REJEST RYZYKA ZDALNEGO NAUCZANIA

Nazwa procesu przetwarzania	**Nauczanie zdalne**	
Charakter przetwarzania	Czasowa realizacja zadań placówki, w tym zajęć z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu ich realizacji w okresie ograniczenia funkcjonowania jednostki systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19	
Zakres przetwarzania	**Kategorie osób, których dane dotyczą**	Uczniowie Nauczyciele Rodzice uczniów Opiekunowie prawni uczniów (ewentualnie inne opisane bliżej w rejestrze czynności przetwarzania)
	Kategorie danych osobowych	Imiona i nazwiska Adresy poczty elektronicznej Wizerunek Głos Oceny postępów w nauce i zachowania Frekwencja
Kontekst przetwarzania	**Podstawa prawna**	Rozporządzenie ogólne o ochronie danych osobowych (RODO) Ustawa z dnia 14 grudnia 2016 - Prawo oświatowe, ze szczególnym uwzględnieniem art. 30b i art. 30c Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 Rozporządzenie Ministra Edukacji Narodowej z dnia 12 sierpnia 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19
	Opis kontekstu	Przetwarzanie danych osobowych dokonywane jest przez nauczycieli na zasadach określonych przez dyrektora szkoły. Zajęcia z wykorzystaniem metod i technik kształcenia na odległość realizowane: * z wykorzystaniem środków komunikacji elektronicznej zapewniających wymianę informacji między nauczycielem, uczniem lub rodzicem, w tym: dziennika elektronicznego, poczty elektronicznej, platformy Teams; * przez podejmowanie przez ucznia aktywności określonych przez nauczyciela, potwierdzających zapoznanie się ze wskazanym materiałem i dających podstawę do oceny pracy ucznia; * przez informowanie rodziców o dostępnych materiałach i możliwych formach ich realizacji przez dziecko lub ucznia w domu.

		W placówce zostały ustalone: * zasady dostępu do infrastruktury informatycznej, oprogramowania i Internetu umożliwiających interakcję między uczniami a nauczycielami prowadzącymi zajęcia; * zasady dotyczące wykorzystywanego sprzętu z uwzględnieniem korzystania ze sprzętu nienależącego do placówki (w tym prywatne komputery, tablety, telefony); * technologie informacyjno-komunikacyjne wykorzystywane przez nauczycieli do realizacji zajęć; * zasady bezpiecznego uczestnictwa w zajęciach; * sposób potwierdzania uczestnictwa uczniów na zajęciach oraz sposób i termin usprawiedliwiania nieobecności uczniów na zajęciach edukacyjnych; * zasady udziału w zajęciach prowadzonych w formie wideokonferencji z uwzględnieniem zasad bezpieczeństwa danych osobowych i ochrony dóbr osobistych; * nauczyciele w czasie zdalnego nauczania przetwarzają dane osobowe w sposób zautomatyzowany, minimalizując zakres przetwarzania danych osobowych w formie papierowej, w szczególności nie posługują się oryginałami dokumentów, do których posiadania zobowiązana jest placówka; w przypadku konieczności posłużenia się oryginałem dokumentu, odbywa się to za wiedzą i zgodą dyrektora placówki. W związku z dostarczaniem rozwiązań informatycznych służących zapewnieniu zdalnego nauczania powierzono przetwarzanie podmiotowi **Vulcan** spółka z ograniczoną odpowiedzialnością, ul. Wołowska 6, 51 – 116 Wrocław. W placówce wyznaczono Inspektora Ochrony Danych (IOD), który zapewnia bieżące wsparcie, wykonując uzasadnia określone w art. 39 ust. 1 RODO.
Cele przetwarzania	Zapewnienie ciągłości procesu nauczania w okresie ograniczenia funkcjonowania jednostki systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19.	
Osoby zaangażowane	Dyrektor placówki, nauczyciele, upoważnieni pracownicy, IOD, personel eksploatacji i utrzymania – Vulcan, uczniowie, rodzice/ opiekunowie prawni uczniów.	

