Informacja dot. przykładowej analizy ryzyka dla stosowania Microsoft Office 365 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:

   > *– Gdy szkoła powierzyła podmiotowi zewnętrznemu np. obsługę dziennika elektronicznego, dyrektor musi mieć pewność, że usługodawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi wskazane w RODO i chroniło prawa osób, których dane dotyczą. Dlatego też, przed podjęciem takiej decyzji szkoła powinna przeanalizować wszystkie możliwe rozwiązania oraz* ***oszacować ryzyko****.*

2. Analiza dotyczy wyłącznie produktów firmy Microsoft. W przypadku innych produktów należy taką analizę przeprowadzić samemu lub uzyskać ją z wiarygodnego źródła, np. producenta.

3. W przypadku życzliwego przyjęcia przedstawionej propozycji analizy udokumentowaniem działania szkoły może być wydruk zamieszczonej analizy ryzyka i zachowanie jej wraz z zalecaną przez UODO analizą zagrożeń. Dodatkowo szkoła może wydrukować „Postanowienia Dotyczące Usług Online" oraz „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft" (oba dokumenty znajdują się na stronie https://www.microsoftvolumelicensing.com/). Dokumentacja taka może stanowić podstawę dla wykazania właściwego podejścia do bezpieczeństwa i ochrony danych w procesie zdalnego nauczania.

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

ANALIZA RYZYKA PRZETWARZANIA DANYCH OSOBOWYCH

W PROCESIE ZDALNEGO NAUCZANIA

PRODUKT/USŁUGA: **MICROSOFT OFFICE 365 A1/A3/A5**

DATA: **MAJ 2020**

Analiza ryzyka przeprowadzona w celu określenia ryzyka przetwarzania danych osobowych w systemach zdalnego nauczania dla produktu Microsoft Office 365 A1/A3/A5 zgodnie z zaleceniami Urzędu Ochrony Danych Osobowych z dnia 31 marca 2020 roku, „DANE OSOBOWE BEZPIECZNE PODCZAS ZDALNEGO NAUCZANIA", https://uodo.gov.pl/pl/138/1473 oraz wynikające z realizacji wymagań dotyczących bezpiecznego przetwarzania danych osobowych zapisanych w Rozporządzenie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.)

Podstawowe informacje dotyczące procesu zdalnego nauczania

Ogólny opis procesu:

Pod pojęciem procesu zdalnego nauczania rozumie się w szczególności:

- Proces edukacji na odległość z udziałem nauczyciela i uczniów obejmujący m.in. wykład i prezentację nauczyciela, komunikację wideo, głosową i tekstową pomiędzy nauczycielem a poszczególnymi uczniami, komunikację wideo, głosową i tekstową pomiędzy uczniami, przekazywanie, edycję i współdzielenie plików (plików tekstowych, arkuszy obliczeniowych, prezentacji, zdjęć, filmów, linków itd. itp.), tworzenie i praca w klasach/zespołach/lekcjach; korzystanie ze wspólnego kalendarza
- (opcjonalnie) Integrację z e-dziennikiem
- Proces wykorzystania i integracji z systemem zewnętrznych zasobów edukacyjnych
- Proces współpracy na odległość pomiędzy nauczycielami obejmujący m.in. wszystkie w/w czynności, a także organizowanie narad i spotkań
- Proces współpracy na odległość pomiędzy nauczycielami a rodzicami pozwalający na komunikację wideo, głosową i tekstową, a także przekazywanie informacji o postępach ucznia, przekazywanie plików itd.
- Proces współpracy na odległość nauczycieli i kadry administracyjnej szkoły z innymi zewnętrznymi interesariuszami, m.in. kuratorium, ośrodkami doskonalenia nauczycieli, organami prowadzącymi, itd. itp.

Dane osobowe przetwarzane w procesie zdalnego nauczania:

- Dane uczniów (imię, nazwisko, adres poczty elektronicznej w systemie szkolnym – lub dane znajdujące się w e-dzienniku)
- Dane nauczycieli (imię, nazwisko, adres poczty elektronicznej w systemie szkolnym)
- Dane innych osób pracujących w szkole np. administracji w zakresie niezbędnym do realizacji obowiązku szkolnego
- Dane osobowe znajdujące się w materiałach służących do realizacji obowiązku szkolnego (m.in. pliki tekstowe, arkusze, prezentacje, zdjęcia itp.)
- Dane osobowe rodziców i opiekunów prawnych wymagane dla zachowania kontaktu i przekazywania informacji pomiędzy nimi a szkołą

