystaniem sprzętu prywatnego obowiązuje (**Załącznik nr 8**)do niniejszego Regulaminu.

§ 23

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

załącznik nr 1
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

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 zdalnejw Szkole Podstawowej nr 1 im. Wojska Polskiego***. 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

załącznik nr 2
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

Protokół
udostępnienia sprzętu elektronicznego do celów służbowych

Z dniem .....udostępniam Pani/Panu .....

zatrudnionemu na stanowisku .....

niżej wymieniony sprzęt elektroniczny:

LP	Typ sprzętu	Model	Numer seryjny
1	np. Smartfon		
2			

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 zaginięciu 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 któregokolwiek 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) w przypadku łączenia się zdalnie z komputerem w zakładzie pracy, po zakończeniu pracy pracownik zobowiązany jest zakończyć połączenie VPN (przerwać połączenie) z pracodawcą, wylogować się z komputera, oraz odpowiednio zabezpieczyć komputer deponując w bezpiecznym miejscu.
    f) 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 jakiejkolwiek formie.

.....

(data i podpis pracownika)

Zwrot udostępnionego sprzętu elektronicznego

Uwagi: _____

Data zwrotu: _____

_____

podpis osoby odbierającej
sprzęt,
upoważnionej przez
pracodawcę

Świadoma/świadom odpowiedzialności cywilnej jak i karnejoraz 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.

_____

data i podpis pracownika

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. Wojska Polskiego, ul. Wojska Polskiego4, 42-480Poręba, tel. 32 67 71 101, email: sekretariat@sp1poreba.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

załącznik nr 4
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

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. Wojska Polskiego,** 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 (dnia.... /zakończenia wykonywania przez Panią/Pana pracy zdalnej.)

Upoważnienie do przetwarzania danych obejmuje wyłącznie miejsce wykonywania pracy zdalnej określone w porozumieniu Pani/Pana z pracodawcą tj. Pani/Pana miejsce zamieszkania. W przypadku wyrażenia przez Pracodawcę zgody na wynoszenie 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. Wojska Polskiego.**
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. Wojska Polskiego**(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)

załącznik nr 5
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

Przyznanie uprawnień do dostępu zdalnego VPN

dla Pani/Pana
.....
.....

stanowisko:
.....
.....

Nadaję Pani/Panu uprawnienia umożliwiające pracę zdalną oraz dostęp do wewnętrznych zasobów Sieci Komputerowej Pracodawcy za pomocą VPN na okres od DD.MM.RRRR do DD.MM.RRRR \ do odwołania.

Identyfikator:.....

Hasło: .....

.....
...
Podpis pracodawcy

Oświadczenie

Oświadczam, że zostałem poinformowany o obowiązku zachowania w tajemnicy przyznanych mi danych uwierzytelniających do dostępu do sieci służbowej VPN oraz o odpowiedzialności dyscyplinarnej oraz karnej za naruszenie zapisów niniejszego oświadczenia.

.....
...
Podpis pracownika

Przyznanie uprawnień do laptopa służbowego na poziomie systemu operacyjnego

dla Pani/Pana

.....

.....

stanowisko:

.....

.....

Nadaję Pani/Panu identyfikator i hasło startowe do systemu operacyjnego komputera udostępnionego na potrzeby wykonywania pracy zdalnej na okres od DD.MM.RRRR do DD.MM.RRRR \ bezterminowo.

Identyfikator:.....

Hasło: .....

Jednocześnie zobowiązuję Panią/Pana do zmiany hasła przy pierwszej próbie zalogowania się do systemu operacyjnego udostępnionego komputera oraz zachowania hasła w tajemnicy pod rygorem odpowiedzialności

.....

...

Podpis pracodawcy

Przyjęłam/przyjąłem do wiadomości i stosowania:

.....

Data i Podpis pracownika

Załącznik 6
do Regulaminu przetwarzania i ochrony danych osobowych w pracy zdalnej

ZASADY BEZPIECZEŃSTWA PRZETWARZANIA DANYCH DLA UŻYTKOWNIKÓW SYSTEMÓW INFORMATYCZNYCH

PORADNIK ADMINISTRATORA DANYCH

Szkoła Podstawowa Nr 1
im. Wojska Polskiego w Porębie
42-480 Poręba, ul. WP 4
tel./fax 32 67 71 101
NIP 649-223-74-31, REGON 000730030
Pieczęć firmowa

DYREKTOR
Szkoły Podstawowej nr 1
im. Wojska Polskiego
mgr A[illegible]

podpis Administratora danych

INSTRUKCJE

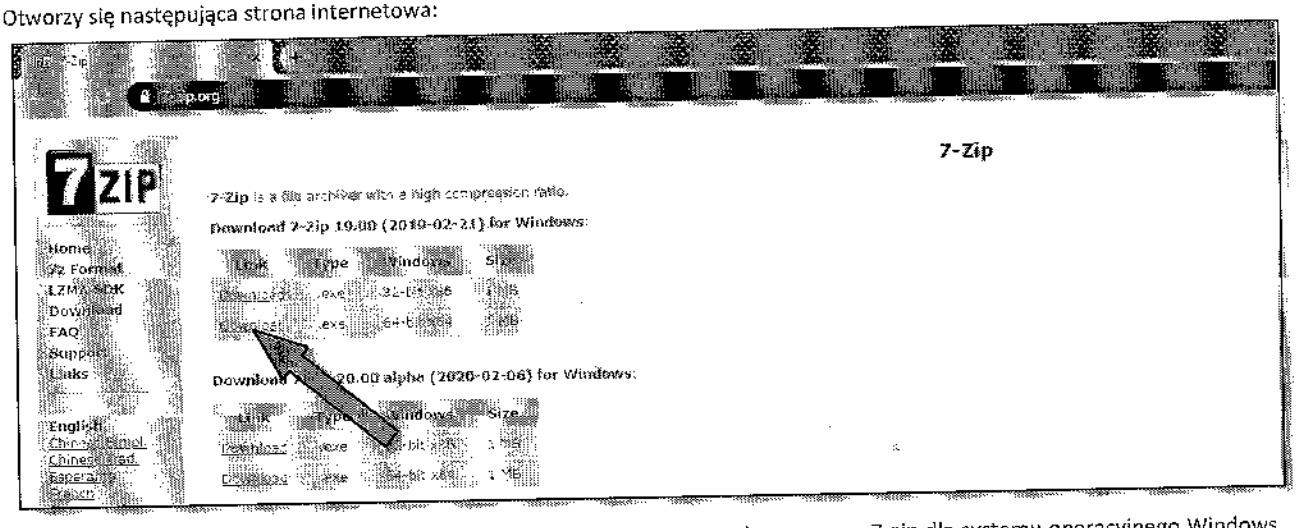
1. **SZYFROWANIE POSZCZEGÓLNYCH PLIKÓW I FOLDERÓW**
   Instrukcja nr 1 - Instrukcja instalacji oraz używania programu 7-zip
2. **SZYFROWANIE I UŻYTKOWANIE PENDRIVE'ÓW**
   Instrukcja nr 2 – Instrukcja szyfrowania pendrive'ów narzędziem BitLocker
3. **BEZPIECZNE KORZYSTANIE Z PRZEGLĄDARKI INTERNETOWEJ**
   Instrukcja nr 3 – Instrukcja bezpiecznego korzystania z przeglądarki internetowej

SZYFROWANIE POSZCZEGÓLNYCH PLIKÓW I FOLDERÓW (Instrukcja użytkowania oprogramowania)

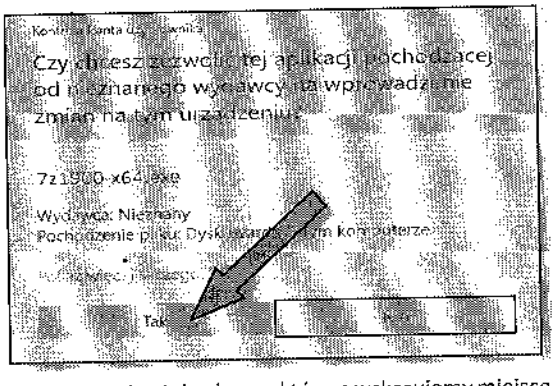
NAZWA OPROGRAMOWANIA:	*7-ZIP*
ZAKRES INSTRUKCJI:	*Instalacja, konfiguracja oraz szyfrowanie danych (plików i folderów)*