Zaangażowanie oraz własność zasobów (aktywów) biorących udział w operacjach przetwarzania przy nauczaniu zdalnym

Sprzęt	**Własność placówki**	**Własność pracownika**
urządzenia przenośne	9	90
urządzenia stacjonarne	2	5
urządzenia peryferyjne	8	98
nośniki danych	0	106
Oprogramowanie	**Zapewniane przez placówkę**	**Zapewniane przez pracownika**
systemy operacyjne	11	95
oprogramowanie do wideokonferencji	0	0

poczta elektroniczna	106	0
inne (platforma Teams)	106	0
Sieć	**Zapewniane przez placówkę**	**Zapewniane przez pracownika**
sieć VPN	0	0
z WiFi	6	5
stałe łącze	2	83
dostęp do Internetu (sieć radiowa, telefoniczna)	0	10
inne	0	0
Zabezpieczenia	**Zastosowane środki techniczne i organizacyjne**	
Komputer (tablet, smartfon)	Legalny system operacyjny. Legalne aplikacje pobierane z oficjalnej strony w przypadku urządzeń mobilnych z oficjalnego sklepu - Google Play lub App Store. Zabezpieczony dostęp (login, hasło). Stosowanie wygaszacza ekranu (chroniony hasłem). Szyfrowanie dysku twardego.	
Środowisko pracy	Organizacja miejsca pracy według zaleceń obowiązujących w placówce w sposób zapewniający bezpieczne przetwarzanie danych. W tym w możliwie wysokim stopniu zapewnienie eliminacji dostępu osób postronnych. Przechowywanie przenośnych nośników danych oraz dokumentów papierowych w miejscach niedostępnych dla osób postronnych. Prowadzenie wideokonferencji oraz rozmów telefonicznych w miejscach zapewniających brak dostępu osób postronnych.	
Personel placówki	Personel przeszkolony w zakresie ochrony danych osobowych w przypadku pracy zdalnej. Stosowanie upoważnień i poleceń przetwarzania danych osobowych. Wdrożono procedury określające zasady bezpiecznej pracy zdalnej. Personel zapoznany z procedurami bezpiecznej pracy zdalnej - zdalnych lekcji, konsultacji, korespondencji.	
Uczniowie, ich rodzice lub opiekunowie	Wdrożono procedury określające zasady bezpiecznej nauki zdalnej obejmujące także zasady postępowania uczniów, kierowane także do ich rodziców i opiekunów. Uczniowie, ich rodzice i opiekunowie zapoznani z procedurami bezpiecznej pracy zdalnej - zdalnych lekcji, konsultacji, korespondencji, itp.	

Zagrożenia i podatności, waga prawdopodobieństwo i ryzyko naruszenia praw lub wolności osób fizycznych przy zdalnym nauczaniu

Analizowane obszary	Zagrożenia	Podatności	Waga	Prawdopodobieństwo	Ryzyko
Komputer (tablet, smartfon)	• niezgodne z prawem lub przypadkowe zniszczenie danych osobowych, • niezgodne z prawem lub przypadkowe utracenie danych, • niezgodne z prawem lub przypadkowa ingerencja w treść danych, • niezgodne z prawem lub przypadkowe udostępnienie danych, • naruszenie dóbr osobistych, • utrata kontroli nad danymi osobowymi, • kradzież tożsamości, • szkody majątkowe, • kradzież tożsamości, • uszkodzenie sprzętu,	• działanie szkodliwego oprogramowania, • niestosowanie programów antywirusowych, • korzystanie z nielegalnego lub nieaktualnego oprogramowania, • nieprzestrzeganie zasad prowadzenia korespondencji mailowej, • nieprawidłowa wysyłka korespondencji mailowej (błędny adresat, użycie opcji do wiadomości wszystkich), • prowadzenie służbowej korespondencji z prywatnego konta pocztowego, • nieuprawnione kopiowanie danych osobowych na nośnik informacji (np. pendrive), • niezabezpieczenie pliku zawierającego dane osobowe, • przesłanie danych osobowych osobie nieuprawnionej, rozpowszechnienie danych, • dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do danych osobowych innej osobie niż osoba upoważniona, • zapisywanie dokumentów lub ich kopii zawierających dane osobowe w miejscach nieautoryzowanych, • zainstalowanie nielegalnego oprogramowania, • opuszczenie stanowiska pracy z pozo-	1	3	3

