Informacja dot. przykładowej analizy zagrożeń w procesie zdalnego nauczania

1. Poniższa analiza zagrożeń odpowiada zadaniu postawionemu przed dyrektorem szkoły w komunikacie Urzędu Ochrony Danych Osobowych (UODO) z dnia 31 marca pt. „Dane osobowe bezpieczne podczas zdalnego nauczania – poradnik UODO dla szkół", https://uodo.gov.pl/pl/138/1473:

   – Szkoła, która chce skorzystać z usług przetwarzania danych z wykorzystaniem innych niż wcześniej używane narzędzia, powinna – wraz z pomocą wyznaczonego inspektora ochrony danych, ***w pierwszej kolejności przeprowadzić analizę zagrożeń****. Szczególna uwaga powinna zostać zwrócona na bezpieczeństwo danych oraz zapewnienie odpowiednich gwarancji praw osób, których dane dotyczą*

2. W poniższej analizie wykorzystano „DOBRE PRAKTYKI POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH PODCZAS LEKCJI ONLINE" zamieszczone w komunikacie, a poszczególne rubryki analizy odpowiadają m.in. na wskazane przez UODO praktyki.

3. W przypadku życzliwego przyjęcia przedstawionej propozycji analizy dobrym udokumentowaniem działania szkoły może być wydruk zamieszczonej analizy wraz z dwoma dokumentami znajdującymi się w komunikacie UODO. Oczywistym dalszym krokiem powinno być wdrożenie tych działań, które pozwolą skutecznie monitorować, ograniczać lub zdecydowanie redukować ryzyko!

4. Poniższa analiza zagrożeń wraz z analizą ryzyka przygotowaną dla konkretnego produktu, wybranego dla prowadzenia procesu zdalnego nauczania może stanowić podstawę dla wykazania właściwego podejścia do bezpieczeństwa i ochrony danych.

5. Wszystkie rubryki i wyliczenia zależą od ostatecznej decyzji osób dokonujących analizy w szkole. Niektóre rubryki analizy zagrożeń zostały już wstępnie wypełnione tam, gdzie ocena ryzyka i ocena jego skutku wydaje się oczywista. We wszystkich pozostałych rubrykach przyjmowane wartości zależą od sytuacji w konkretnej szkole.

6. Poniższe informacje nie stanowią opinii prawnej i mają wyłącznie charakter orientacyjny. Poniższa analiza zagrożeń ma charakter przykładowy i może nie obejmować wszystkich potencjalnych zagrożeń. Prosimy o dokonanie swojej analizy przed podjęciem decyzji co do sposobu postępowania. Każda szkoła może wykorzystać załączony przykład lub przygotować odmienną własną analizę.

ANALIZA ZAGROŻEŃ W PROCESIE ZDALNEGO NAUCZANIA

Zagrożenia dla bezpieczeństwa danych i praw osób, których dane dotyczą
(wypełnienie zaleceń UODO z 31 marca 2020)

METRYKA SZKOŁY

(wypełnia szkoła)

Dane szkoły: .....

.....

.....

.....

Podpisy: ……..…… ……..

Data przygotowania analizy: …….

Każde przedstawione poniżej zagrożenie podlega analizie pod kątem jego istotności dla osiągania celów i zadań związanych z procesem zdalnego nauczania oraz bezpieczeństwa danych i praw osób, których dane dotyczą. Analiza ryzyka dla każdego zagrożenia została przygotowana w oparciu obecny stan wdrożenia zdalnego nauczania w szkole.

Odniesienia Poradnik UODO dla szkół, https://uodo.gov.pl/pl/138/1473:

(1) „Dobre praktyki" – dokument „DOBRE PRAKTYKI POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH PODCZAS LEKCJI ONLINE",

(2) „Bezpieczne dane" – dokument „DANE OSOBOWE BEZPIECZNE PODCZAS ZDALNEGO NAUCZANIA",

oraz **(3)** Rozporządzenie PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO)