ETAP I: INSTALACJA

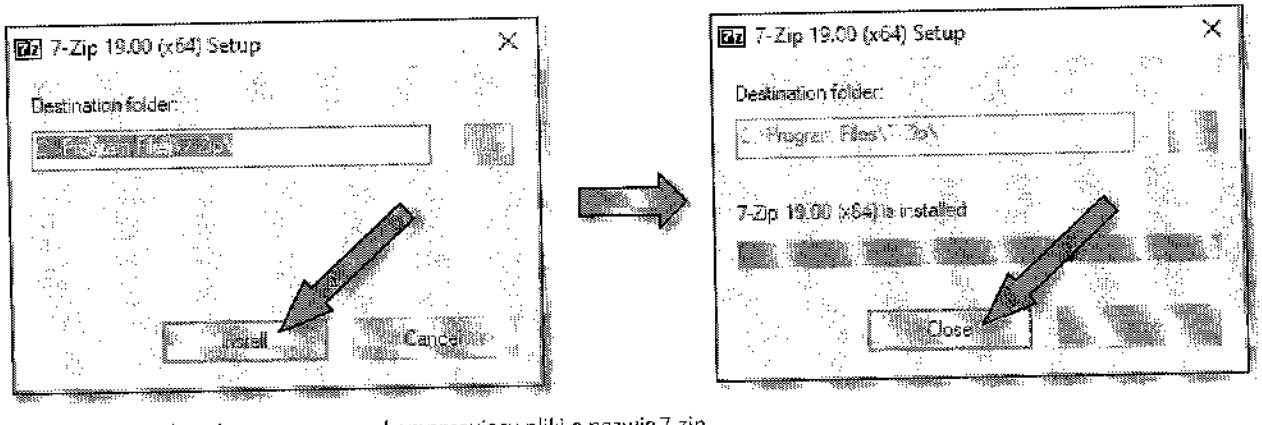
1. Otwórz przeglądarkę internetową (Chrome, Firefox, Edge itp.), następnie w pasku adresu wpisz: „**7-zip.org**" oraz naciśnij „**ENTER**". Otworzy się następująca strona internetowa:



2. Aby pobrać program, kliknij „Download" dla wersji 64-bit x64. Jest to wersja programu 7-zip dla systemu operacyjnego Windows 7, 8, 8.1, 10 w wersji 64 bitowej (bardzo rzadko spotyka się już systemy Windows wersji 32 bitowej z uwagi na przestarzałą technologię).
3. Następnie uruchom program. W przeglądarce Chrome znajdziemy skrót do programu w dolnym lewym rogu. W innych przeglądarkach zazwyczaj pobrane programy znajdują się w katalogu: „**Pobrane**". Po uruchomieniu programu może się pojawić komunikat i klikamy „**Tak**":



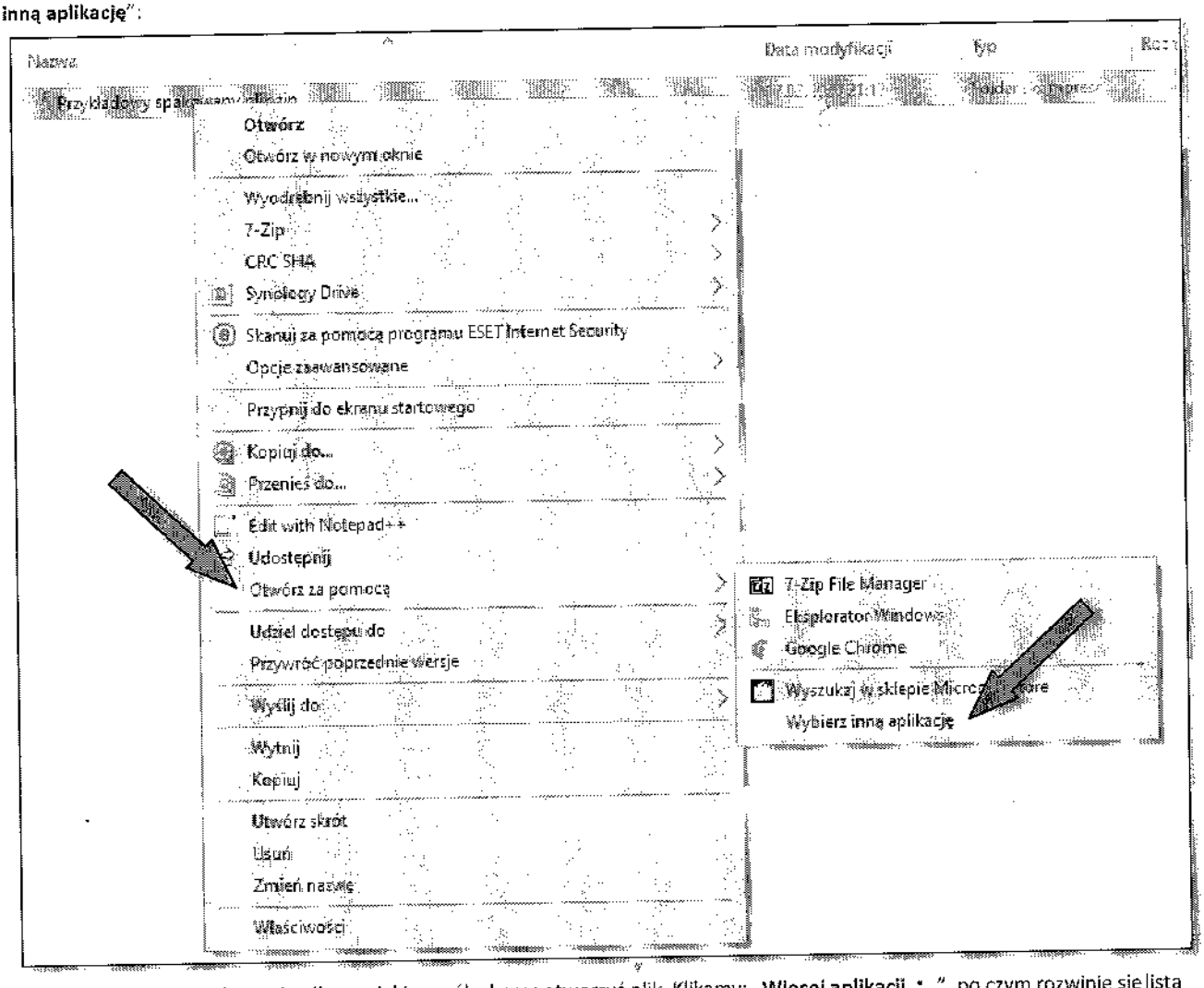
4. Następnie pojawi się okno w którym wskazujemy miejsce zainstalowania programu. Nie trzeba nic zmieniać. Klikamy tylko „**Install**", a po zainstalowaniu programu „**Close**":