		stawieniem aktywnej aplikacji umożliwiającej dostęp do danych osobowych, • pozostawienie w miejscu niezabezpieczonym zapisanego identyfikatora/hasła dostępu do plików/komputera w którym przetwarzane są dane osobowe, • wyjście z programu lub opuszczenie stacji roboczej bez wylogowania,			
Środowisko pracy	• niezgodne z prawem lub przypadkowe zniszczenie danych osobowych, • niezgodne z prawem lub przypadkowe utracenie danych, • niezgodne z prawem lub przypadkowa ingerencja w treść danych, • niezgodne z prawem lub przypadkowe udostępnienie danych, • transfer danych do państwa trzeciego, • naruszenie dóbr osobistych, • utrata kontroli nad danymi osobowymi, • szkoda majątkowa,	• wadliwe zorganizowanie środowiska pracy (nieprzestrzeganie "polityki czystego biurka"), • nieprzestrzeganie polityki czystego ekranu, • nieuprawnione zniszczenie dokumentu zawierającego dane osobowe, • pozostawienie dokumentu zawierającego dane osobowe w miejscu nienadzorowanym, • niezachowanie dyskrecji przez osoby przetwarzające dane osobowe, • zgubienie dokumentu zawierającego dane osobowe, • brak kontroli nad stanowiskiem pracy - niekontrolowany dostęp do dokumentów i narzędzi osób trzecich, • wyrzucenie dokumentów zawierających dane osobowe w formie umożliwiającej ich odczytanie (bez zniszczenia/ anonimizacji), • dopuszczenie do kopiowania dokumentów zawierających dane osobowe przez osoby nieuprawnione, • awaria prądu,	1	2	2

		• awaria połączenia z siecią, • korzystanie z narzędzi i usług, z którymi związany jest transfer danych do państwa trzeciego, • brak zabezpieczenia przed nieuprawnionym dostępem do danych osobowych i innych treści podczas wideokonferencji,			
Personel placówki	• wtargnięcie na zajęcia lekcyjne osób postronnych, • zamieszczanie na portalach społecznościowych linków do wideokonferencji, • rozpowszechnienie nagrania wideokonferencji, • rozpowszechnianie danych osobowych za pośrednictwem mediów społecznościowych, • udział w zdalnej lekcji osoby postronnej,	• wadliwa organizacja zdalnej lekcji umożliwiająca wtargniecie na nią przez osoby postronne, • zgubienie komputera, • łączenie przez niezabezpieczoną sieć wifi, • zamieszczanie na portalach społecznościowych zdjęć/filmów z wideokonferencji, • nagrywanie wideokonferencji bez zgody osób w niej uczestniczącej,	1	2	2
Uczniowie, ich rodzice lub opiekunowie	• wtargnięcie na zajęcia lekcyjne osób postronnych, • zamieszczanie na portalach społecznościowych linków do wideokonferencji, • rozpowszechnienie nagrania wideokonferencji, • rozpowszechnianie danych osobowych za pośrednictwem mediów społecznościowych, • udział w zdalnej lekcji osoby postronnej,	• wadliwa organizacja zdalnej lekcji umożliwiająca wtargniecie na nią przez osoby postronne, • łączenie przez niezabezpieczoną sieć WiFi, • zamieszczanie na portalach społecznościowych zdjęć/filmów z wideokonferencji, • nagrywanie wideokonferencji bez zgody osób w niej uczestniczącej, • niezastosowanie się do procedur dotyczących uczestnictwa w zdalnych lekcjach i poszanowania dóbr osobistych osób w nich uczestniczących.	1	4	4

Waga zagrożenia

W przypadku zarówno wagi zagrożenia oraz prawdopodobieństwa jego wystąpienia zastosowano skali 1-4, według następujących założeń:

wartość 1 **niska waga zagrożenia**	osoby, których dane dotyczą, nie zostaną dotknięte skutkami naruszenia lub spotkają je drobne niedogodności, które pokonają bez najmniejszych problemów (zniecierpliwienie, irytacja, czas potrzebny na ponowne wprowadzenie danych lub zalogowanie, itp.),
wartość 2 **średnia waga zagrożenia**	osoby, których dane dotyczą, mogą napotkać znaczące niedogodności, które będą w stanie pokonać pomimo pewnych trudności (naruszenie godności dziecka lub innej osoby, strach, niezrozumienie, stres, naruszenie poufności danych osobowych chronionych tajemnicą zawodową, dodatkowe koszty, itp.),
wartość 3 **wysoka waga zagrożenia**	osoby, których dane dotyczą, mogą napotkać znaczące niedogodności, które powinny być w stanie pokonać, ale z poważnymi trudnościami (dyskryminacja dziecka lub innej osoby, pozbawienie możliwości sprawowania kontroli nad swoimi danymi osobowymi, kradzież tożsamości, oszustwa finansowe, szkody majątkowe, utrata zatrudnienia, pozwanie i udział w postępowaniu, pogorszony stan zdrowia itp.),
wartość 4 **bardzo wysoka waga zagrożenia**	osoby, których dane dotyczą, mogą napotkać znaczące, a nawet nieodwracalne konsekwencje, których mogą nie pokonać (problemy finansowe, niezdolność kontynuacji nauki, niezdolność do pracy, długotrwałe psychologiczne lub fizyczne urazy, śmierć itp.).