	RODZAJ ZAGROŻENIA/RYZYKA	ZAGROŻENIE/RYZYKO	Prawdopodobieństwo * wystąpienia ryzyka (skala 1-4 pkt)	Skutek** (skala 1-4 pkt)	Poziom wpływu ryzyka na bezpieczeństwo*** Iloczyn 2 i 3 (skala 1-16 pkt)	Ocena ryzyka	Istniejące mechanizmy kontroli i działania ograniczające ryzyko
	1		2	3	4	5	6
1.	Zagrożenie ciągłości działania **(3)**	Awarie/uszkodzenia urządzeń w infrastrukturze szkoły wykorzystywanych w procesie zdalnego nauczania (obejmuje także awarie komputerów przenośnych należących do szkoły) Ataki cybernetyczne na infrastrukturę szkoły	2	3	6	umiarkowane	***Ograniczenie ryzyka***: Urządzenia objęte gwarancjami i serwisem pogwarancyjnym. Odpowiednie umowy serwisowe gwarantujące właściwą ochronę danych osobowych związaną z fizycznym dostępem do sprzętu; Zalecenia dotyczące jakości i sposobów wyboru optymalnego sprzętu (przygotowane przez MEN lub odpowiednią agendę rządową; ostatecznie przygotowane przez szkołę). Przygotowanie planu ciągłości działania i zasad postepowania podczas awarii.
2.	Zagrożenie ciągłości działania	Awarie/uszkodzenia urządzeń prywatnych wykorzystywanych w procesie zdalnego nauczania należących do uczniów i nauczycieli	4	1	4	nieznaczne	***Ograniczenie ryzyka***: Zalecenia dotyczące jakości i sposobów wyboru optymalnego sprzętu (przygotowane przez MEN lub odpowiednią agendę rządową; ostatecznie przygotowane przez szkołę)

3.	Zagrożenie ciągłości działania	Awaria sieci uniemożliwiająca dostęp do infrastruktury szkolnej podczas pracy zdalnej lub znacznie spowalniająca pracę zdalną.	2	4	8	wysokie	***Znaczna redukcja ryzyka:*** Przeniesienie infrastruktury szkolnej do chmury obliczeniowej - wykorzystanie rozwiązań chmurowych od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpiecznej pracy zdalnej i ochronę danych osobowych[i] (por. punkt 4) ***Ograniczenie ryzyka:*** Umowy z dostawcami Internetu oraz serwisem infrastruktury szkolnej gwarantujące odpowiedni czas reakcji; Przygotowanie planu ciągłości działania i zasad postepowania podczas awarii.
4.	Zagrożenie ciągłości działania	Awaria sieci uniemożliwiająca dostęp do infrastruktury szkolnej w chmurze obliczeniowej podczas pracy zdalnej lub znacznie spowalniająca pracę zdalną. Ataki cybernetyczne na infrastrukturę chmurową wykorzystywaną przez szkołę	1	4	4	nieznaczne	***Znaczna redukcja ryzyka:*** Wykorzystanie rozwiązań chmurowych od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpiecznej pracy zdalnej i ochronę danych osobowych[i]
5.	Zagrożenie ciągłości działania **(1) p.14**	Brak kopii zapasowych lub nieaktualne kopie zapasowe, przechowywanie kopii zapasowych w tych samych pomieszczeniach co pozostała część infrastruktury szkolnej; problemy z przywróceniem funkcjonowania w przypadku awarii lub cyberataku					***Znaczna redukcja ryzyka:*** Wykorzystanie rozwiązań chmurowych z wysokim poziomem ciągłości działania od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpiecznej pracy zdalnej i ochronę danych osobowych[i] ***Ograniczenie ryzyka:*** Regularne tworzenie i dokumentowanie kopii zapasowych; przygotowanie planu awaryjnego przywracania sprawności szkolnego systemu oraz przetestowanie takich działań; odpowiednie zapisy w umowach z serwisem infrastruktury szkolnej

6.	Zagrożenie ciągłości działania **(3)**	Brak aktualnej dokumentacji (w tym brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania, licencji, rejestru czynności dla ochrony danych) utrudniające przywracanie środowiska i zarządzanie nim, np. kiedy odejdzie administrator IT lub w przypadku zerwania kontraktu przez firmę sprawującą opiekę nad infrastrukturą; Zagrożenie prawidłowej rozliczalności procesu przetwarzania danych					***Ograniczenie ryzyka:*** Przygotowanie i wprowadzenie w życie rozliczalności procesów przetwarzania danych poprzez tworzenie odpowiedniej dokumentacji; przygotowanie planu awaryjnego przywracania sprawności szkolnego systemu oraz przetestowanie takich działań; odpowiednie zapisy w umowach z serwisem infrastruktury szkolnej