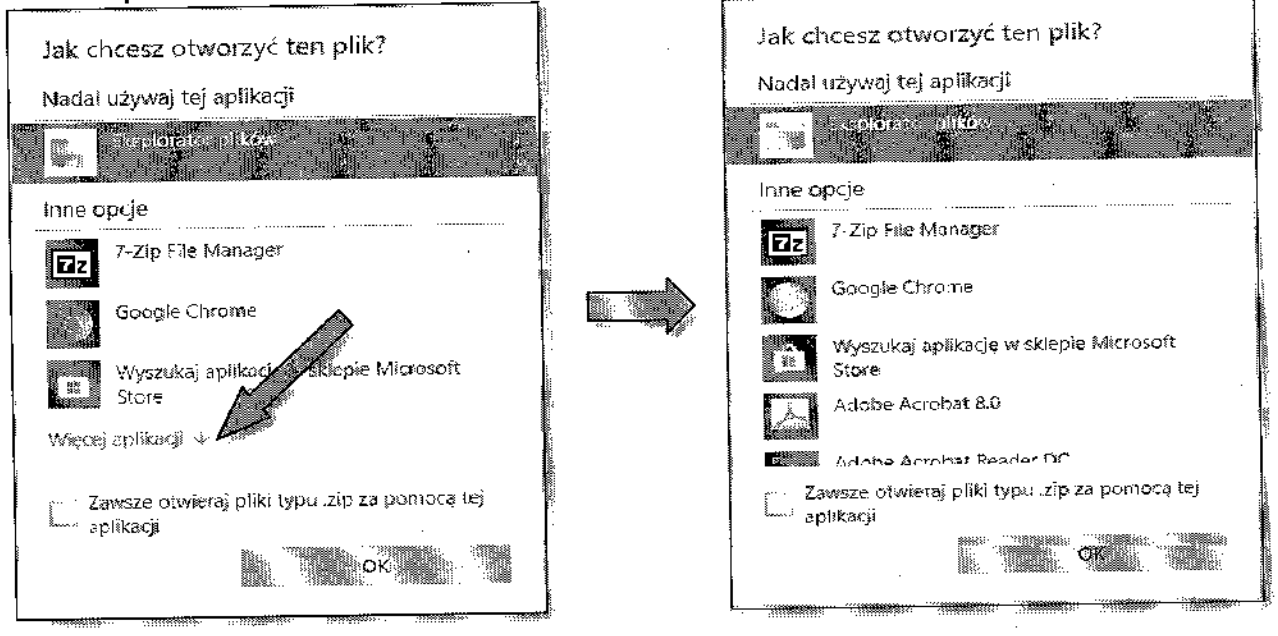
5. Od teraz masz zainstalowany program kompresujący pliki o nazwie 7-zip.

ETAP II: KONFIGURACJA

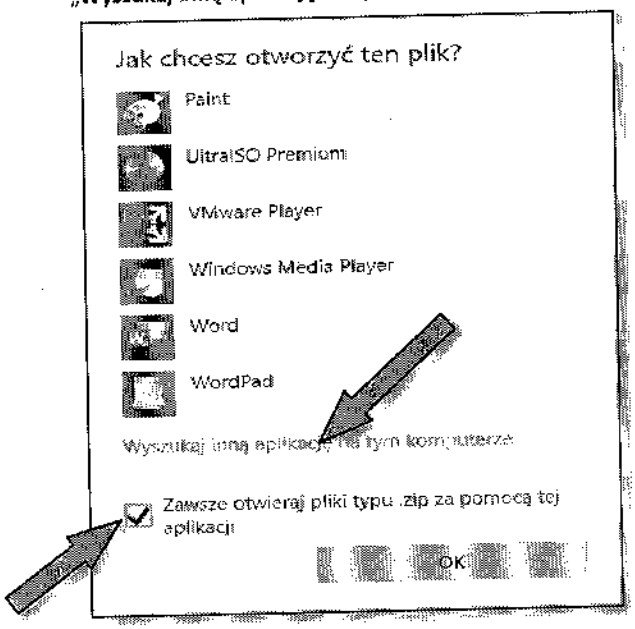
1. Czasami system operacyjny Windows pomimo instalacji programu 7-zip otwiera pliki skompresowane „spakowane" poprzez swoje zaimplementowane narzędzie do archiwów. Stwarza to częste problemy w przypadku „zahasłowanych" archiwów. Warto to zmienić. Aby to wykonać:
2. Znajdź na swoim komputerze jakikolwiek „skompresowany „spakowany" plik z rozszerzeniem *.zip.
3. Kliknij go prawym przyciskiem myszy → rozwinie się podręczne menu, w którym klikamy po kolei: **„Otwórz za pomocą" → „Wybierz inną aplikację"**:



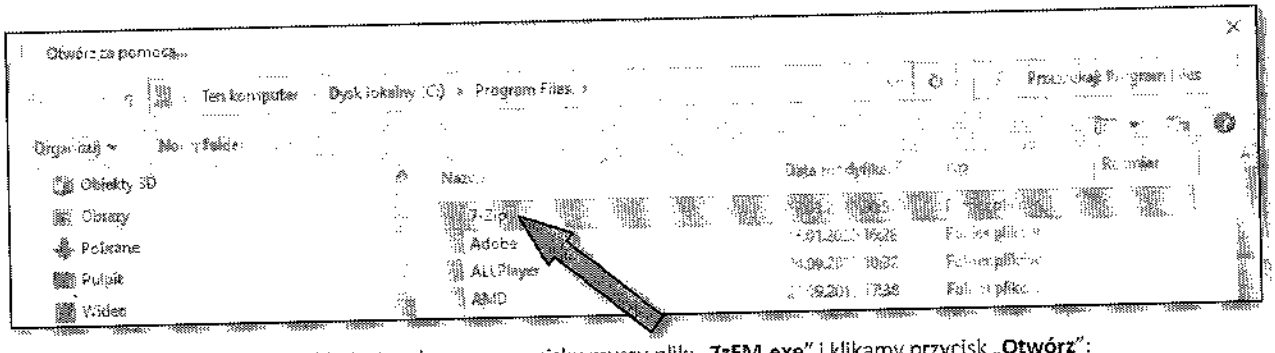
4. Otworzy się okno, w którym określasz w jaki sposób chcesz otworzyć plik. Klikamy: **„Więcej aplikacji** ˅ **"**, po czym rozwinie się lista z większa ilością programów:



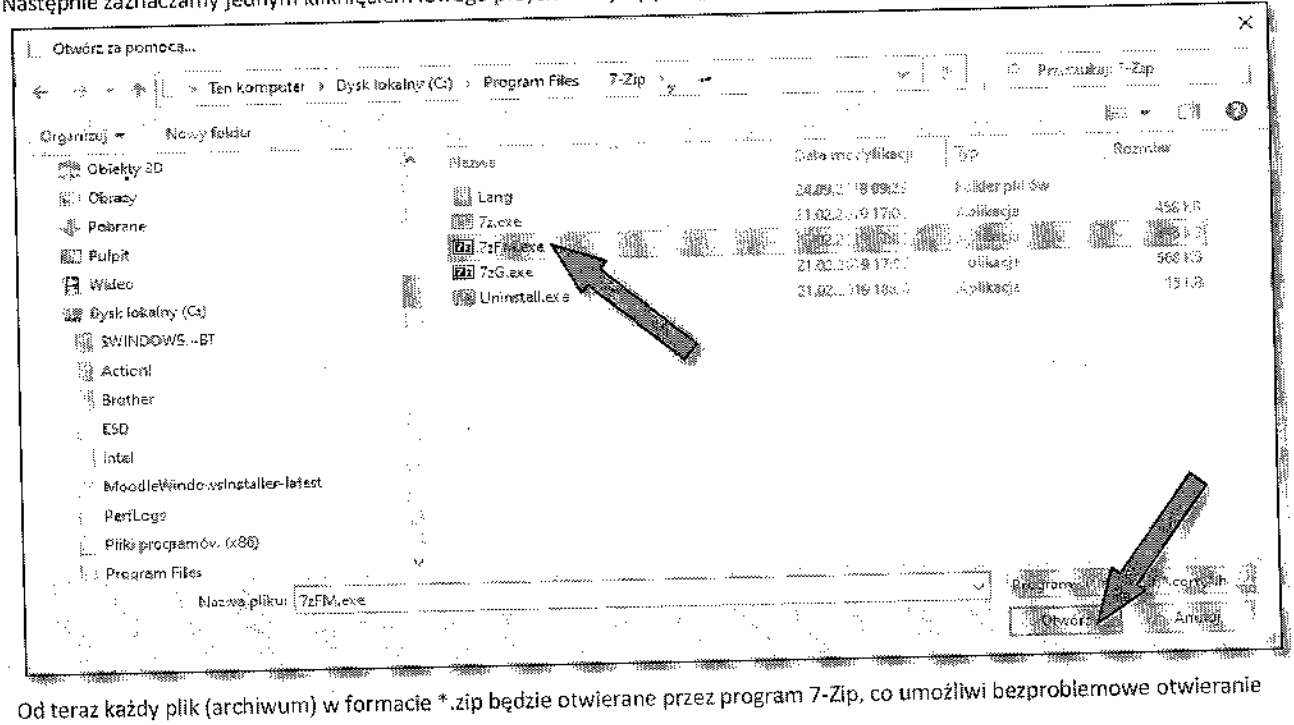
5. Następnie przewiń listę na sam dół, zaznacz „✓" checkbox **„Zawsze otwieraj pliki typu .zip za pomocą tej aplikacji"** oraz kliknij **„Wyszukaj inną aplikację na tym komputerze"**.