Określenie prawdopodobieństwa wystąpienia zagrożenia

wartość 1 **niskie prawdopodobieństwo**	urzeczywistnienie się zagrożenia w związku z wykorzystaniem podatności zasobów biorących udział w operacjach przetwarzania nie wydaje się możliwe
wartość 2 **średnie prawdopodobieństwo**	urzeczywistnienie się zagrożenia w związku z wykorzystaniem podatności zasobów biorących udział w operacjach przetwarzania jest trudne
wartość 3 **wysokie prawdopodobieństwo**	urzeczywistnienie się zagrożenia w związku z wykorzystaniem podatności zasobów biorących udział w operacjach przetwarzania jest możliwe
wartość 4 **bardzo wysokie prawdopodobieństwo**	urzeczywistnienie się zagrożenia w związku z wykorzystaniem podatności zasobów biorących udział w operacjach przetwarzania jest bardzo łatwe, wręcz oczywiste

Określenie poziomu ryzyka

Poziom ryzyka stanowi iloczyn wagi zagrożenia oraz prawdopodobieństwa jego wystąpienia dla danego obszaru (zasobu) operacji przetwarzania danych jaką jest nauczanie zdalne.

Możliwe kombinacje wskazanych wartości przedstawia poniższa tabela, wartości tu określone zostały odzwierciedlone w powyższej analizie - w polu "Ryzyko"

WAGA	Bardzo wysoka (4)	4	8	12	16
	Wysoka (3)	3	6	9	12
	Średnia (2)	2	4	6	8
	Niska (1)	1	2	3	4
		Niskie (1)	Średnie (2)	Wysokie (3)	Bardzo wysokie (4)
	Prawdopodobieństwo				

Skala dopuszczalności ryzyka

Ocena ryzyka	**Dopuszczalność ryzyka**	**Działania**
Ryzyko bardzo wysokie poziom: 12-16	Niedopuszczalne	Przetwarzanie danych osobowych nie może być podjęte ani kontynuowane do czasu obniżenia poziomu ryzyka do dopuszczalnego.
Ryzyko wysokie poziom: 8-11	Dopuszczalne - do zredukowania	Przetwarzanie danych osobowych jest dopuszczalne, ale konieczna jest ocena skutków dla ochrony danych osobowych oraz podjęcie działań zmierzających do obniżenia poziomu ryzyka do akceptowalnego.
Ryzyko średnie - akceptowalne poziom: 4-7	Akceptowalne	Przetwarzanie danych osobowych jest dopuszczalne, konieczne jest podejmowanie działań mających na celu obniżanie poziomu ryzyka i niedopuszczenie do wzrostu jego poziomu.
Ryzyko nieznaczne lub pomijalne poziom: 1-3	Akceptowalne - możliwe do pominięcia	Przetwarzanie danych osobowych jest dopuszczalne, konieczne jest podejmowanie działań mających na celu obniżanie poziomu ryzyka i niedopuszczenie do wzrostu jego poziomu.

Skutki wystąpienia zagrożenia dla praw lub wolności osoby fizycznej przy nauczaniu zdalnym oraz zastosowanie rozwiązań mającym na celu przeciwdziałanie wystąpienia tym skutkom