Podstawowe informacje o procesie przetwarzania danych osobowych:

- Cel przetwarzania: realizacja obowiązku szkolnego
- Adekwatność danych osobowych: wyłącznie dane niezbędne dla realizacji celu przetwarzania
- Czas przetwarzania: wynikający z obowiązku szkolnego

Ogólny opis produktu/usługi używanego w procesie zdalnej edukacji:

Office 365 A1	Office 365 A3	Office 365 A5
• Internetowe wersje aplikacji Word, PowerPoint, Excel, OneNote i Outlook • Klasyczna wersja programu OneNote • Microsoft Teams — centrum cyfrowe, w którym zintegrowane są konwersacje, zawartość i aplikacje potrzebne w instytucji edukacyjnej do lepszej współpracy i zwiększania zaangażowania • Notesy zajęć i notesy dla personelu • Grupy PLC (Professional Learning Community) • Testy do samodzielnej oceny w usłudze Forms • Opowiadanie historii w formacie cyfrowym za pomocą aplikacji Sway • Zapewnianie pełnego dostępu do informacji i zaangażowania za pomocą witryn do komunikacji i witryn zespołów w całym intranecie przy użyciu programu SharePoint • Rozwiązania zapewniania zgodności za pomocą ujednoliconego centrum zbierania elektronicznych materiałów dowodowych • Zarządzanie prawami, ochrona przed utratą danych i szyfrowanie • Usługa wideo dla przedsiębiorstw do bezpiecznego tworzenia i udostępniania klipów wideo oraz zarządzania nimi w całej organizacji	• Internetowe wersje aplikacji Word, PowerPoint, Excel, OneNote i Outlook • Wersje klasyczne aplikacji pakietu Office na maksymalnie 5 komputerach PC lub Mac na użytkownika [3] • Aplikacje pakietu Office na maksymalnie 5 tabletach i 5 telefonach na użytkownika [4] • Microsoft Teams — centrum cyfrowe, w którym zintegrowane są konwersacje, zawartość i aplikacje potrzebne w instytucji edukacyjnej do lepszej współpracy i zwiększania zaangażowania • Notesy zajęć i notesy dla personelu • Grupy PLC (Professional Learning Community) • Testy do samodzielnej oceny w usłudze Forms • Opowiadanie historii w formacie cyfrowym za pomocą aplikacji Sway • Zapewnianie pełnego dostępu do informacji i zaangażowania za pomocą witryn do komunikacji i witryn zespołów w całym intranecie przy użyciu programu SharePoint • Rozwiązania zapewniania zgodności za pomocą ujednoliconego centrum zbierania elektronicznych materiałów dowodowych • Zarządzanie prawami, ochrona przed utratą danych i szyfrowanie	• Internetowe wersje aplikacji Word, PowerPoint, Excel, OneNote i Outlook • Wersje klasyczne aplikacji pakietu Office na maksymalnie 5 komputerach PC lub Mac na użytkownika [3] • Aplikacje pakietu Office na maksymalnie 5 tabletach i 5 telefonach na użytkownika [4] • Microsoft Teams — centrum cyfrowe, w którym zintegrowane są konwersacje, zawartość i aplikacje potrzebne w instytucji edukacyjnej do lepszej współpracy i zwiększania zaangażowania • Notesy zajęć i notesy dla personelu • Grupy PLC (Professional Learning Community) • Testy do samodzielnej oceny w usłudze Forms • Opowiadanie historii w formacie cyfrowym za pomocą aplikacji Sway • Zapewnianie pełnego dostępu do informacji i zaangażowania za pomocą witryn do komunikacji i witryn zespołów w całym intranecie przy użyciu programu SharePoint • Rozwiązania zapewniania zgodności za pomocą ujednoliconego centrum zbierania elektronicznych materiałów dowodowych • Zarządzanie prawami, ochrona przed utratą danych i szyfrowanie