6. Teraz otworzy się okno, w którym wskazujemy folder zawierający program 7-zip. W każdej wersji Windowsa (czy to 7, 8, 8.1 bądź 10) może być inaczej. Niniejsza instrukcja opiera się o system operacyjny Windows 10, gdzie folder z programem ma następującą ścieżkę: „/Ten komputer/Dysk lokalny (C)/Program files/7-Zip/" lub w nomenklaturze informatycznej: „C:\Program Files\7-Zip". A więc klikamy dwa razy lewym przyciskiem myszy (aby otworzyć) folder **„7-Zip"**:



7. Następnie zaznaczamy jednym kliknięciem lewego przycisku myszy plik: **„7zFM.exe"** i klikamy przycisk **„Otwórz"**:

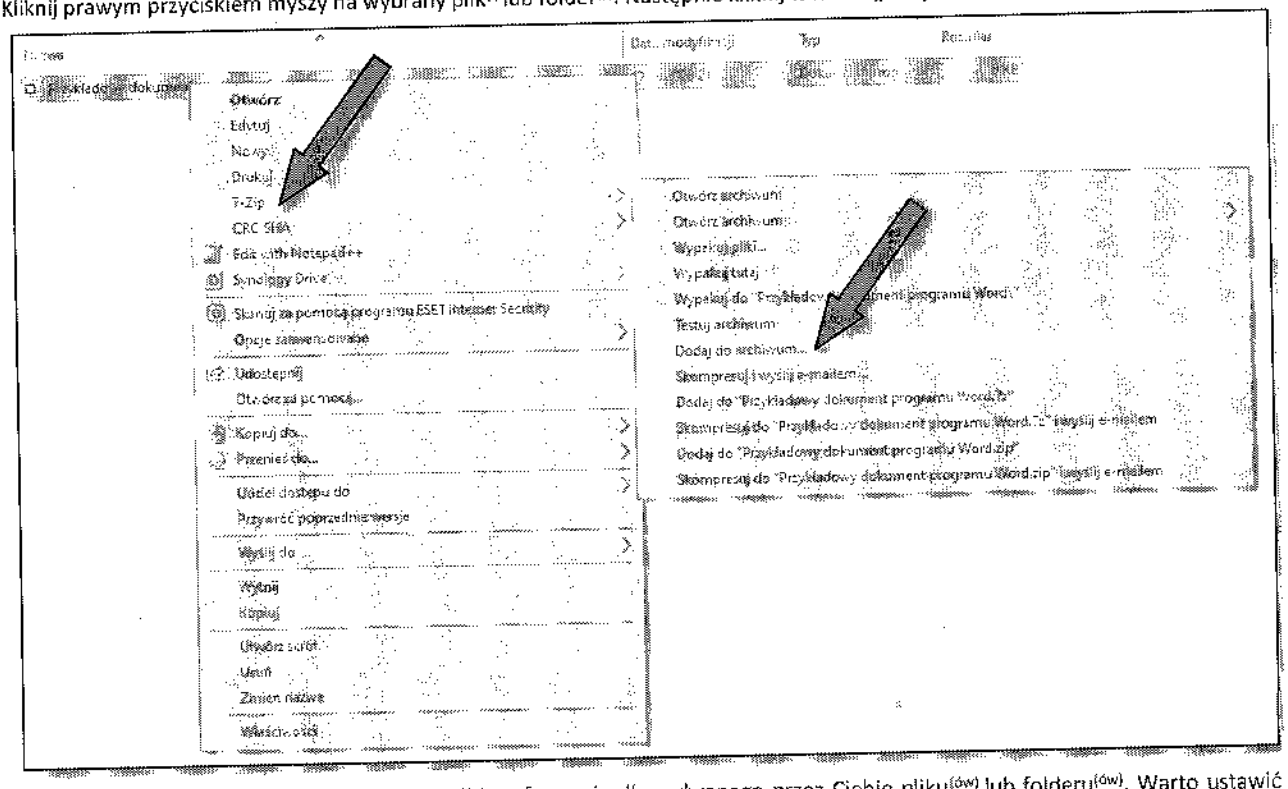


8. Od teraz każdy plik (archiwum) w formacie *.zip będzie otwierane przez program 7-Zip, co umożliwi bezproblemowe otwieranie „zahasłowanych" plików.

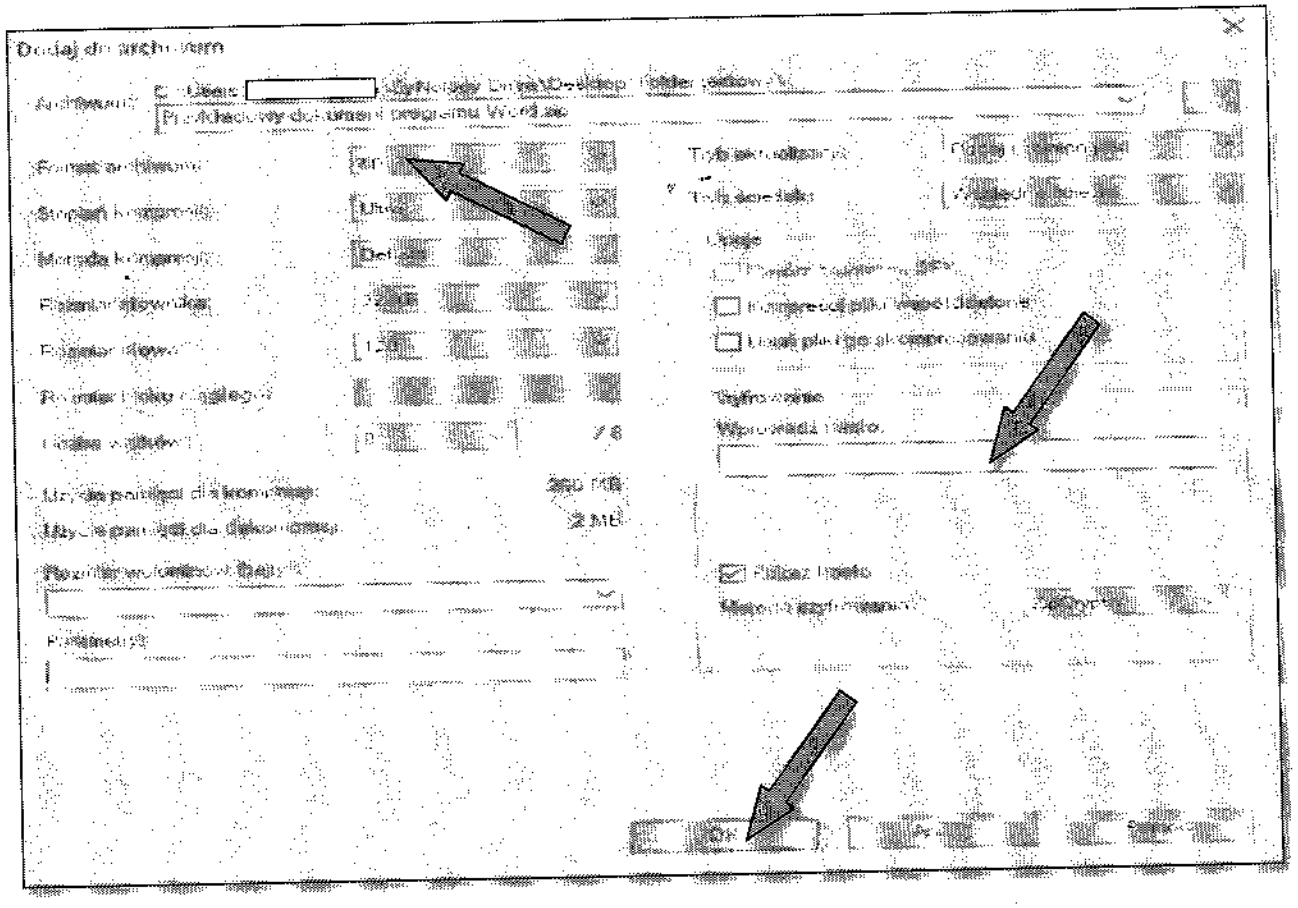
ETAP III: SZYFROWANIE DANYCH (PLIKÓW I FOLDERÓW)