Możliwe skutki wystąpienia zagrożenia dla praw lub wolności osoby fizycznej brane pod uwagę przy dokonywaniu analizy	Wprowadzone rozwiązania zaradcze (działania mitygujące ryzyko)
zniecierpliwienie, irytacja,	• wdrożenie procedur dotyczących pracy zdalnej i zdalnego nauczania, • przeszkolenie personelu w zakresie ochrony danych osobowych przy pracy zdalnej, zdalnym nauczaniu i zdalnych lekcjach i poszanowania dóbr osobistych, w szczególności poszanowania prywatności, • pouczenie uczniów, ich rodziców i opiekunów prawnych o zasadach bezpiecznego przebiegu zdalnych lekcji, zasadach bezpiecznej komunikacji i poszanowania dóbr osobistych, w szczególności poszanowania prywatności, • określenie zasad bezpiecznego organizowania, prowadzenia i udziału w zdalnych lekcjach z wykorzystaniem narzędzi do wideokonferencji, • obowiązek zorganizowania stanowiska pracy w sposób określony przez pracodawcę, zapewniający bezpieczne prowadzenie pracy zdalnej i zdalnego nauczania, • przechowywanie dokumentów w zabezpieczonych miejscach, • pilne strzeżenie sprzętu - komputerów, tabletów smartfonów służących do pracy zdalnej i zdalnego nauczania, ograniczanie transportu, nośników danych do minimum, • ograniczenie tworzenia kopii dokumentów papierowych, unikanie tworzenia kopii na nośnikach przenośnych, w razie umieszczenia danych osobowych na takim nośniku (USB, płyta) pilne strzeżenie nośnika przed dostępem osób postronnych, • pilne strzeżenie haseł dostępowych do urządzeń i programów, • procedury prowadzenia korespondencji mailowej, • niepozostawianie otwartych dokumentów w wersji elektronicznej, bez nadzoru (widocznych dla osób postronnych), • po zakończonej pracy - zamknięcie używanych programów i wylogowanie oraz zabezpieczanie nośników w miejscu niedostępnym dla
czas potrzebny na ponowne wprowadzenie danych lub zalogowanie,	
naruszenie godności dziecka lub innej osoby,	
strach, niezrozumienie, stres,	
dodatkowe koszty,	
naruszenie poufności danych osobowych chronionych tajemnicą zawodową,	
oszustwa finansowe,	
szkody majątkowe,	
utrata zatrudnienia,	
dyskryminacja dziecka lub innej osoby,	
pozbawienie możliwości sprawowania kontroli nad swoimi danymi osobowymi,	
kradzież tożsamości,	
problemy finansowe,	
niezdolność kontynuacji nauki, niezdolność,	
niezdolność do pracy,	
długotrwałe psychologiczne lub fizyczne urazy, śmierć,	
strata finansowa po stronie dziecka, jego rodzica lub opiekuna prawnego, bądź innej osoby,	
naruszenie dobrego imienia,	
naruszenie prywatności,	
nieuprawnione odwrócenie pseudonimizacji,	
znaczna szkodą gospodarcza lub społeczna,	
pozbawienie osób fizycznych przysługujących im praw i wolności,	
pozbawienie możliwości sprawowania kontroli nad swoimi danymi osobowymi,	

bezprawne przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych, danych genetycznych, dane dotyczących zdrowia lub seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa,	innych osób, • niepozostawianie dokumentów papierowych bez nadzoru (widocznych dla osób postronnych), • po zakończonej pracy - zabezpieczanie dokumentów w miejscu niedostępnym dla innych osób, • zapewnienie pracownikom dostęp do Internetu dostarczanego przez pracodawcę, a w przypadku braku takiej możliwości zobowiązanie do korzystania z odpowiednio zabezpieczonej sieci i zakaz korzystania z publicznych sieci WiFi, • korzystanie z usług zweryfikowanych dostawców zapewniających usługi o najwyższym poziomie zabezpieczeń (Internet, komunikatory wideokonferencje), • korzystanie wyłącznie z narzędzi i usług zapewniających przetwarzanie danych osobowych w UE, bez transferu danych do państwa trzeciego, • stosowanie programów antywirusowych z ich częstymi aktualizacjami, blokad antyspamowych w poczcie.
podszywanie się, personalizacja ataków / phishing,	
brak/utrata możliwości powiadomienia o incydencie,	
spamowanie, uciążliwe telefony,	
zaciągnięcie zobowiązań finansowych,	
szkody majątkowe po stronie osoby, której dane dotyczą,	
wpis w biurze informacji gospodarczej, wyłudzenia i oszustwa,	
utrata dobrego imienia,	
nieuprawnione rozpowszechnienie lub inne naruszenia prawa do ochrony wizerunku,	
szkody majątkowe/ kradzież/ uszkodzenie mienia,	
naruszenie miru domowego,	
wykorzystanie trudnej sytuacji materialnej,	
posłużenie się podrobionym lub dokumentem osoby, której dane dotyczą,	
włamanie do komputera,	
szantaż,	
oferty korupcyjne lub zarzucenie korupcji.	