• Opracowywanie aplikacji bez pisania kodu w celu szybkiego rozszerzania danych biznesowych za pomocą niestandardowych aplikacji mobilnych i sieci Web • Automatyzacja procesów biznesowych bez pisania kodu za pomocą automatyzacji przepływów pracy między aplikacjami i usługami • Planowanie harmonogramów i dziennych zadań za pomocą aplikacji Microsoft Teams • Poczta e-mail ze skrzynką pocztową o rozmiarze 50 GB [1] • Nielimitowany osobisty magazyn w chmurze [2] • Konferencje wideo HD • Maksymalna liczba użytkowników: nieograniczona • Nieograniczone miejsce do magazynowania wiadomości e-mail z archiwum zbiorczym • Zaawansowana poczta e-mail z funkcją archiwizacji, w tym archiwizacji ze względów prawnych	• Usługa wideo dla przedsiębiorstw do bezpiecznego tworzenia i udostępniania klipów wideo oraz zarządzania nimi w całej organizacji • Opracowywanie aplikacji bez pisania kodu w celu szybkiego rozszerzania danych biznesowych za pomocą niestandardowych aplikacji mobilnych i sieci Web • Automatyzacja procesów biznesowych bez pisania kodu za pomocą automatyzacji przepływów pracy między aplikacjami i usługami • Planowanie harmonogramów i dziennych zadań za pomocą aplikacji Microsoft Teams • Poczta e-mail ze skrzynką pocztową o rozmiarze 100 GB [1] • Nielimitowany osobisty magazyn w chmurze [2] • Nieograniczone miejsce do magazynowania wiadomości e-mail z archiwum zbiorczym • Zaawansowana poczta e-mail z funkcją archiwizacji, w tym na potrzeby wynikające z przepisów prawa • Konferencje wideo HD • Hostowanie spotkań dla nawet 10 000 osób dzięki funkcji zdarzeń na żywo usługi Microsoft Teams • Ocenianie ryzyka i dokładne analizowanie danych dotyczących potencjalnych zagrożeń dzięki usłudze Office 365 Cloud App Security • Planowanie w trybie online spotkań z nauczycielami przez rodziców lub opiekunów przy użyciu usługi Microsoft Bookings • Zaawansowana analiza osobista przy użyciu usługi MyAnalytics • Maksymalna liczba użytkowników: nieograniczona	• Usługa wideo dla przedsiębiorstw do bezpiecznego tworzenia i udostępniania klipów wideo oraz zarządzania nimi w całej organizacji • Opracowywanie aplikacji bez pisania kodu w celu szybkiego rozszerzania danych biznesowych za pomocą niestandardowych aplikacji mobilnych i sieci Web • Automatyzacja procesów biznesowych bez pisania kodu za pomocą automatyzacji przepływów pracy między aplikacjami i usługami • Planowanie harmonogramów i dziennych zadań za pomocą aplikacji Microsoft Teams • Poczta e-mail ze skrzynką pocztową o rozmiarze 100 GB [1] • Nielimitowany osobisty magazyn w chmurze [2] • Nieograniczone miejsce do magazynowania wiadomości e-mail z archiwum zbiorczym • Zaawansowana poczta e-mail z funkcją archiwizacji, w tym na potrzeby wynikające z przepisów prawa • Konferencje wideo HD • Hostowanie spotkań dla nawet 10 000 osób dzięki funkcji zdarzeń na żywo usługi Microsoft Teams • Ocenianie ryzyka i dokładne analizowanie danych dotyczących potencjalnych zagrożeń dzięki usłudze Office 365 Cloud App Security • Planowanie w trybie online spotkań z nauczycielami przez rodziców lub opiekunów przy użyciu usługi Microsoft Bookings • Kontrolowanie sposobu, w jaki pomoc techniczna uzyskuje dostęp do Twojej skrzynki pocztowej, za pomocą skrytki klienta • Chroni przed zaawansowanymi zagrożeniami, takimi jak wyłudzanie informacji i złośliwe oprogramowanie typu zero-day

		• Zaawansowana analiza osobista i organizacyjna przy użyciu usług MyAnalytics i Power BI Pro • Ulepszony wgląd w środowisko usługi Office 365 i kontrola nad nim • Tworzenie spotkań z numerem telefonicznym pozwalającym uczestnikom na dołączanie z telefonu dzięki usłudze Konferencje głosowe [5] • Nawiązywanie, odbieranie i przekazywanie połączeń za pomocą wielu różnych urządzeń, z opcją dodania pakietu telefonicznego.[6] • Maksymalna liczba użytkowników: nieograniczona

1 W przypadku subskrypcji, które nie obejmują pełnych, instalowanych aplikacji pakietu Office: Aby móc korzystać z już znanej, zaawansowanej aplikacji klienckiej, użytkownicy mogą łączyć się ze swoją pocztą e-mail klasy biznesowej przy użyciu następujących wersji programu Outlook: najnowszej wersji programu Outlook, Outlook 2013 i Outlook 2011 dla komputerów Mac. Poprzednie wersje programu Outlook, takie jak Outlook 2010 i Outlook 2007, mogą współdziałać z usługą Office 365 z ograniczoną funkcjonalnością. Ta zgodność z programem Outlook nie dotyczy planów Exchange Online Kiosk i Office 365 K1.