Chcąc zaszyfrować plik lub cały folder, musisz wykonać następujące czynności:

1. Kliknij prawym przyciskiem myszy na wybrany plik(i) lub folder(y). Następnie kliknij w menu **„7-Zip"** oraz **„Dodaj do archiwum..."**:



2. Teraz otworzy się okno konfiguracji kompresji i szyfrowania dla wybranego przez Ciebie pliku(ów) lub folderu(ów). Warto ustawić format archiwum na **„ZIP"**. W przyszłości automatycznie każda czynności kompresji i szyfrowania będzie zapamiętana dla tego ustawienia. Oczywiście w polu **„Wprowadź hasło"** wpisujemy je. Następnie klikamy **„OK"**. Po skompresowaniu („spakowaniu") pliku(ów) lub folderu(ów) plik z rozszerzeniem *.zip zapisze się w macierzystym katalogu, w którym były źródłowe dane. Wszystko gotowe :



SZYFROWANIE I UŻYTKOWANIE PENDRIVE'ÓW (Instrukcja użytkowania oprogramowania)

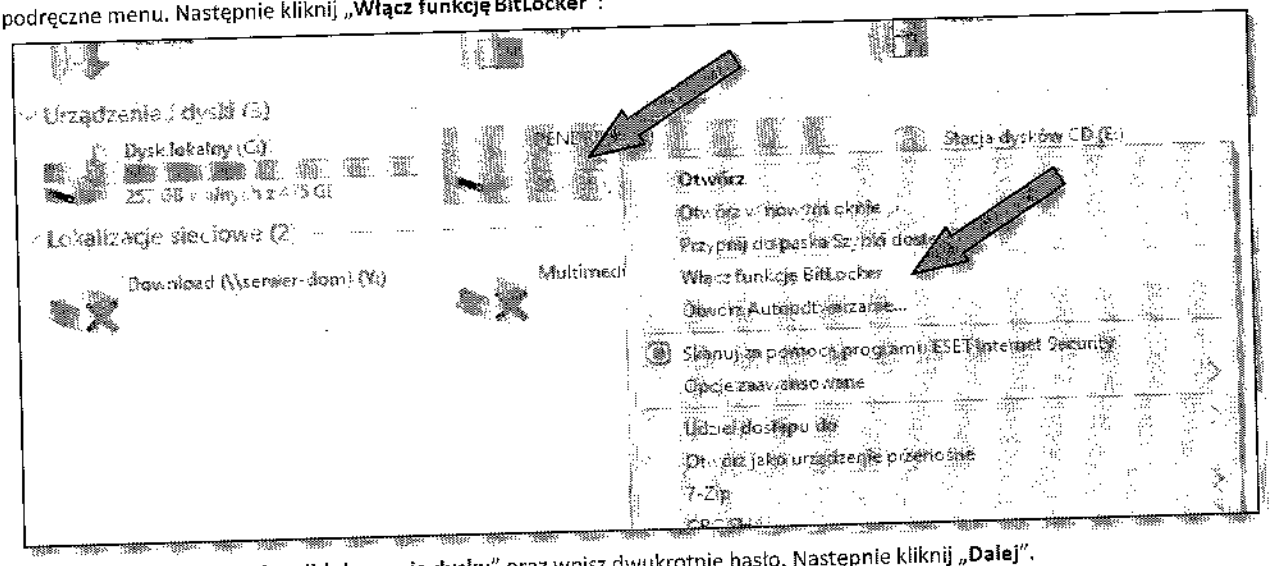
NAZWA OPROGRAMOWANIA:	*BitLocker*
ZAKRES INSTRUKCJI:	*Warunki techniczne, proces pierwszego szyfrowania, użytkowanie zaszyfrowanego penrive'a, odzyskiwanie pendrive'a poprzez „klucz odzyskiwania".*

ETAP I: WARUNKI TECHNICZNE

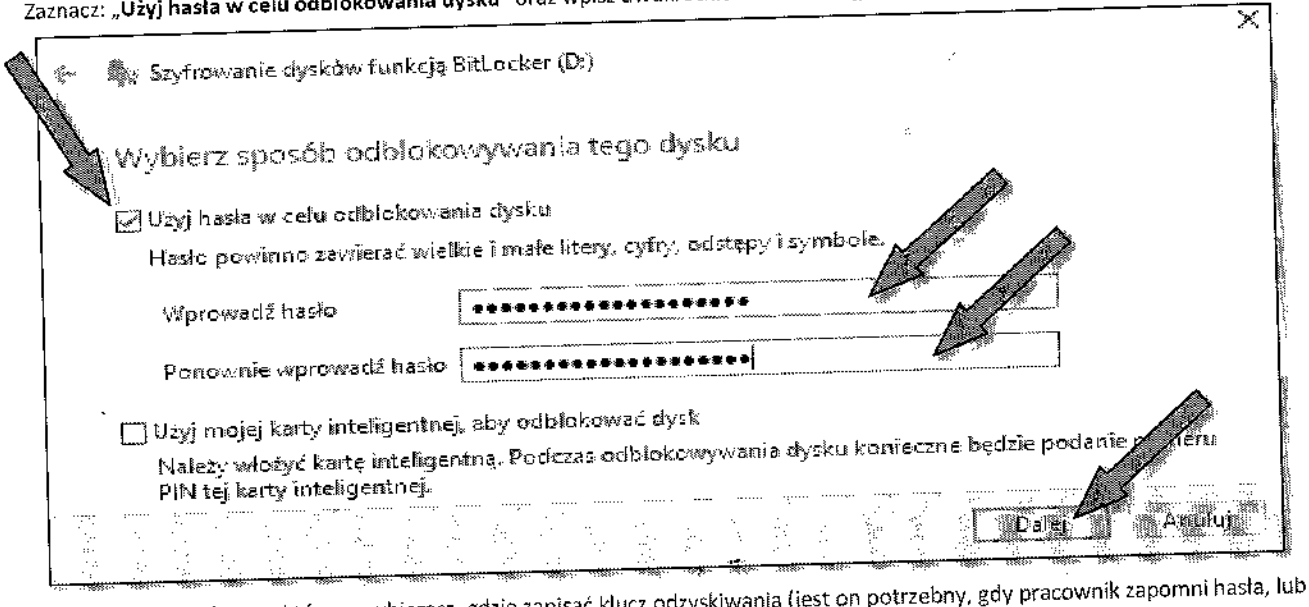
1. Chcąc korzystać z szyfrowania urządzeń zewnętrznych (np. pendrive'ów) na rynku IT jest wiele dostępnych narzędzi płatnych oraz bezpłatnych. Warto zauważyć, że większość z nich wymaga specjalistycznego oprogramowania oraz aby umożliwić odczyt zaszyfrowanego urządzenia na każdym komputerze → wymaga się zainstalowanego „agenta" lub innej formy dostępu do danych (w tym też dodatkowych plików „rozruchowych" na pendrive'ie). Jest to uciążliwe i w praktyce nie zawsze zapewniające w 100% bezpieczeństwo (chociażby z uwagi na częste praktyki dzielenia przestrzeni pamięci pendrive'a na zaszyfrowaną i niezaszyfrowaną, co skłania użytkowników do częstego zapisu w tej części nieszyfrowanej). Obecne techniki szyfrowania opierają się algorytmy szyfrowania typu AES-256, które gwarantują bardzo wysoki poziom bezpieczeństwa.
2. Zalecaną forma szyfrowania jest wbudowana funkcja BitLocker w system operacyjny Microsoft Windows, jednakże tylko niektóre wersje potrafią szyfrować przy czym każda obsługuje (odczyt i zapis) zaszyfrowany pendrive (oczywiście są wyjątki, ale mowa tu o bardzo przestarzałych wersjach sprzed parunastu lat).
3. Systemy operacyjne Microsoft Windows, które maja wbudowaną funkcję szyfrowania urządzeń zewnętrznychto:
   a) Windows 7 Ultimate oraz Enterprise,
   b) Windows 8 Pro oraz Enterprise,
   c) Windows 10 Pro Enterprise oraz Education
   d) Windows 11 Pro Enterprise oraz Education.
4. Jeżeli posiadamy chociażby jeden komputer z system operacyjnym spośród wyżej wymienionych, możemy zaszyfrować wszelakie pendrive i będą one działały na wszystkich systemach operacyjnych Microsoft Windows w tym na wersjach „Home", które niestety dość często są używane w sektorze publicznym i niepublicznym z uwagi na koszt zakupu wraz z nowym sprzętem (warto zauważyć, iż podczas zakupu sprzętu poleasingowego, zjawisko to właściwie nie występuję).
5. Warto rozważyć 2 scenariusze:
   a) zakup pendrive'ów oraz ich zaszyfrowanie (proces ten nie musi się nawet odbyć na sprzęcie organizacji → oczywiście z zachowaniem najwyższej staranności w zakresie bezpieczeństwa informacji). Na obecna chwilę, ceny rynkowe pendrive'ów są bardzo niskie. Wystarczająca pojemność oscyluje w granicach od 2 do 4 GB pamięci.
   b) wypracowanie z pracownikami organizacji wspólnego stanowiska co do zaszyfrowania ich prywatnego pendrive'a, co nie ograniczy swobody i prywatności pracownika (nadal ma pełny dostęp do danych), a wręcz polepszy ich prywatne bezpieczeństwo.
6. Urządzenie (pendrive) zaszyfrowane ww. metodą jest nadal w pełni funkcjonalne, sam proces szyfrowania jest bardzo krótki (parę minut), a dodatkowo podłączanie do komputera ogranicza się do włożenia urządzenia do portu USB, oraz wpisania hasła w wyskakującym okienku. Po wyciągnięciu urządzenia, pendrive jest w 100% zaszyfrowany, co uchroni organizację przez utratą poufności danych.

