ZARZĄDZENIE NR 38/2020

DYREKTORA

Szkoły Podstawowej nr 5 im. Leonida Teligi

w Grodzisku Mazowieckim

z dnia 6 listopada 2020 r.

w sprawie bezpiecznego przetwarzania danych osobowych w okresie wprowadzenia w placówce konieczności pracy w modelu zdalnym na czas trwania sytuacji kryzysowych

§1

Mając na względzie ustawowy obowiązek ochrony danych osobowych przetwarzanych w postaci dokumentów tradycyjnych lub elektronicznych, wprowadzam w **Szkole Podstawowej nr 5 im. L. Teligi w Grodzisku Mazowieckim** usystematyzowane zasady użycia wskazanych sposobów komunikacji elektronicznej adekwatnych do celów, formy, wielkości dokumentów i kontekstu przetwarzania danych osobowych.

§2

Usystematyzowane zasady użycia, o których mowa w §1, jako integralny dokument obowiązującej Polityki Ochrony Danych Osobowych zawiera opracowanie pod nazwą **„Zasady bezpiecznego przetwarzania danych osobowych w okresie wprowadzenia w placówce konieczności pracy w modelu zdalnym na czas trwania sytuacji kryzysowych”**, stanowi załącznik nr 1 do niniejszego zarządzenia.

§3

Ustanowione zasady bezpiecznego przetwarzania danych osobowych ujęte w załączniku nr 1 obowiązują każdego pracownika posiadającego upoważnienie Administratora dopuszczające do przetwarzania danych osobowych na powierzonym stanowisku.

§4

Opracowane zasady przetwarzania danych osobowych ujęte w załączniku nr 1 obowiązują bez względu na użyty przez pracownika typ sprzętu teleinformatycznego i jego podmiotowy charakter.

§5

W przypadku, kiedy pracownik decyduje się dokonywać przetwarzania danych podczas wykonywania zadań służbowych z użyciem sprzętu będącego jego własnością jest zobowiązany do złożenia stosownej deklaracji dyrektorowi placówki.

§6

Zarządzenie wchodzi w życie z dniem ogłoszenia.

……..

/ Administrator danych – Dyrektor szkoły /

Załącznik nr 1
do Zarządzenia nr 38 /2020

Zasady bezpiecznego przetwarzania danych osobowych w okresie wprowadzenia w placówce konieczności pracy w modelu zdalnym na czas trwania sytuacji kryzysowych

1. Niniejszy dokument z racji wrażliwości opisanych technik zabezpieczenia danych osobowych oraz opisu właściwych metod przetwarzania w różnych sytuacjach działania pracowników placówki ustanawia się dokumentem o klauzuli – do użytku służbowego, tym samym nie podlega udostępnieniu na podstawie wnioskowania podmiotów trzecich opartych o ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2001 Nr 112 poz.1198).
2. Określa się poniższe zasady wykorzystania dopuszczonych przez Administratora danych placówki narzędzi teleinformatycznych i oprogramowania w zależności od kontekstu i charaktery danych osobowych zawartych w przetwarzaniu pomiędzy stronami komunikacji:

KOMUNIKACJA SZKOŁA - PODMIOTY ZEWNĘTRZNE

1. Wszelką komunikację z podmiotami zewnętrznymi na czas trwania pracy w modelu zdalnym placówka realizuje przez zespół / pracownika sekretariatu z wykorzystaniem służbowego adresu poczty elektronicznej oraz dedykowanego numeru telefonu.
2. Wszelka odbierana korespondencja elektroniczna w postaci źródłowej wraz z załącznikami powinna być składowana na lokalnym dysku do wydzielonego katalogu skrzynki odbiorczej.
3. Całość korespondencji prowadzonej przez sekretariat placówki powinna być archiwizowana z użyciem mechanizmu wbudowanego w oprogramowanie stosowane do obsługi komunikacji za pomocą poczty elektronicznej.
4. Wszelka komunikacja prowadzona pomiędzy palcówką, a podmiotem zewnętrznym powinna odbywać się z dołączonym w polu „DW" adresem służbowej poczty elektronicznej Administratora danych (dyrektora)
5. Wszystkie załączane dokumenty zawierające dane osobowe przesyłane w prowadzonej korespondencji z wykorzystaniem usługi poczty elektronicznej powinny być- bezwzględnie zabezpieczone z wykorzystaniem mechanizmu szyfrowania.
6. W przypadku, kiedy użyte oprogramowanie do wytworzenia dokumentu zawierającego w swojej treści dane osobowe nie posiada wymaganej funkcjonalności szyfrowania, należy użyć przyjętego, jako standard programu 7-Zip.
7. W przypadku konieczności przenoszenia dokumentów zawierających dane osobowe między komputerami nie pracującymi w jednej sieci lokalnej – obowiązuje zasada szyfrowania całego nośnika danych z wykorzystaniem metod programowych lub sprzętowych.
8. Wartość hasła użytego w procesie szyfrowania dokumentów lub nośników zawierających dane osobowe użytych do ich przenoszenia dotycząca długości i złożoności powinna spełniać ogólne wymagania ujęte w Polityce Ochron Danych.
9. Hasło niezbędne do odszyfrowania dokumentu lub zapewnienia dostępu do zaszyfrowanego nośnika danych nie powinno nigdy być przesyłane \ przekazywane razem z zaszyfrowanym dokumentem \ nośnikiem.

