Częstochowa 22.05.2020r.

Zarządzenie nr 44 2019/2020
Dyrektora Szkoły Podstawowej nr 27 w Częstochowie
z dnia 22.05.2020r.

w sprawie: wprowadzenia Procedury bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej w okresie epidemii COVID-19 w Szkole Podstawowej nr 27 w Częstochowie

Na podstawie rozporządzenia Ministra Edukacji Narodowej z dnia 20 marca 2020r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek (Dz.U.2020, poz. 493) zarządzam, co następuje**:**

§ 1

Wprowadzam w życie Procedurę bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej w okresie epidemii COVID-19 w Szkole Podstawowej nr 27 w Częstochowie**,** która stanowią **załącznik 1** do niniejszego zarządzenia

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia.

Dyrektor
Szkoły Podstawowej nr 27
(-) Sylwia Szczygłowska

Załącznik nr 1 do Zarządzenia nr 44 2019/2020

PROCEDURA BEZPIECZNEGO PRZETWARZANIA DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ W OKRESIE EPIDEMII COVID-19 W SZKOLE PODSTAWOWEJ NR 27 W CZĘSTOCHOWIE

Celem niniejszej procedury jest zminimalizowanie wysokiego ryzyka naruszenia praw i wolności osób, których dane osobowe są przetwarzane w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19. Procedura ta została opracowana na podstawie przeprowadzonej wcześniej analizy ryzyka (załącznik nr 1) i oceny zagrożeń (załącznik nr 2 i 3) w świetle przepisów 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 zwane w skrócie „RODO"). Załączniki nr 1,2 i 3 dostępne są do wglądu jedynie dla osób upoważnionych.

§ 1Postanowienia ogólne

1. Przetwarzanie danych osobowych w ramach pracy zdalnej następuje na podstawie pisemnego polecenia pracy zdalnej wydanego przez pracodawcę.
2. Pracownik, któremu wydano polecenie pracy zdalnej zobowiązany jest w jej trakcie do przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych oraz innymi przepisami regulujących pracę jednostki systemu oświaty, zwłaszcza z polityką bezpieczeństwa przetwarzania danych osobowych i instrukcją zarządzania systemami informatycznymi.
3. Pracownik zobowiązuje się do przetwarzania udostępnionych mu danych osobowych jedynie w celach służbowych, określonych w umowie o pracę.
4. Zabronione jest wykorzystywanie przez pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.

§ 2 Bezpieczeństwo obszaru przetwarzania

1. Pracownik zobowiązuje się zorganizować stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy.
2. Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych osobowych przetwarzanych przez niego w ramach pracy zdalnej.
3. Pracownik zobowiązany jest do zachowania poufności informacji, na przykład podczas służbowych rozmów telefonicznych lub wideokonferencji.
4. Pracownik zobowiązany jest do zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.

5. Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu lub zastosowanie filtru prywatyzującego.
6. Pracownik zobowiązany jest do stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy.
7. Po zakończeniu pracy na sprzęcie elektronicznym należy każdorazowo wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu.
8. Pracownik zobowiązuje się do bezpiecznego przechowywania danych osobowych zawartych w dokumentacji w formie papierowej, na przykład w meblach zamykanych na klucz.

§ 3 Bezpieczeństwo domowej sieci

1. Sprzęt komputerowy powinien być podłączony do zabezpieczonej, domowej sieci WiFi. Zabronione jest korzystanie z otwartych sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych czy hot-spoty w kawiarniach.
2. Dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem, którym nie jest hasło domyślne, zdefiniowane podczas pierwszej konfiguracji urządzenia.
3. Oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.
4. Możliwość konfiguracji sprzętu sieciowego z urządzeniami znajdującymi się poza siecią LAN powinna być wyłączona lub ograniczona tylko do zdefiniowanych adresów IP.
5. Zaleca się zdefiniowanie urządzeń, które mogą uzyskać dostęp do domowej sieci WiFi, na przykład z wykorzystaniem filtracji adresów MAC.

§ 4 Procedura bezpiecznego logowania

1. Dostęp do sprzętu lub programu wykorzystywanego do pracy zdalnej powinien być możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła, na przykład poprzez ustawianie PIN-u lub innej formy uwierzytelnienia.
2. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być odpowiednio długie i złożone. Nie powinno być ono zbudowane za pomocą ciągu znajdujących się obok siebie znaków na klawiaturze lub oparte na prostych skojarzeniach związanych z użytkownikiem, na przykład numer telefonu, data urodzenia, imiona lub nazwiska.
3. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być zmieniane w cyklach 30-dniowych.
4. Zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach nie gwarantujących ich poufności.
5. Zabronione jest domyślne zapamiętywanie hasła dostępu do konta użytkownika systemu na sprzęcie oraz programów wykorzystywanych w pracy zdalnej, w szczególności dziennika elektronicznego i platform wykorzystywanych w kształceniu na odległość.