7.	Zagrożenie dla bezpieczeństwa danych **(1) p.1.**	Brak aktualizacji systemu operacyjnego dla urządzeń użytkowników					***Monitorowanie:*** na bieżąco, jeśli możliwe lub przynajmniej raz w roku ***Redukcja ryzyka:*** Wykluczenie ze zdalnego nauczania urządzeń z systemami operacyjnymi bez wsparcia producenta lub po zakończeniu wsparcia. ***Ograniczenie ryzyka*:** stosowanie urządzeń z systemami operacyjnymi, w których aktualizacja może być wykonywana automatycznie lub półautomatycznie; w przypadku urządzeń należących do szkoły możliwość zarządzania procesem aktualizacji tak aby nie kolidował z nauczaniem; aktualizacja wyłącznie ze stron producenta; zadanie sprawdzania aktualizacji w umowie wsparcia technicznego dla szkoły; ***także***: wymaganie stosowania aktualnego systemu operacyjnego dla komputerów prywatnych używanych w procesie zdalnego nauczania
8.	Zagrożenie dla bezpieczeństwa danych **(1) p.1.**	Brak aktualizacji systemu operacyjnego w infrastrukturze serwerowej					***Monitorowanie:*** automatyczne monitorowanie w chmurze obliczeniowej; w infrastrukturze własnej: na bieżąco przez administratora lub zapisane w umowie wsparcia technicznego dla szkoły ***Znaczna redukcja ryzyka:*** wykorzystanie rozwiązań chmurowych w modelu PaaS i SaaS, w których odpowiedzialność za aktualizację leży po stronie dostawcy; Wykorzystanie rozwiązań chmurowych od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpiecznej pracy zdalnej[i] ***Ograniczenie ryzyka:*** odpowiednie umowy dotyczące wsparcia technicznego dla infrastruktury szkolnej lub chmurowego modelu IaaS; alokacja odpowiedniego budżetu w przypadku konieczności zakupu nowego systemu operacyjnego

9.	Zagrożenie dla bezpieczeństwa danych **(1) p.2, 4, 5, 13.**	Brak lub nieaktualne oprogramowanie wspomagające zapewnienie bezpieczeństwa we wszystkich urządzeniach w procesie zdalnego nauczania (oprogramowanie antywirusowe, antymalware, antyspyware) Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania Ataki socjotechniczne: phishing, spearphishing, cybersquatting					***Monitorowanie***: polityka automatycznej aktualizacji oprogramowania wspierającego; okresowy przegląd stosowanych rozwiązań; polityka pobierania oprogramowania wyłącznie z zaufanych źródeł ***Zdecydowana redukcja ryzyka***: połączenie rozwiązań na urządzeniach końcowych i chmurowych rozwiązań z wbudowanymi aplikacjami wspomagającymi bezpieczeństwo typu Advanced Threat Protection (zapewnia bezpieczeństwo w przypadku przesłania załącznika lub linku z nieznanego źródła, automatycznie blokuje potencjalne zagrożenia); ***Ograniczenie ryzyka:*** wdrożenie jednolitej polityki dot. stosowanych narzędzi wspomagających bezpieczeństwo; polityka regularnego stosowania tych narzędzi przez wszystkich użytkowników sieci szkolnych; wykorzystanie narzędzi wbudowanych i aktualizowanych w systemie operacyjnym
10.	Zagrożenie dla bezpieczeństwa danych **(1) p.9, 19**	Nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe (zwłaszcza serwerowni i pozostałych elementów infrastruktury IT); słabe zabezpieczenia plików i innych zasobów sieciowych w infrastrukturze własnej					***Zdecydowana redukcja ryzyka***: wykorzystanie rozwiązań chmurowych od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpieczeństwa fizycznego centrów przetwarzania danych, nośników, oraz odpowiedniego doboru i przeszkolenia personelu[i] ***Ograniczenie ryzyka***: wprowadzenie odpowiedniej polityki dostępu do pomieszczeń; wprowadzenie zasad zabezpieczania plików i zasobów sieciowych