ETAP II: PROCES PIERWSZEGO SZYFROWANIA

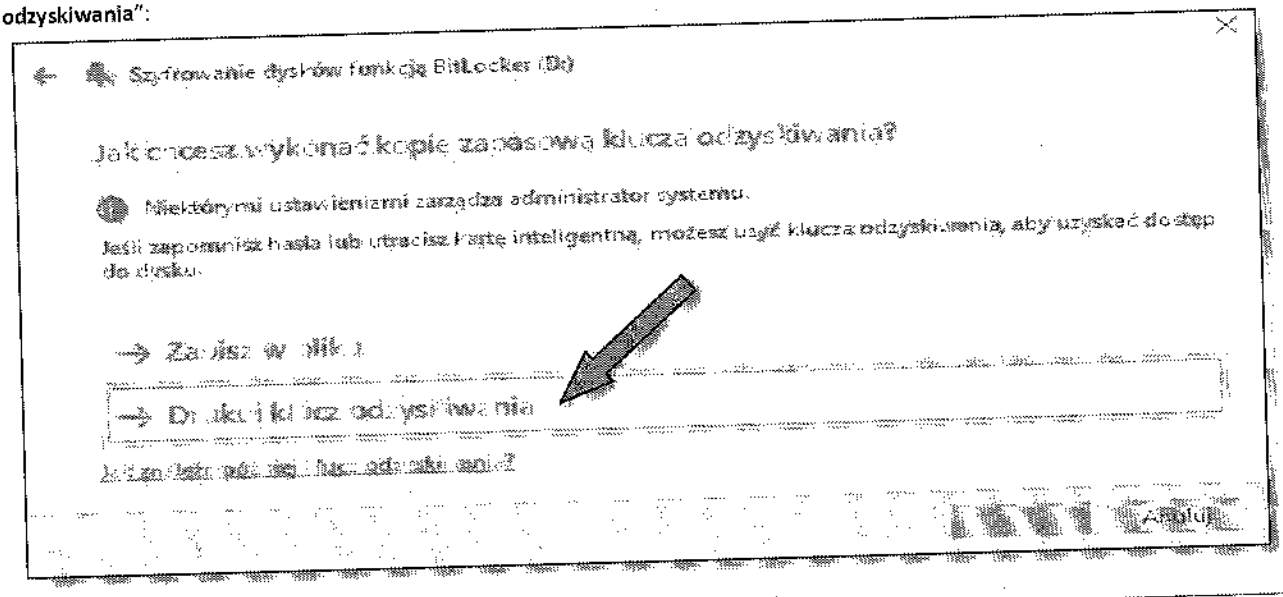
1. Włóż pendrive do jakiegokolwiek portu USB w komputerze z zainstalowanym systemem operacyjnym wymienionym w punkcie I-3.
2. Wejdź do „**Eksplorator plików**" oraz klikając prawym przyciskiem myszy na ikonkę pendrive'a który chcemy zaszyfrować rozwiń podręczne menu. Następnie kliknij „**Włącz funkcję BitLocker**":



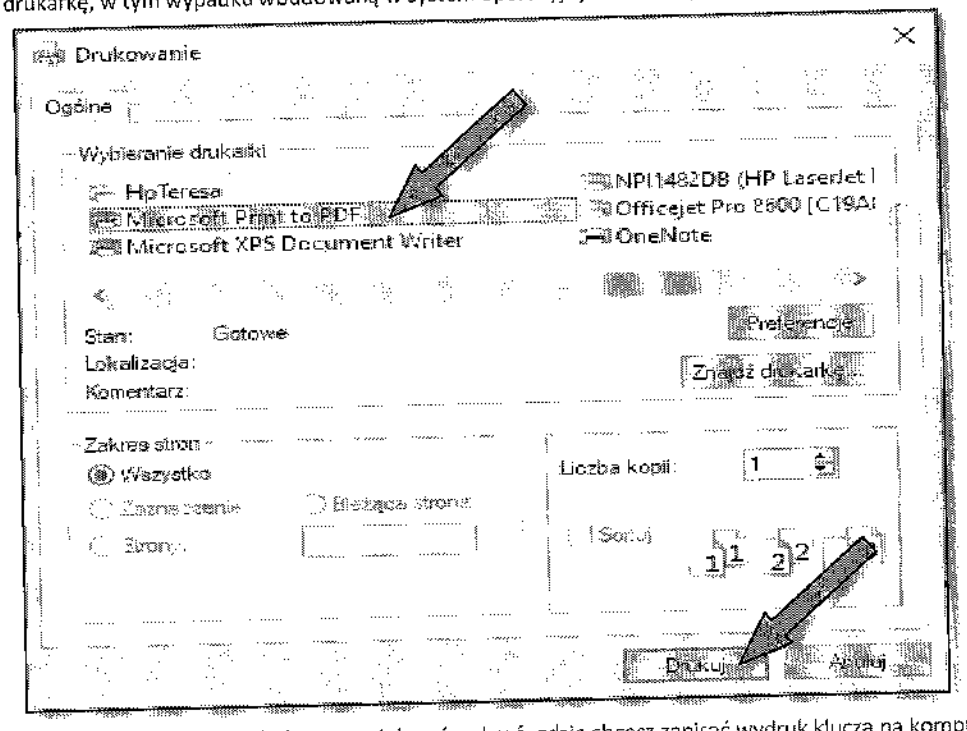
3. Zaznacz: „**Użyj hasła w celu odblokowania dysku**" oraz wpisz dwukrotnie hasło. Następnie kliknij „**Dalej**".