§ 5 Bezpieczne korzystanie z programów i platform wykorzystywanych w pracy zdalnej (w tym wideokonferencji)

1. Użycie w pracy zdalnej danego programu/platformy wymaga pisemnej zgody pracodawcy.
2. W przypadku udostępniania danych osobowych w programach/platformach wykorzystywanych w pracy zdalnej Administrator danych zobowiązany jest do zawarcia umowy powierzenia przetwarzania danych osobowych. Umowa ta ma zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie spełniało wymogi wskazane w RODO i chroniło prawa osób, których dane dotyczą.
3. Programy/platformy w przypadku, których nie ma możliwości zawarcia umowy powierzenia przetwarzania danych osobowych nie mogą być wykorzystywane do przetwarzania danych osobowych.
4. W pracy zdalnej zalecane jest korzystanie z aplikacji webowych, nie desktopowych.
5. Przed rozpoczęciem korzystania z programu/platformy wykorzystywanej do pracy zdalnej pracownik zobowiązany jest do zapoznania się z ogólnymi warunkami jej użytkowania oraz polityką prywatności.
6. W przypadku korzystania z programów z funkcją wideokonferencji zaleca się wyłączenie opcji nagrywania i przechowywania.
7. Przy podłączaniu się do programu z funkcją telekonferencji zalecane jest korzystanie z kodów dostępu/PIN-ów.
8. Przed rozpoczęciem korzystania z programów z funkcją telekonferencji zalecane jest przeskanowanie ich systemem antywirusowym lub antymalwareowym.
9. W trakcie korzystania z programów lub platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych (zasada minimalizacji danych).
10. W przypadku kiedy pracownikowi został przydzielony służbowy adres e-mail zabronione jest korzystanie przez niego z prywatnego adresu e-mail do celów służbowych.
11. Zabrania się udostępniania dokumentów służbowych, za pomocą publicznego czatu lub innych komunikatorów.
12. Zabrania się udostępniania w mediach społecznościowych linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej.
13. Zaleca się udostępnianie linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej, na przykład poprzez wskazany adres e-mail lub dziennik elektroniczny.
14. Należy korzystać z opcji „poczekalnia” tak, aby kontrolować uczestników telekonferencji, w celu uniknięcia przypadkowych lub niechcianych osób.

§ 6 Bezpieczne przechowywanie danych

1. Nośniki urządzeń mobilnych wykorzystywane w celach służbowych, w tym komputer, telefon lub tablet powinny być zaszyfrowane, na przykład za pomocą hasła.

2. Zewnętrzne karty pamięci, a także inne nośniki danych, takie jak pendrive lub dysk zewnętrzny, wykorzystywane w celach służbowych powinny być szyfrowane, na przykład za pomocą hasła.
3. Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci. W przypadku nauczycieli mogą oni jedynie publikować tam materiały edukacyjne, natomiast nie mogą przetwarzać danych osobowych uczniów i ich rodziców.

§ 7 Ochrona przed cyberatakami

1. Sprzęt wykorzystywany do pracy zdalnej musi być wyposażony w uruchomione i zaktualizowane oprogramowanie antywirusowe.
2. Systemy, w tym system operacyjny wykorzystywany do pracy zdalnej musi być regularnie aktualizowany.
3. Komputer wykorzystywany do pracy zdalnej musi mieć uruchomioną zaporę sieciową.

§ 8 Procedury bezpieczeństwa podczas pracy zdalnej

1. Zabrania się samodzielnej lub z wykorzystaniem wsparcia podmiotów zewnętrznych naprawy sprzętu wykorzystywanego do pracy zdalnej. W celu naprawy uszkodzonego sprzętu należy bezzwłocznie zwrócić go pracodawcy.
2. Zabrania się drukowania dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów czy osób trzecich.
3. Komunikacja z uczniami, rodzicami i innymi klientami jednostki systemu oświaty powinna być prowadzona przede wszystkim za pośrednictwem wdrożonych rozwiązań teleinformatycznych, na przykład poprzez dziennik elektroniczny.
4. Pracownik zobowiązany jest do weryfikowania nadawców wiadomości e-mailowych oraz w przypadku wątpliwości do nieotwierania załączników oraz hiperłączy znajdujących się w tekście.
5. Podczas wysyłania korespondencji zbiorczej należy korzystać z opcji „kopia ukryta” (pole UDW – Ukryci Do Wiadomości lub BCC – Blind Carbon Copy), dzięki której odbiorcy wiadomości nie zobaczą wzajemnie swoich adresów e-mail.
6. Pracownik zobowiązany jest do szyfrowania wiadomości e-mailowych zawierających dane osobowe i przekazywania hasła zawsze inną formą, na przykład telefonicznie.
7. Zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne konta e-mailowe.
8. Zabrania się włączać opcję autouzupełniania formularzy w opcjach przeglądarki internetowej.
9. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki „kłódka”. W tej sytuacji należy „kliknąć” na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

§ 9 Dodatkowe zalecenia do pracy zdalnej na prywatnym sprzęcie komputerowym

1. Zalecane jest stworzenie oddzielnego konta użytkownika systemu w pracy na prywatnym sprzęcie, wykorzystywanym do pracy zdalnej. Konto użytkownika powinno posiadać ograniczone uprawnienia i być chronione silnym hasłem oraz nie udostępniane osobom trzecim.
2. Za legalność oprogramowania, w tym programu antywirusowego odpowiada właściciel sprzętu.
3. Po zakończeniu okresu pracy poza miejscem jej stałego wykonywania pracownik jest zobowiązany bezzwłocznie przekazać pracodawcy wszystkie dane zapisane na prywatnym sprzęcie (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi, a następnie usunąć je w sposób trwały.

§ 10 Bezpieczne przetwarzanie danych osobowych zawartych w dokumentacji papierowej podczas pracy zdalnej

1. Dokumentacja papierowa zawierająca dane osobowe udostępniana jest pracownikowi w zakresie niezbędnym do realizacji obowiązków służbowych w zakresie pracy zdalnej, za zgodą pracodawcy.
2. Pracodawca zapewnia ewidencjonowanie wydanych pracownikom dokumentów zawierających dane osobowe.
3. Pracownik zobowiązany jest przechowywać udostępnione dokumenty papierowe przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (zasada ograniczenia przetwarzania). Po tym czasie zobowiązany jest niezwłocznie zwrócić je pracodawcy.
4. Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia dokumentów w taki sposób, aby były niewidoczne dla osób trzecich, na przykład w zabezpieczonej teczce.
5. Pracownik zobowiązany jest do bezpiecznego niszczenia dokumentów papierowych, na przykład za pomocą niszczarki do dokumentów. Jeżeli pracownik nie posiada niszczarki dokumentów, powinien dokumenty zabezpieczyć, a po zakończeniu pracy zdalnej niezwłocznie zniszczyć je w siedzibie pracodawcy.
6. Zabrania się pracownikowi wyrzucania papierowych dokumentów służbowych do domowego kosza na śmieci.