11.	Zagrożenie dla bezpieczeństwa danych **(1) p. 6,7,8,11 (2)**	Niedostateczne bezpieczeństwo uwierzytelniania w systemie zdalnego nauczania, m.in. proste hasła, powtarzające się hasła, hasła zapisywane na kartkach lub zapamiętywane w aplikacjach webowych, brak możliwości stosowania wieloskładnikowego uwierzytelnienia (2FA/MFA)					***Zdecydowana redukcja ryzyka***: stosowanie wieloskładnikowego uwierzytelniania (2FA/MFA), w szczególności połączonego z systemami warunkowego uwierzytelniania (system automatycznie zaczyna rozpoznawać, że użytkownik podłącza się z niezaufanego/nieznanego urządzenia lub publicznych/niezabezpieczonych sieci i wymusza drugi składnik uwierzytelnienia) w szczególności dla nauczycieli ***Ograniczenie ryzyka:*** wdrożenie w życie polityki zarządzania hasłami wraz z bezpieczeństwem ich stosowania (długość haseł, ich złożoność, częstotliwość zmiany, przechowywanie itd.); ograniczenie możliwości logowania się z pomocą tożsamości z serwisów społecznościowych wykorzystywanych prywatnie
12.	Zagrożenie dla bezpieczeństwa danych **(1) p. 10,18**	Korzystanie z publicznych lub niezabezpieczonych połączeń internetowych dla użytkowników pracujących zdalnie Brak zabezpieczeń punktów dostępowych na terenie szkoły					***Monitorowanie:*** regularne sprawdzanie poziomu bezpieczeństwa sieci szkolnej w budynku szkolnym; ***Ograniczenie ryzyka:*** wprowadzenie polityki połączenia z systemem szkolnym wyłącznie poprzez sieci VPN; regularna aktualizacja oprogramowania w urządzeniach sieciowych; dokumentowanie działań i odpowiednie zapisy w umowach wsparcia technicznego dla szkoły

13.	Zagrożenie dla bezpieczeństwa danych i praw osób, których dane dotyczą **(1) p.15, 16, 17, 20 (2) (3)**	Utrata nośnika zawierającego dane osobowe lub nieprawidłowe/brak procedur niszczenia nośników z danymi Nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik	3	3	9	wysokie	***Ograniczenie ryzyka:*** szyfrowanie wszystkich nośników, zarówno na urządzeniach końcowych, jak i w części serwerowej infrastruktury (w przypadku zastosowania rozwiązania chmurowego zasada szyfrowania danych w spoczynku i w tranzycie); anonimizacja i pseudonimizacja danych tam, gdzie to możliwe; wdrożona polityka dotycząca stosowania nośników podłączanych do urządzeń w sieci szkolnej **Obowiązkowo także**: wprowadzenie polityki powiadamiania o naruszeniach bezpieczeństwa danych i praw osób, których dane dotyczą
14.	Zagrożenie dla bezpieczeństwa danych i praw osób, których dane dotyczą **(3)**	Upublicznienie danych w przestrzeni publicznej, dostęp przez Internet, przesłanie lub wydawanie danych osobowych osobie nieupoważnionej Nieuprawniona modyfikacja lub usunięcie danych osobowych Nieuprawnione kopiowanie danych osobowych (kopiowanie danych z katalogów, dysków, baz, programów)	4	4	16	**niedopuszczalne**	***Zdecydowana redukcja ryzyka:*** korzystanie z usług katalogowych i wprowadzenie odpowiednich uprawnień w dostępie do danych wyłącznie dla odpowiednich osób; klasyfikowanie danych i wprowadzenie reguł w systemie informatycznym pozwalających na określone czynności z poszczególnymi kategoriami danych (np. dane tylko wewnętrzne, tylko dla określonych osób, dane z określonym czasem dostępu); wprowadzenie w systemie szkolnym narzędzi typu DLP (Data Loss Protection), które pozwalają na ograniczenie lub zarządzanie dostępem; a wreszcie: wykorzystanie rozwiązań chmurowych wypełniających wszystkie powyższe zadania od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpiecznej pracy zdalnej[i] ***Ograniczenie ryzyka:*** Wprowadzenie polityki postępowania z danymi osobowymi w systemie szkolnym; stosowanie anonimizacji i pseudonimizacji tam, gdzie to możliwe **Obowiązkowo także**: wprowadzenie polityki powiadamiania o naruszeniach bezpieczeństwa danych i praw osób, których dane dotyczą