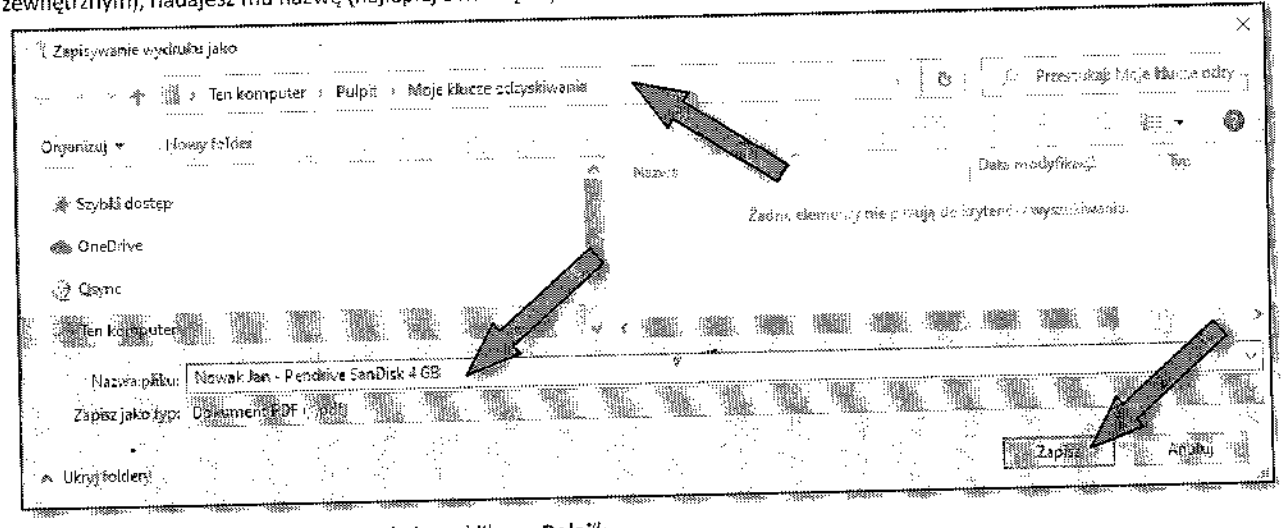
4. Teraz pojawi się okno, w którym wybierasz, gdzie zapisać klucz odzyskiwania (jest on potrzebny, gdy pracownik zapomni hasła, lub je zmieni bez wiedzy pracodawcy). Jeżeli wybierzesz opcję „**Zapisz w pliku**", to będzie potrzebny dodatkowy pendrive (na dysku twardym komputera, lub docelowo szyfrowanym pendrive nie można zapisać klucza). Zaleca się zaznaczyć/kliknąć: „**Drukuj klucz odzyskiwania**":



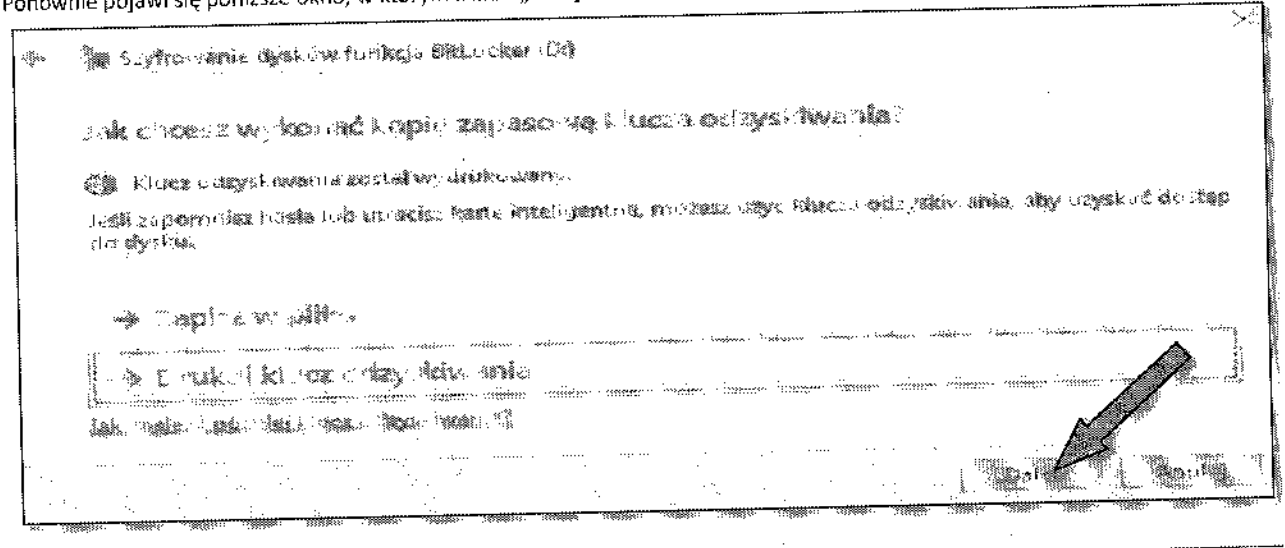
5. Następnie pojawi się okno „Drukowanie". W nim możesz wybrać, czy chcesz wydrukować zapasowy klucz odzyskiwania lub „wirtualnie" wydrukować do pliku PDF (czyli zapisać do PDF na dysku komputera). Większość systemów operacyjnych Windows ma takową funkcję pod postacią wirtualnej drukarki o nazwie: „Microsoft Print to PDF". Jeśli takiej nie masz, proponuje się zainstalować na komputerze darmową „drukarkę PDF" o nazwie PDF Creator (aby pobrać program, kliknij: link). Czyli zaznaczamy wirtualną drukarkę, w tym wypadku wbudowaną w system operacyjny Windows pod postacią „**Microsoft Print to PDF**" i klikasz „**Drukuj**".



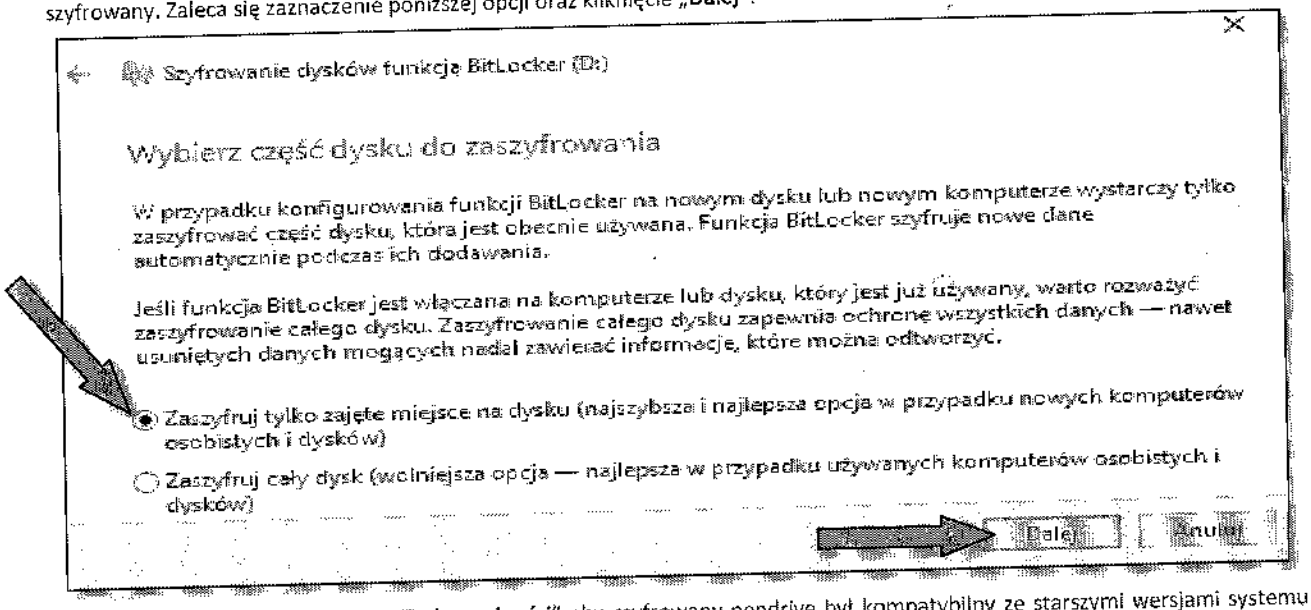
6. Teraz pojawi się okno, w którym powinieneś wybrać, gdzie chcesz zapisać wydruk klucza na komputerze (bądź innym urządzeniu zewnętrznym), nadajesz mu nazwę (najlepiej z nazwą użytkownika i urządzenia) oraz klikasz „**Zapisz**"