§ 11 Naruszenie ochrony danych osobowych podczas pracy zdalnej

1. Pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym lub w systemie tradycyjnym, zobowiązany jest do niezwłocznego pisemnego poinformowania o tym administratora danych – pracodawcę (załącznik nr 4).
2. W przypadku powzięcia informacji o naruszeniu ochrony danych osobowych Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:
   a. ustala zakres i przyczyny naruszenia ochrony danych osobowych oraz jego ewentualne skutki;

b. informuje i konsultuje tok postępowania z Inspektorem Ochrony Danych;
c. podejmuje działania prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

3. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu – Urząd Ochrony Danych Osobowych oraz w pewnych przypadkach powiadamia osoby, których dane dotyczą.
4. Jeżeli przyczyną naruszenia zasad ochrony danych osobowych było zaniedbanie ze strony pracownika, administrator może wyciągnąć konsekwencje dyscyplinarne wynikające z regulaminu pracy.

Zabrania się świadomego lub nieumyślnego wywoływania naruszeń przez osoby upoważnione do przetwarzania danych.

Załącznik nr 2 do procedury bezpiecznego przetwarzanie danych osobowych podczas pracy zdalnej w okresie epidemii COVID-19

KARTA OCENY SKUTÓW PRZETWARZANIA DANYCH OSOBOWYCH (PIA)

1. INFORMACJA O ADMINISTRATORZE DANYCH

1.1. Administrator danych:
Nazwa Administratora: Szkoła Podstawowa nr 27
Adres: ul. Rozdolna 5, 42-202 Częstochowa
REGON:000713958, NIP: 9491864185
tel. +48 34 3617139
e-mail: sp27@edukacja.czestochowa.pl

1.2. Inspektor Ochrony Danych: Justyna Sprycha

2. INFORMACJE O PROCESIE OCENY

2.1 Numer karty oceny: 01
2.2 Podstawa wykonania oceny: art. 35 ust.1 RODO
2.3 Data oceny: 18.05.2020 r.
2.4 Wersja oceny: 1.1
2.5 Ocenę skutków (PIA) wykonał: Sylwia Szczygłowska
2.6 PIA monitorował: Justyna Sprycha

3. KONTEKST OCENY

3.1 **Czynność przetwarzania**: Wykorzystanie platform edukacyjnych do nauki zdalnej
3.2 **Osoby/komórki odpowiedzialne**: dyrektor placówki
3.3 **Własność procesu:** czynność własna
3.4 **Zakres danych osobowych w czynności**: utrwalenie, organizowanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, przesyłanie, udostępnianie, usuwanie lub niszczenie danych osobowych za pomocą programów/platform wykorzystywanych do kształcenia na odległość informacji o uczniach, ich rodzicach i pracownikach, między innymi imię, nazwisko, data i miejsce urodzenia, dane teleadresowe, PESEL, informacje dotyczące sytuacji zdrowotnej/prawnej/rodzinnej, dane dotyczące przekonania religijnego, informacje o rozwoju psychofizycznym i postępach edukacyjnych ucznia, frekwencji na zajęciach,

wizerunek oraz inne dane osobowe wymagane przepisami prawa, czasie pracy w systemach informatycznych i odwiedzanych stronach internetowych.

3.5 **Krótki opis funkcjonalny**: nauka zdalna realizowana jest poprzez:

a. platformy/ programy, w których jednostka systemu oświaty jest administratorem danych, w tym przypadku zawarta jest umowa powierzenia przetwarzania danych osobowych z dostawcą usług;

b. platformy/ programy wykorzystywane do nauki zdalnej, w których jednostka systemu oświaty nie jest administratorem danych – w tym przypadku platformy/ programy wymagają samodzielnego założenia konta przez rodzica/ucznia. Placówka oświatowa nie ma wpływu na zakres udostępnionych danych osobowych i nie odpowiada za poziom zabezpieczeń. Administratorem danych są właściciele platform/ programów. Rodzic/ uczeń akceptuje we własnym zakresie polityki prywatności i regulaminy platform/programów. Jednostka systemu oświaty rekomenduje używanie danej platformy/ programu poprzez, na przykład przesłanie linku do „wirtualnego pokoju". Niekiedy przesyła jedynie link do danego programu/platformy i nie wymaga założenia konta na wskazanej platformie – mimo to rodzic/uczeń może zrobić to samodzielnie.

4. WYMAGANIA DOTYCZĄCE CZYNNOŚCI PRZETWARZANIA

4.1 **Cel przetwarzania danych**: realizacja obowiązku nauki w formie zdalnej

4.2 **Podstawa prawna**:

a. Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2019 r. poz. 1148 z późn. zm.);

b. Ustawa 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. 2020 poz. 374 z późn. zm.)

c. Rozporządzenie Ministra Edukacji Narodowej z dnia 11 marca 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. 2020 poz. 410 z późn. zm.)

d. Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczegółowych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. 2020 poz. 493 z późn. zm.)

e. Art. 6 ust. 1 lit e RODO - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

4.3 **ADEKWATNOŚĆ ZBIERANYCH DANYCH W STOSUNKU DO CELU**

a. w przypadku platform/programów, w których jednostka systemu oświaty jest administratorem danych: zbierane dane są adekwatne do celu;

b. w przypadku platform/programów, w których jednostka systemu oświaty nie jest administratorem danych: brak wpływu na zakres danych osobowych udostępnionych przez ucznia/rodzica.