15.	Zagrożenie dla bezpieczeństwa danych i praw osób, których dane dotyczą **(3)**	W systemie zdalnej nauki przetwarzane są szczególne kategorie danych osobowych (np. dane medyczne, dane biometryczne)		4			***Natychmiastowa redukcja ryzyka:*** Całkowite wyłączenie przetwarzania takich danych w systemie zdalnej nauki; wprowadzenie odpowiednich polityk ***Ograniczenie ryzyka:*** wykorzystanie rozwiązań, które gwarantują odpowiednie bezpieczeństwo danych, m.in. korzystanie z usług katalogowych i wprowadzenie odpowiednich uprawnień w dostępie do danych; klasyfikowanie danych i wprowadzenie reguł pozwalających na określone czynności ze szczególnymi kategoriami danych osobowych; wprowadzenie w systemie szkolnym narzędzi typu DLP (Data Loss Protection), które pozwalają na ograniczenie lub zarządzanie dostępem; a wreszcie: wykorzystanie rozwiązań chmurowych wypełniających wszystkie powyższe zadania od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpiecznej pracy zdalnej[i]; **Obowiązkowo także**: wprowadzenie polityki powiadamiania o naruszeniach bezpieczeństwa danych i praw osób, których dane dotyczą
16.	Zagrożenie dla bezpieczeństwa danych i praw osób, których dane dotyczą **(2) (3)**	W procesie realizowane jest tworzenie profili zachowania lub profili marketingowych osób, których dane dotyczą, w szczególności osób małoletnich, a informacja taka jest przekazywana dla wykorzystania jej komercyjnie Błędy w oprogramowaniu wykorzystywanym w zdalnym nauczaniu prowadzące do niewłaściwego przetwarzania danych osobowych		4			***Natychmiastowa redukcja ryzyka:*** Natychmiastowe wyłączenie z eksploatacji wszelkich rozwiązań, które mogą prowadzić do tworzenia profili zachowania lub profili marketingowych – brak takiego działania powinien mieć odzwierciedlenie w umowach jakie przedstawiają dostawcy rozwiązań; stosowanie rozwiązań dedykowanych edukacji i wyłączenie stosowania rozwiązań konsumenckich jeśli nie jest to absolutnie konieczne (odpowiednia polityka bezpieczeństwa powinna być przekazana wszystkim użytkownikom systemu); wykorzystanie rozwiązań chmurowych od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpiecznej pracy zdalnej[i]

							Ograniczenie ryzyka: Wykorzystywanie ograniczonej liczby produktów, usług i oprogramowania w systemie szkolnym; informacja przekazana nauczycielom i rodzicom co do wybranych w szkole rozwiązań i wymaganie zastosowania się do tego ograniczenia **Obowiązkowo także**: wprowadzenie polityki powiadamiania o naruszeniach bezpieczeństwa danych i praw osób, których dane dotyczą
17.	Zagrożenie dla bezpieczeństwa danych i praw osób, których dane dotyczą **(3)**	Wykorzystanie rozwiązań, w szczególności rozwiązań chmurowych, w których zapisy polityki ochrony danych osobowych nie mają wprost odniesienia do wymagań prawa, w szczególności od dostawców niemających reprezentacji w Polsce i mających siedzibę poza EOG	**4**	3	12	**niedopuszczalne**	***Natychmiastowa redukcja ryzyka:*** Całkowite wyeliminowanie takich rozwiązań z praktyki zdalnego nauczania ze względu na brak możliwości wyegzekwowania wymagań związanych z ochroną danych osobowych ***Ograniczenie ryzyka:*** stosowanie takich rozwiązań wyłącznie dla danych nieosobowych **Obowiązkowo także**: wprowadzenie polityki powiadamiania o naruszeniach bezpieczeństwa danych i praw osób, których dane dotyczą
18.	Zagrożenie dla bezpieczeństwa danych i praw osób, których dane dotyczą **(3)**	Techniczny problem z realizacją praw osób, których dane dotyczą związane z dostępem, edycją i usuwaniem danych osobowych – żmudny i uciążliwy proces	3				***Natychmiastowa redukcja ryzyka***: zastosowanie narzędzi pozwalających na znajdowanie i odpowiednie działania z danymi osobowymi pozwalające na realizację praw osób, których dane dotyczą ***Ograniczenie ryzyka:*** wprowadzenie polityki ograniczania przetwarzania danych osobowych poza strukturalnymi bazami danych poddających się łatwemu przeszukiwaniu; pseudonimizacja; polityki usuwania danych osobowych natychmiast po ustaniu celu przetwarzania; klasyfikowanie danych

LEGENDA

Sposób oceny prawdopodobieństwa wystąpienia ryzyka

Prawdopodobieństwo wystąpienia ryzyka	Liczba punktów	Przesłanki
Bardzo wysokie (81-100%)	**4**	Przewiduje się, że zdarzenie z pewnością wystąpi w ciągu roku
Wysokie (61-80%)	**3**	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku
Średnie (21-60%)	**2**	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub kilka razy w ciągu roku
Niskie (0-20%)	**1**	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub nie zdarzy się w ciągu roku