10. W sprawach interpretacji poprawnego zastosowania zasad opisanych w pkt. 1.1 – 1.9 pracownik ma obowiązek komunikować się z wyznaczonym przez dyrektora placówki ASI Operacyjnym lub Inspektorem Ochrony Danych

KOMUNIKACJA NAUCZYCIEL - RODZIC

1. Wszelką komunikację z opiekunem prawnym ucznia na czas trwania pracy w modelu zdalnym wychowawca \ nauczyciel przedmiotowy realizuje z wykorzystaniem **systemu e-dziennika** oraz **służbowego adresu poczty elektronicznej** i **dedykowanego numeru telefony.**
2. Wszelka korespondencja realizowana pocztą elektroniczną w postaci źródłowej wraz z załącznikami powinna być składowana na lokalnym dysku komputera do wydzielonego katalogu skrzynki odbiorczej.
3. Całość korespondencji prowadzonej przez nauczyciela powinna być archiwizowana z użyciem mechanizmu wbudowanego w oprogramowanie stosowane do obsługi komunikacji za pomocą poczty elektronicznej.
4. Wszelka komunikacja prowadzona pomiędzy palcówką, a grupą Opiekunów powinna odbywać się z dołączonym w polu „DW" adresem służbowej poczty elektronicznej Administratora danych (dyrektora)
5. Wszelka komunikacja elektroniczna zawierająca dane osobowe prowadzona pomiędzy nauczycielem, a Opiekunem prawnym ucznia powinna odbywać się za pomocą e-dziennika wdrożonego w szkole.
6. Informacje organizacyjne oraz materiału dydaktyczne mogą być przekazywane uczniowi z wykorzystaniem obszarów dysków wirtualnych lub jako załączniki do poczty elektronicznej.
7. Wszystkie załączane dokumenty zawierające dane osobowe przesyłane w prowadzonej korespondencji z wykorzystaniem usługi poczty elektronicznej powinny być- bezwzględnie zabezpieczone z wykorzystaniem mechanizmu szyfrowania.
8. W przypadku, kiedy użyte oprogramowanie do wytworzenia dokumentu zawierającego w swojej treści dane osobowe nie posiada wymaganej funkcjonalności szyfrowania, należy użyć przyjętego, jako standard programu 7-Zip.
9. W przypadku konieczności przenoszenia dokumentów zawierających dane osobowe między komputerami nie pracującymi w jednej sieci lokalnej – obowiązuje zasada szyfrowania całego nośnika danych z wykorzystaniem metod programowych lub sprzętowych.
   9.1 Wartość hasła użytego w procesie szyfrowania dokumentów lub nośników zawierających dane osobowe użytych do ich przenoszenia dotycząca długości i złożoności powinna spełniać ogólne wymagania ujęte w Polityce Ochron Danych.
   9.2 Hasło niezbędne do odszyfrowania dokumentu lub zapewnienia dostępu do zaszyfrowanego nośnika danych nie powinno nigdy być przesyłane \ przekazywane razem z zaszyfrowanym dokumentem \ nośnikiem.
10. W sprawach interpretacji poprawnego zastosowania zasad opisanych w pkt. 1.1 – 1.9 pracownik ma obowiązek komunikować się z wyznaczonym przez dyrektora placówki ASI Operacyjnym lub Inspektorem Ochrony Danych

KOMUNIKACJA NAUCZYCIEL – NAUCZYCIEL; NAUCZYCIEL – DYREKTOR

1. Wszelką komunikację na czas pracy w modelu zdalnym pomiędzy nauczycielami oraz nauczycielem, a dyrektorem należy realizować z wykorzystaniem **systemu e-dziennika** oraz **służbowego adresu poczty elektronicznej** i **dedykowanego numeru telefonu.**
2. Komunikacja w postaci video organizowana jako forma służbowych spotkań dyrektora z pracownikami w przypadku nagrywania z użyciem wbudowanych mechanizmów platformy komunikacyjnej – powinna być przetwarzana tylko i wyłącznie w celu dokumentowania spotkania bez publikowania materiału na ogólnych serwisach społecznościowych.
3. Procedura niniejsza posiada status dokumentu otwartego – co oznacza, że jego zawartość będzie dostosowywana do zmieniającej się formy działania placówki i kontekstu przetwarzanych informacji zawierającej dane osobowe.
4. Administrator danych (dyrektor) za każdym razem kiedy nastąpi zmiana lub uszczegółowienie zakresu zasad przetwarzania – będzie informował wszystkich pracowników w sposób zapewniający bezpieczny i ujednolicony tryb przetwarzania danych w placówce.