4.4 **PRAWIDŁOWOŚĆ ZBIERANYCH DANYCH**

Dane osobowe aktualizowane są w sposób ciągły, automatycznie przy użyciu systemu informatycznego.

4.5 **OKRES RETENCJI DANYCH**

Dane osobowe przechowywane są zgodnie z przepisami prawa:

a. dziennik elektroniczny, zgodnie z Jednolitym Rzeczowym Wykazem Akt;
b. platformy/programy wykorzystane do nauki zdalnej, na czas kształcenia na odległość (rozporządzenie MEN).

4.6 **ZASADY POWIERZENIA DANYCH:**

a. w przypadku platform/programów, w których jednostka systemu oświaty jest administratorem danych zawierana jest umowa powierzenia przetwarzania danych osobowych;
b. w przypadku platform/programów, w których jednostka systemu oświaty nie jest administratorem danych: uczeń/rodzic samodzielnie akceptuje politykę prywatności i regulamin.

4.7 **PRZETWARZANIA DANYCH POZA UE**

Dane osobowe przekazywane są poza UE.

4.8 **Opis spełnienia obowiązku informacyjnego**

Klauzula informacyjna została rozesłana poprzez dziennik elektroniczny.

4.9 **OPIS ZBIERANIA ZGODY**

Zgoda nie jest pobierana.

4.10 **OPIS SPOSOBU REALIZACJI PRAW**

a. W przypadku platform/programów, w których jednostka systemu oświaty jest administratorem danych pracownik/ uczeń/ rodzic może dochodzić swoich praw poprzez wystąpienie z wnioskiem do administratora danych. W procesie przetwarzania pracownik posiada następujące prawa:
   - prawo do bycia poinformowanym – realizowane,
   - prawo dostępu do danych – realizowane na żądanie,
   - prawo sprostowania - realizowane na żądanie,
   - prawo do usunięcia - realizowane na żądanie,
   - prawo do sprzeciwu - realizowane na żądanie,
   - prawo do ograniczenia - realizowane na żądanie.
b. W przypadku platform/programów, w których jednostka systemu oświaty nie jest administratorem danych nie ma możliwości realizacji praw osób, których dane dotyczą – pracowników, uczniów i ich rodziców.

5. IDENTYFIKACJA ZAGROŻEŃ O WYSOKIM POZIOMIE RYZYKA NARUSZENIA

Tabela 1. Zagrożenia o wysokim poziomie ryzyka naruszenia praw lub wolności osób, których dane dotyczą

IDENTYFIKACJA AKTYWÓW				RYZYKO I SZACOWANIE	
Grupa aktywa	**Waga aktywa**	**Aktywo**	**Właściciel aktywa (ryzyka)**	**Zagrożenie**	**Poziom ryzyka**
Ludzie	**4**	Pracownicy administratora	**Administrator danych**	błędy ludzkie spowodowane np. nieuwagą lub zmęczeniem	Ryzyko wysokie
	4			niezgłoszenie administratorowi danych naruszenia ochrony danych osobowych	Ryzyko wysokie
	4	Platformy edukacyjne (wymagające samodzielnego założenia konta przez rodzica/ ucznia)		wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą wynikające z braku możliwości zarządzania danymi osobowymi udostępnianymi na platformach edukacyjnych	Ryzyko wysokie
Wykonawcy	**3**	Platformy edukacyjne (z którymi zawarta jest Umowa powierzenia)		brak umów powierzenia z wykonawcami gwarantujących prawidłowe przetwarzanie danych	Ryzyko wysokie

6. WPŁYW NA OSOBY, KTÓRE DANE DOTYCZĄ

6.1 Identyfikacja ryzyka

Główne zagrożenia dla osób zgodnie z zagrożeniami wskazanymi w tabeli nr 1:

a. utrata poufności,

b. utrata integralności,
c. dostępność danych.

7. Opis skutków

7.1 **Główne skutki dla osób, których dane dotyczą przy materializacji ryzyka**:

a. kradzież lub fałszowanie tożsamości,
b. utrata reputacji,
c. cyberprzemoc,
d. straty materialne,
e. zwiększenie niepożądanej korespondencji e-mail,
f. utrata kontroli nad danymi,
g. ograniczenie możliwości realizacji praw,
h. dyskryminacja.

7.2 **Ocena niezbędności i proporcji**

Charakter przetwarzanych danych osobowych, kary finansowe oraz straty wizerunkowe grożące Administratorowi z tytułu utraty poufności, integralności i dostępności informacji powodują, że stosowane zabezpieczenia ochrony danych osobowych nie są wystarczające. Dlatego wymagane jest wprowadzenie działań minimalizujących ryzyko naruszenia praw i wolności osób, których dane dotyczą.

8. Ocena skutków

8.1 **Stosowane zabezpieczenia minimalizujące ryzyko:**

a. środki techniczne i organizacyjne zgodne z polityką bezpieczeństwa ochrony danych osobowych i instrukcją zarządzania systemami informatycznymi,
b. umowy powierzenia przetwarzania danych osobowych.

9. Planowane działania

9.1 **Planowane do wdrożenia zabezpieczenia minimalizujące ryzyko:**

a. wprowadzenie procedury przetwarzania danych osobowych podczas pracy zdalnej;
b. ograniczenie przetwarzania danych osobowych w przypadku platform/programów, w których jednostka systemu nie jest administratorem danych;
c. szkolenia dla nauczycieli z zasad przetwarzania danych osobowych podczas pracy zdalnej,
d. przygotowanie instrukcji korzystania z platform/programów wykorzystywanych do nauki zdalnej dla uczniów/rodziców przez wyznaczonego pracownika administratora danych.