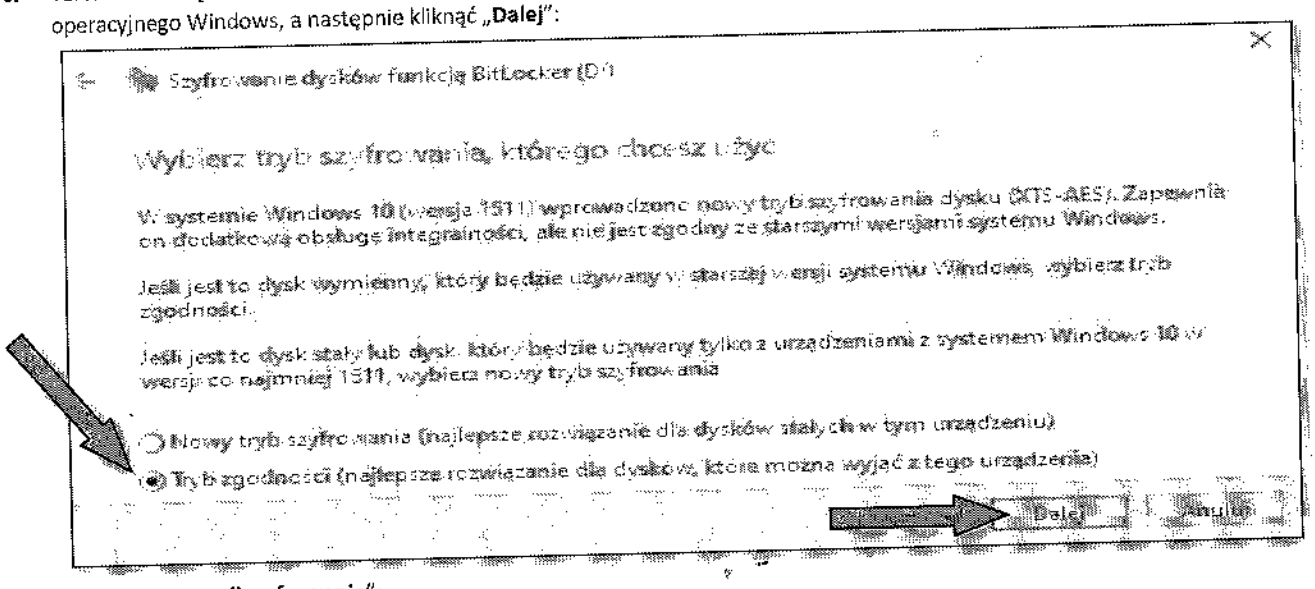
7. Ponownie pojawi się poniższe okno, w którym klikasz „**Dalej**":



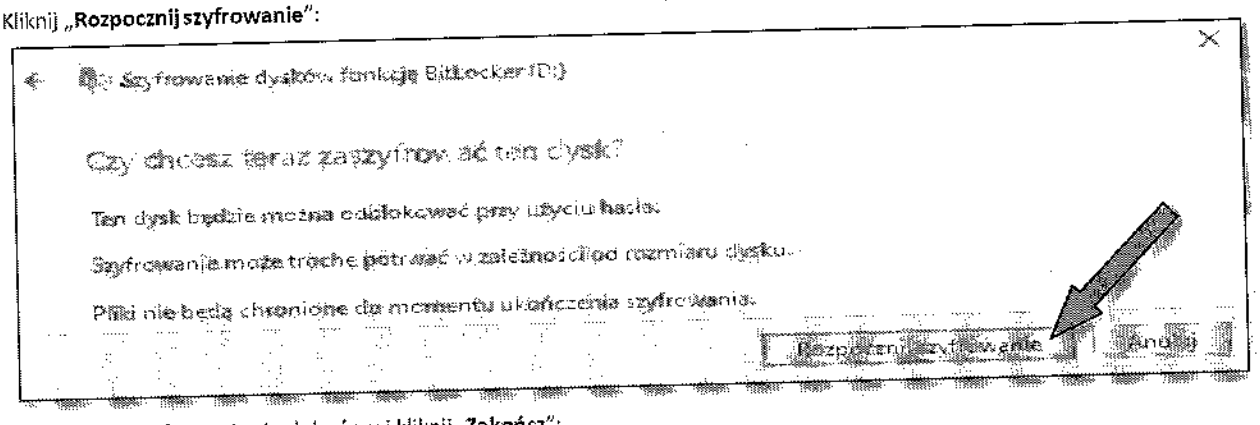
8. Na tym etapie wybierasz zakres szyfrowania tj. czy cały dysk, czy zapisaną część. Wszystko zależy, ile masz czasu, jednakże opcja „Zaszyfruj tylko zajęte miejsce na dysku..." jest wystarczająca. Każdy nowy plik dodany do pamięci pendrive'a będzie automatycznie szyfrowany. Zaleca się zaznaczenie poniższej opcji oraz kliknięcie „**Dalej**":



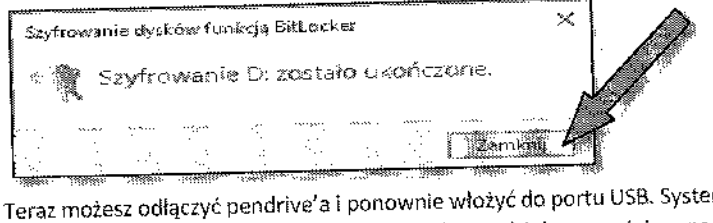
9. Teraz zaleca się zaznaczyć opcję: „**Tryb zgodności**" aby szyfrowany pendrive był kompatybilny ze starszymi wersjami systemu operacyjnego Windows, a następnie kliknąć „**Dalej**":



10. Kliknij „**Rozpocznij szyfrowanie**":



11. Poczekaj, aż szyfrowanie się dokończy i kliknij „**Zakończ**":



12. Teraz możesz odłączyć pendrive'a i ponownie włożyć do portu USB. System poprosi Cię o hasło.
13. Pamiętaj, aby trzymać „**klucze odzyskiwania**" w wydzielonym miejscu na komputerze lub innymurządzeniu..

załącznik nr 7
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

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 wSzkole Podstawowej nr 1 im. Wojska Polskiego** i zobowiązuję się do jego przestrzegania i respektowania wszelkich zasad z niego wynikających.

.....

(data i podpis pracownika)

załącznik nr 8
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

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 .... do ..... zobowiązuje się używać komputera prywatnego wyłącznie do wykonywania zadań służbowych w formie pracy zdalnej.
5. Praca zdalna na komputerze prywatnym pracownika polega na połączeniu się z miejsca wykonywania pracy zdalnej – z poziomu komputera prywatnego pracownika, poprzez funkcję pulpit zdalny z komputerem służbowym w zakładzie pracy.
6. Pracownik w celu połączenia się za pomocą pulpitu zdalnego z komputerem służbowym w pracy musi przeprowadzić proces uwierzytelniania (zalogowania się) zgodnie z nadanymi uprawnieniami do nawiązania bezpiecznego połączenia tunelowego VPN.
7. 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.
8. Pracownik zobowiązany jest kategorycznie przestrzegać wprowadzonych zasad komunikacji zdalnej umożliwiającej mu połączenie się zdalne ze stanowiskiem komputerowym w zakładzie pracy i wykonywaniem zadań służbowych, w szczególności poprzez:
   a) łączenie się za pomocą pulpitu zdalnego wyłącznie na czas wykonywania pracy zdalnej.
   b) po zakończeniu pracy za pomocą pulpitu zdalnego lub odejściu od stanowiska pracy na dłużej, bez możliwości monitorowania stanu uruchomionego komputera pracownik zobowiązany jest przerwać połączenie zdalne, wylosowując się bezpiecznie z funkcji zdalnego dostępu do komputera w zakładzie pracy.
9. 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.
10. 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.

19. Użytkownik ma prawo zapisywania dokumentów elektronicznych wyłącznie na udostępnionym zdalnie za pomocą łącza VPN komputerze w zakładzie pracy lub służbowym nośniku zewnętrznym (np. pendrive).
20. Użytkownik oświadcza, że zobowiązuje się przestrzegać zasad ochrony danych na komputerze podczas wykonywania obowiązków służbowych, 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 łączenia się z zakładem pracy,
    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) do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia.
21. 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. Wojska Polskiego, ul. Wojska Polskiego4, 42-480Poręba, tel.32 67 71 101** e-mail: **sekretariat@sp1poreba.pl**, dalej: Administrator.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się za pośrednictwem następujących danych kontaktowych: **e-mail: iod@sp1poreba.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)./*w tym punkcie można także doprecyzować odbiorców danych osobowych, jeżeli dane udostępniane są jeszcze innym podmiotom*/
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.