Sposób oceny skutku ryzyka

Skutek wystąpienia ryzyka*	Liczba punktów	Przesłanki
Bardzo wysoki	4	Poważna niezgodność z przepisami prawa. Brak procedur dla danego procesu. Olbrzymie zakłócenia pracy. Znaczny uszczerbek na wizerunku. Bardzo wysokie niebezpieczeństwo dla ochrony danych. Zagrożenia spowodują brak zachowania ciągłości procesów działania, utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów. Brak osiągnięcia kluczowych celów.
Wysoki	3	Duże zagrożenie realizacji kluczowych zadań albo osiągania założonych celów. Wysokie niebezpieczeństwo dla ochrony danych. Znaczny uszczerbek na wizerunku. Długotrwały i trudny proces przywracania stanu poprzedniego.
Średni	2	Spadek efektywności działania i obniżenie jakości wykonywania zadań. Średnie niebezpieczeństwo dla ochrony danych. Nieznaczny negatywny wpływ na wizerunek. Trudny proces przywracania stanu poprzedniego
Niski	1	Zakłócenie lub opóźnienie w wykonywaniu zadań. Bez uszczerbku dla wizerunku. Niewielkie niebezpieczeństwo dla ochrony danych. Skutki łatwe do usunięcia

Skala dopuszczalności ryzyka

Oszacowanie ryzyka	Dopuszczalność ryzyka	Działania
Ryzyko poważne Skala: 12–16 pkt.	Niedopuszczalne (nieakceptowane)	Działania nie mogą być podjęte ani kontynuowane do czasu zmniejszenia ryzyka do poziomu dopuszczalnego
Ryzyko wysokie Skala: 8–11 pkt.	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane zmniejszenie ryzyka
Ryzyko umiarkowane Skala: 4–7 pkt	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane i skuteczne zmniejszenie ryzyka
Ryzyko nieznaczne Skala: 1–3 pkt	Dopuszczalne (akceptowane)	Zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie

Załączniki do Analizy (należy wydrukować i dołączyć do dokumentacji):
Poradnik UODO dla szkół: https://uodo.gov.pl/pl/138/1473
(1) „DOBRE PRAKTYKI POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH PODCZAS LEKCJI ONLINE”
(2) „DANE OSOBOWE BEZPIECZNE PODCZAS ZDALNEGO NAUCZANIA”

[i] Przyjęte **wymagania wobec wiarygodnego dostawcy chmury obliczeniowej** zapewniającego odpowiednie warunki techniczne i organizacyjne przetwarzania danych oraz ochronę danych osobowych, w szczególności: (1) umowa regulująca relacje pomiędzy użytkownikiem chmury a dostawcą chmury, w tym w szczególności precyzyjne zapisy odnoszące się do ochrony danych osobowych np. wskazanie dostawcy jako podmiotu przetwarzającego wraz z potwierdzeniem spełniania wymagań (2) prawem właściwym dla umowy jest prawo polskie lub prawo kraju członkowskiego UE, (3) dostawca chmury w jurysdykcji EOG, (4) zapisy dotyczące przetwarzania w chmurze nie zmieniają się w czasie trwania umowy, (5) dane należą do użytkownika i znany jest tryb odzyskania danych po zakończeniu umowy, (6) zasady bezpieczeństwa są potwierdzone odpowiednimi certyfikatami

Cechy **eliminujące dostawcę usługi chmurowej** z możliwości wykorzystania w szkole, m.in.: (1) wykorzystanie danych użytkowników, zwłaszcza osób małoletnich, do profilowania i późniejszego wykorzystania tego profilu w celach komercyjnych, (2) przekazywanie danych osobowych lub stworzonych profili użytkowników, zwłaszcza osób małoletnich, innym podmiotom, które mogą wykorzystać je do celów komercyjnych, (3) żądanie przekazania przez użytkowników danych, które nie są niezbędne do wykonania usługi chmurowej np. dostęp do zdjęć, lokalizacji, kont w serwisach społecznościowych, (4) brak umownych relacji z dostawcą, w szczególności dotyczących ochrony danych osobowych np. odesłanie do strony internetowej z zasadami prywatności, które mogą się w każdej chwili zmienić, (5) dostawca w jurysdykcji spoza EOG, (6) brak lub nieznany sposób odzyskania danych po zakończeniu usługi, (7) brak, niepełna lub nieznana informacja dotycząca podprzetwarzających, (8) brak lub nieznane zasady zachowania bezpieczeństwa potwierdzone odpowiednimi certyfikatami