10. OCENA ZAGROŻEŃ

Tabela 2. Ocena zagrożeń

IDENTYFIKACJA AKTYWÓW		**RYZYKO I SZACOWANIE**				
Grupa aktywa	**Aktywo**	*Zagrożenie*	*Prawdopod.*	*Skutek*	***Ryzyko***	***Poziom Ryzyka***
Ludzie	Pracownicy administratora	błędy ludzkie spowodowane np. nieuwagą lub zmęczeniem	3	1	**12**	Ryzyko wysokie
		niezgłoszenie administratorowi danych naruszenia ochrony danych osobowych	3	1	**12**	Ryzyko wysokie
	Platformy edukacyjne (wymagające samodzielnego założenia konta przez rodzica/ ucznia)	wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą wynikające z braku możliwości zarządzania danymi osobowymi udostępnianymi na platformach edukacyjnych	4	1	**16**	Ryzyko wysokie
Wykonawcy	Platformy edukacyjne (z którymi zawarta jest Umowa powierzenia)	brak umów powierzenia z wykonawcami gwarantujących prawidłowe przetwarzanie danych	4	1	**12**	Ryzyko wysokie

11. Ocena działań

Ze względu na sytuację epidemiologiczną jednostka systemu oświaty nie miała możliwości przygotowania niezbędnej infrastruktury i dokumentacji odnośnie programów/platform wykorzystywanych do kształcenia na odległość. Nowe przepisy dotyczące realizacji zajęć przedszkolnych/szkolnych w formie pracy zdalnej dają szeroką możliwość realizowania przez nauczycieli zajęć z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu kształcenia, w tym z wykorzystaniem środków komunikacji elektronicznej. Pozostawiają zatem jednostkom systemu oświaty dużą swobodę odnośnie wyboru

właściwego narzędzia przy uwzględnieniu wszystkich aspektów związanych z możliwościami placówki, nauczycieli, a przede wszystkim, biorąc pod uwagę możliwości techniczne i organizacyjne rodziców i uczniów. Wobec powyższego do nauki zdalnej wykorzystywane są nie tylko bezpieczne programy/platformy. Dlatego w opinii Administratora danych zachodzi wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, w szczególności w przypadku programów/platform, w których placówka oświatowa nie jest administratorem danych – nie ma kontroli nad udostępnionymi danymi osobowymi.
Dlatego też, na dzień analizy zostały zaplanowane działania zaradcze przedstawione w pkt. 9.

…….
Data, podpis i pieczęć Administratora Danych

Załącznik nr 3 do procedury bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej w okresie epidemii COVID-19

KARTA OCENY SKUTÓW PRZETWARZANIA DANYCH OSOBOWYCH (PIA)

1. INFORMACJA O ADMINISTRATORZE DANYCH

1.3. Administrator danych:
Nazwa Administratora: Szkoła Podstawowa nr 27
Adres: ul. Rozdolna 5, 42-202 Częstochowa
REGON: 000713958, NIP: 9491864185
tel. +48 34 3617139
e-mail: sp27@edukacja.czestochowa.pl

1.4. Inspektor Ochrony Danych: Justyna Sprycha

2. INFORMACJE O PROCESIE OCENY

2.1 Numer karty oceny: 02

2.2 Podstawa wykonania oceny: art. 35 ust.1 RODO

2.3 Data oceny: 18.05.2020 r.

2.4 Wersja oceny: 2.1

2.5 Ocenę skutków (PIA) wykonał: Sylwia Szczygłowska

2.6 PIA monitorował: Justyna Sprycha

3. KONTEKST OCENY

3.1 **Czynność przetwarzania**: praca zdalna poza siedzibą administratora danych

3.2 **Osoby/komórki odpowiedzialne**: dyrektor placówki

3.3 **Własność procesu:** czynność własna

3.4 **Zakres danych osobowych w czynności**: utrwalenie, organizowanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, przesyłanie, udostępnianie, usuwanie lub niszczenie danych osobowych za pomocą programów/platform wykorzystywanych do pracy zdalnej i przetwarzanych informacji o uczniach, ich rodzicach oraz pracownikach, między innymi imię, nazwisko, data i miejsce urodzenia, dane teleadresowe, PESEL, informacje dotyczące sytuacji zdrowotnej/prawnej/rodzinnej, dane dotyczące przekonania religijnego, informacje o rozwoju psychofizycznym i postępach edukacyjnych ucznia, frekwencji na zajęciach, wizerunek oraz inne dane osobowe wymagane przepisami prawa, czasie pracy w systemach informatycznych i odwiedzanych stornach internetowych.

3.5 **Krótki opis funkcjonalny**: praca realizowana jest poprzez:

c. platformy/ programy (w tym poczta elektroniczna), w których placówka oświatowa jest administratorem danych, w tym przypadku zawarta jest umowa powierzenia przetwarzania danych osobowych z dostawcą usług;

d. prywatne platformy/ programy (w tym poczta elektroniczna) wykorzystywane do pracy zdalnej – jednostka systemu oświaty nie ma wpływu na zakres udostępnionych danych osobowych i nie odpowiada za poziom zabezpieczeń. Administratorem danych

są właściciele platform/ programów. Pracownik akceptuje we własnym zakresie polityki prywatności i regulaminy platform/programów.

e. dokumentacja papierowa – pracownicy, którzy otrzymali polecenie pracy zdalnej mają możliwość wyniesienia, korzystania i opracowywania dokumentacji papierowej niezbędnej do realizacji obowiązków służbowych.

4. WYMAGANIA DOTYCZĄCE CZYNNOŚCI PRZETWARZANIA

4.1 **Cel przetwarzania danych**: realizacja obowiązków służbowych w ramach pracy zdalnej

4.2 **Podstawa prawna**:

f. Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2019 r. poz. 1148 z późn. zm.)

g. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 1974 Nr 24 poz. 141 z późn. zm.)

h. Ustawa 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. 2020 poz. 374 z późn. zm.)

i. Rozporządzenie Ministra Edukacji Narodowej z dnia 11 marca 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. 2020 poz. 410 z późn. zm.)

j. Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczegółowych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. 2020 poz. 493 z późn. zm.)

k. Art. 6 ust. 1 lit e RODO - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

4.3 **Adekwatność zbieranych danych w stosunku do celu**

c. W przypadku platform/programów, w których placówka oświatowa jest administratorem danych: zbierane dane są adekwatne do celu.

d. W przypadku prywatnych platform/ programów: brak wpływu na zakres udostępnionych danych osobowych.

e. W przypadku dokumentacji papierowej: zbierane dane są adekwatne do celu.

4.4 **Prawidłowość zbieranych danych**

a. Pracownicy przetwarzają dane osobowe zawarte w dokumentacji papierowej i elektronicznej poza siedzibą Administratora danych na podstawie polecenia pracy zdalnej.

b. Pracownicy posiadają upoważnienie do przetwarzania danych osobowych adekwatne do zajmowanego stanowiska pracy.

c. Dane osobowe aktualizowane są automatycznie, w sposób ciągły przy użyciu systemu informatycznego.

d. Używanie nowych platform/programów przez pracowników wymaga zgody Administratora danych.
e. Dane osobowe przetwarzane w formie papierowej są ograniczone.

4.5 **Okres retencji danych**

Dane osobowe przechowywane są zgodnie z przepisami prawa:

c. Jednolitym Rzeczowym Wykazem Akt;
d. platformy/programy wykorzystany do pracy zdalnej, na czas pracy zdalnej (rozporządzenie MEN).

4.6 Z**asady powierzenia danych**:

c. w przypadku platform/programów, w których jednostka systemu oświaty jest administratorem danych zawierana jest umowa powierzenia przetwarzania danych osobowych;
d. w przypadku platform/programów, w których jednostka systemu oświaty nie jest administratorem danych: pracownik samodzielnie akceptuje politykę prywatności i regulamin.

4.7 **Przetwarzania danych poza UE**

Dane osobowe przekazywane są poza UE.

4.8 **Opis spełnienia obowiązku informacyjnego**

Klauzula informacyjna dla pracowników do umowy o pracę (akta osobowe). Ponadto w poleceniu pracy zdalnej zawarte są podstawy prawne przetwarzania danych w czasie epidemii COVID- 19.

4.9 **Opis zbierania zgody**

Zgoda nie jest pobierana.

4.10 **Opis sposobu realizacji praw**

c. W przypadku platform/programów, w których jednostka systemu oświaty jest administratorem danych osoby oraz dokumentacji papierowej – osoby, których dane dotyczą mogą dochodzić swoich praw poprzez wystąpienie z wnioskiem do administratora danych.

d. W procesie przetwarzania posiadają następujące prawa:

- prawo do bycia poinformowanym – realizowane,
- prawo dostępu do danych – realizowane na żądanie,
- prawo sprostowania - realizowane na żądanie,
- prawo do usunięcia - realizowane na żądanie,
- prawo do sprzeciwu - realizowane na żądanie,
- prawo do ograniczenia - realizowane na żądanie.

e. W przypadku platform/programów (w tym prywatna poczta elektroniczna pracownika), w których jednostka systemu oświaty nie jest administratorem danych nie ma możliwości realizacji praw osób, których dane dotyczą.

5. IDENTYFIKACJA ZAGROŻEŃ O WYSOKIM POZIOMIE RYZYKA NARUSZENIA

Tabela 1. Zagrożenia o wysokim poziomie ryzyka naruszenia praw lub wolności osób, których dane dotyczą

IDENTYFIKACJA AKTYWÓW				RYZYKO I SZACOWANIE	
Grupa aktywa	**Waga aktywa**	**Aktywo**	**Właściciel aktywa (ryzyka)**	*Zagrożenie*	***Poziom Ryzyka***
Ludzie	**4**	Pracownicy administratora	**Administrator danych**	błędy ludzkie spowodowane np. nieuwagą lub zmęczeniem	Ryzyko wysokie
	4			niewykorzystywanie/ brak służbowej poczty elektronicznej do pracy zdalnej	Ryzyko wysokie
	4			brak/nieznajomość procedur pracy zdalnej	Ryzyko wysokie
	4			nieuprawniony dostęp do danych osobowych	Ryzyko wysokie
	4			używanie tych samych haseł/ zapamiętywanie ich w różnych systemach informatycznych	Ryzyko wysokie
	4			brak szkolenia z zakresu pracy zdalnej	Ryzyko wysokie
	4			niewylogowanie się z programów/ systemów informatycznych	Ryzyko wysokie
	4			nieprawidłowe zabezpieczenie sprzętu przed kradzieżą, uszkodzeniem lub zniszczeniem	Ryzyko wysokie
	4			niezgłoszenie administratorowi danych naruszenia ochrony danych osobowych	Ryzyko wysokie
Oprogramowanie	**3**	Programy/ platformy wykorzystywane do pracy zdalnej		przypadkowa lub niezgodna z prawem utrata danych osobowych	Ryzyko wysokie

IDENTYFIKACJA AKTYWÓW				RYZYKO I SZACOWANIE	
Grupa aktywa	**Waga aktywa**	**Aktywo**	**Właściciel aktywa (ryzyka)**	*Zagrożenie*	***Poziom Ryzyka***
Urządzenia	**4**	Prywatny sprzęt: laptop, komputer, telefon, tablet, itp.		brak zabezpieczeń urządzenia/plików zawierających dane osobowe	Ryzyko wysokie
	4			współdzielenie sprzętu z wieloma osobami	Ryzyko wysokie
	4			ujawnienie danych osobom nieupoważnionym (min. poprzez wgląd)	Ryzyko wysokie
	4			korzystanie z nielicencjonowanego oprogramowania, brak aktualizacji	Ryzyko wysokie
	4			wykorzystywanie sprzętu nie tylko do celów służbowych	Ryzyko wysokie
	4			nieprzestrzeganie / brak znajomości zasad korzystania z prywatnego sprzętu w celach służbowych ustalanych z pracodawcą	Ryzyko wysokie
Informacje	**3**	Dokumentacja papierowa		brak zabezpieczeń danych osobowych w miejscu wykonywania pracy zdalnej, np. pozostawienie dokumentów w niezabezpieczonej lokalizacji, umożliwienie wglądu osobom trzecim	Ryzyko wysokie
	3			brak ewidencji wydanych pracownikom dokumentów zawierających dane osobowe	Ryzyko wysokie
	3			niewłaściwe brakowanie dokumentacji, np. wyrzucenie do kosza, nie	Ryzyko wysokie

IDENTYFIKACJA AKTYWÓW				RYZYKO I SZACOWANIE	
Grupa aktywa	**Waga aktywa**	**Aktywo**	**Właściciel aktywa (ryzyka)**		
				Zagrożenie	***Poziom Ryzyka***
				użycie niszczarki do dokumentów	
	3	Dokumentacja elektroniczna		brak zabezpieczeń danych osobowych w miejscu wykonywania pracy zdalnej, np. brak haseł dostępu do plików/dysków/komputera	Ryzyko wysokie
	3			niewłaściwe brakowanie dokumentacji	
Wykonawcy	**3**	Platformy/programy do pracy zdalnej		brak umów powierzenia z wykonawcami gwarantujących prawidłowe przetwarzanie danych	Ryzyko wysokie

6. WPŁYW NA OSOBY, KTÓRYCH DANE DOTYCZĄ

6.1 **Identyfikacja ryzyka**

Główne zagrożenia dla osób zgodnie z zagrożeniami wskazanymi w tabeli nr 1.:

d. utrata poufności,
e. utrata integralności,
f. dostępność danych.

7. OPIS SKUTKÓW

7.1 **Główne skutki dla osób, których dane dotyczą przy materializacji ryzyka**:

i. kradzież lub fałszowanie tożsamości,
j. utrata reputacji,
k. cyberprzemoc,
l. straty materialne,
m. zwiększenie niepożądanej korespondencji e-mail,
n. utrata kontroli nad danymi,
o. ograniczenie możliwości realizacji praw,
p. dyskryminacja.

7.2 **Ocena niezbędności i proporcji**

Charakter przetwarzanych danych osobowych, kary finansowej oraz straty wizerunkowe grożące Administratorowi z tytułu utraty poufności, integralności i dostępności informacji powodują, że stosowane zabezpieczenia ochrony danych osobowych nie są wystarczające.

Dlatego wymagane jest wprowadzenie działań minimalizujących ryzyko naruszenia praw i wolności osób, których dane dotyczą.

8. OCENA SKUTKÓW

8.1 **Stosowane zabezpieczenia minimalizujące ryzyko:**

c. środki techniczne i organizacyjne zgodne z polityką bezpieczeństwa ochrony danych osobowych i instrukcją zarządzania systemami informatycznymi,

d. umowy powierzenia przetwarzania danych osobowych.

9. PLANOWANE DZIAŁANIA

9.1 **Planowane do wdrożenia zabezpieczenia minimalizujące ryzyko:**

e. wprowadzenie procedury przetwarzania danych osobowych podczas pracy zdalnej;

f. ograniczenie przetwarzania danych osobowych w przypadku platform/programów, w których jednostka systemu oświaty nie jest administratorem danych;

g. szkolenia dla pracowników z zasad bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej.

10. OCENA ZAGROŻEŃ

Tabela 2. Ocena zagrożeń

IDENTYFIKACJA AKTYWÓW		**RYZYKO I SZACOWANIE**				
Grupa aktywa	**Aktywo**	*Zagrożenie*	*Prawdopod.*	*Skutek*	***Ryzyko***	***Poziom Ryzyka***
Ludzie	Pracownicy administratora	błędy ludzkie spowodowane np. nieuwagą lub zmęczeniem	3	1	**12**	Ryzyko wysokie
		niewykorzystywanie/ brak służbowej poczty elektronicznej do pracy zdalnej	3	1	**12**	Ryzyko wysokie
		brak/nieznajomość procedur pracy zdalnej	4	1	**16**	Ryzyko wysokie
		nieuprawniony dostęp do danych osobowych	3	1	**12**	Ryzyko wysokie
		używanie tych samych haseł/ zapamiętywanie ich w różnych systemach informatycznych	3	1	**12**	Ryzyko wysokie
		brak szkolenia z zakresu pracy zdalnej	4	1	**16**	Ryzyko wysokie
		niewylogowanie się z programów/ systemów informatycznych	3	1	**12**	Ryzyko wysokie
		nieprawidłowe	3	1	**12**	Ryzyko

IDENTYFIKACJA AKTYWÓW		RYZYKO I SZACOWANIE				
Grupa aktywa	**Aktywo**	*Zagrożenie*	*Prawdopod.*	*Skutek*	***Ryzyko***	***Poziom Ryzyka***
		zabezpieczenie sprzętu przed kradzieżą, uszkodzeniem lub zniszczeniem				wysokie
		niezgłoszenie administratorowi danych naruszenia ochrony danych osobowych	3	1	**12**	Ryzyko wysokie
Oprogramowanie	Programy/ platformy wykorzystywane do pracy zdalnej	przypadkowa lub niezgodna z prawem utrata danych osobowych	4	1	**12**	Ryzyko wysokie
Urządzenia	Prywatny sprzęt: laptop, komputer, telefon, tablet, itp.	brak zabezpieczeń urządzenia/plików zawierających dane osobowe	4	1	**16**	Ryzyko wysokie
		współdzielenie sprzętu z wieloma osobami	4	1	**16**	Ryzyko wysokie
		ujawnienie danych osobom nieupoważnionym (min. poprzez wgląd)	3	1	**12**	Ryzyko wysokie
		korzystanie z nielicencjonowanego oprogramowania, brak aktualizacji	3	1	**12**	Ryzyko wysokie
		wykorzystywanie sprzętu nie tylko do celów służbowych	4	1	**16**	Ryzyko wysokie
		nieprzestrzeganie / brak znajomości zasad korzystania z prywatnego sprzętu w celach służbowych ustalnych z pracodawcą	3	1	**12**	Ryzyko wysokie
Informacje	Dokumentacja papierowa	brak zabezpieczeń danych osobowych w miejscu wykonywania	4	1	**12**	Ryzyko wysokie

IDENTYFIKACJA AKTYWÓW		RYZYKO I SZACOWANIE				
Grupa aktywa	**Aktywo**	*Zagrożenie*	*Prawdopod.*	*Skutek*	***Ryzyko***	***Poziom Ryzyka***
		pracy zdalnej, np. pozostawienie dokumentów w niezabezpieczonej lokalizacji, umożliwienie wglądu osobom trzecim				
		brak ewidencji wydanych pracownikom dokumentów zawierających dane osobowe	4	1	**12**	Ryzyko wysokie
		niewłaściwe brakowanie dokumentacji, np. wyrzucenie do kosza, nie użycie niszczarki do dokumentów	4	1	**12**	Ryzyko wysokie
	Dokumentacja elektroniczna	brak zabezpieczeń danych osobowych w miejscu wykonywania pracy zdalnej, np. brak haseł dostępu do plików/dysków/komputera	4	1	**12**	Ryzyko wysokie
		niewłaściwe brakowanie dokumentacji	4	1	**12**	Ryzyko wysokie
Wykonawcy	Platformy/programy do pracy zdalnej	brak umów powierzenia z wykonawcami gwarantujących prawidłowe przetwarzanie danych	4	1	**12**	Ryzyko wysokie

11. OCENA DZIAŁAŃ

Ze względu na sytuację epidemiologiczną jednostka systemu oświaty nie miała możliwości przygotowania niezbędnej infrastruktury i dokumentacji w zakresie bezpiecznego przetwarzania danych osobowych zawartej w dokumentacji papierowej oraz elektronicznej podczas pracy zdalnej. Szczególnie nowe przepisy dotyczące realizacji zajęć przedszkolnych/szkolnych w formie pracy zdalnej dają szeroką możliwość realizowania przez nauczycieli zajęć z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu kształcenia, w tym z wykorzystaniem środków komunikacji elektronicznej.

Pozostawiają zatem jednostkom systemu oświaty dużą swobodę odnośnie wyboru właściwego narzędzia przy uwzględnieniu wszystkich aspektów związanych z możliwościami placówki, nauczycieli, a przede wszystkim, biorąc pod uwagę możliwości techniczne i organizacyjne rodziców i uczniów. Dlatego do pracy zdalnej nie są wykorzystywane wyłącznie służbowe programy/platformy (w tym prywatna poczta e-mail) i sprzęty, np. laptopy. Wobec powyższego w opinii Administratora danych zachodzi wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, w szczególności w przypadku:

- programów/platform, w których jednostka systemu oświaty nie jest administratorem danych (prywatne adresy e-mail, komunikatory typu Messenger lub WhatsApp);
- prywatnego sprzętu pracownika, na przykład laptopa;
- przetwarzania danych osobowych w lokalizacji zewnętrznej, którym jest mieszkanie pracownika.

W związku z powyższym nie ma kontroli nad danymi osobowymi w dokumentacji dotyczącej uczniów, rodziców i pracowników jednostki systemu oświaty.
Dlatego też, na dzień analizy zostały zaplanowane działania zaradcze przedstawione w pkt. 9.

……..
Data, podpis i pieczęć Administratora Danych

Załącznik nr 4 do procedury bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej w okresie epidemii COVID-19

Zgłoszenie naruszenia ochrony danych osobowych

1. Imię i nazwisko osoby zgłaszającej:
   .....
2. Data i czas zaistnienia/ rozpoczęcia naruszenia
   ……
3. Naruszenie ochrony danych dotyczyło:
   a) zgubienia lub kradzieży nośnika/urządzenia;
   b) dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niebezpiecznej lokalizacji;
   c) korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem nadawcy;
   d) nieuprawnione uzyskanie dostępu do informacji;
   e) nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń;
   f) złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych;
   g) uzyskanie poufnych informacji poprzez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej;
   h) nieprawidłowa anonimizacja danych osobowych w dokumencie;
   i) nieprawidłowe usunięcie/ zniszczenie danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez administratora;
   j) niezamierzona publikacja;
   k) dane osobowe wysłane do niewłaściwego odbiorcy;
   l) ujawnienie danych niewłaściwej osobie;
   m) ustne ujawnienia danych osobowych;
   n) inne: …….

4. Szczegółowy opis kategorii osób (np. uczeń) i danych osobowych (np.: imię, nazwisko, data urodzenia, miejsce zamieszkanie, dane dotyczące zdrowia):

   ……

5. Opis okoliczności naruszenia

   ……
   ……