2 Nieograniczony osobisty magazyn w chmurze w przypadku kwalifikujących się planów dla subskrypcji obejmującej co najmniej pięciu użytkowników. W przeciwnym razie 1 TB na użytkownika. Firma Microsoft udostępni na początku 1 TB przestrzeni dyskowej usługi OneDrive dla Firm dla każdego użytkownika. Administratorzy mogą zwiększyć tę ilość do 5 TB na użytkownika. Dodatkową przestrzeń dyskową można uzyskać, kontaktując się z działem pomocy technicznej firmy Microsoft. Usługa OneDrive dla Firm zapewnia maksymalną przestrzeń dyskową wynoszącą 25 TB na użytkownika. Przestrzeń dyskową większą niż 25 TB poszczególni użytkownicy mogą uzyskać, korzystając z witryn zespołu programu SharePoint o pojemności 25 TB.

Klient synchronizacji usługi OneDrive dla Firm jest dostępny z pakietem Office 2016 lub subskrypcją usługi Office 365 obejmującą aplikacje pakietu Office 2016. Jeśli nie masz pakietu Office 2016, możesz też bezpłatnie pobrać klienta synchronizacji usługi OneDrive dla Firm.

3 Publisher i Access: tylko funkcje i program kliencki na komputery z systemem Windows. Nie można używać na różnych urządzeniach.

Większość planów, które nie zawierają klasycznej wersji pakietu Office, współdziała z najnowszą wersją pakietu Office oraz z pakietami Office 2013 i Office 2011 dla komputerów Mac. Poprzednie wersje pakietu Office, takie jak Office 2010 i Office 2007, mogą współdziałać z usługą Office 365 z ograniczoną funkcjonalnością. Ta zgodność z pakietem Office nie dotyczy planów Exchange Online Kiosk i Office 365 F1.

4 Dowiedz się więcej na temat aplikacji mobilnych w usłudze Office 365 dla firm. Zobacz listę urządzeń i aplikacji.

5 Dostępność konferencji głosowych zależy od regionu.

6 Dostępność pakietu telefonicznego zależy od regionu.

Źródła informacji dotyczące produktu/usługi używanego w procesie zdalnej edukacji:

- „Postanowienia Dotyczące Usług Online” (kwiecień 2020, https://www.microsoftvolumelicensing.com/)
- „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft” (kwiecień 2020, https://www.microsoftvolumelicensing.com/)
- Strona Microsoft Service Trust Portal; http://aka.ms/stp

Zagadnienie
1. Ocena wiarygodności dostawcy
Dostawca: Microsoft Corporation ***Kraj pochodzenia***: Irlandia (spółką właściwą dla UE jest Microsoft Ireland Operations Limited) ***Wiarygodność dostawcy (firma):*** Microsoft Corporation – od 1975 roku na rynku, kapitalizacja ponad 1000 miliardów dolarów, zatrudnienie ponad 100 tysięcy osób, producent oprogramowania takiego jak Windows, Office, Dynamics, Minecraft, jak również produktów takich jak Xbox, Surface. ***Wiarygodność dostawcy (wdrożenie odpowiednich środków technicznych i organizacyjnych - usługi chmurowe, w szczególności usługi pracy grupowej):*** ponad 150 centrów przetwarzania danych, 45 regionów, ponad 200 milionów użytkowników Office 365; inwestycje poświęcone bezpieczeństwu – powyżej 1 miliarda USD rocznie; ***Biuro dostawcy w Polsce***: tak, od 1993 roku. ***Możliwość uzyskania dodatkowego wsparcia w języku polskim:*** tak ***Zakres odpowiedzialności dostawcy (w tym powierzenie danych) opisany umową lub umowami w języku polskim:*** tak ***Umowa obowiązująca bez modyfikacji przez cały czas wykorzystania usługi:*** tak ***Prawo właściwe:*** prawo irlandzkie (w przypadku stosowania Standardowych Klauzul Umownych, będących załącznikiem dokumentu „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft" prawem właściwym jest prawo polskie) ***Umownie zapewnione warunki ciągłości działania usługi:*** tak
2. Własność danych
Klient zachowuje wszelkie prawa, tytuł i interes prawny do danych zgodnie z dokumentami „Postanowienia Dotyczące Usług Online" oraz „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft", które łącznie definiują relacje użytkownika (Klienta) z Microsoft. Microsoft nie będzie używać ani w inny sposób przetwarzać Danych Klienta ani Danych Osobowych na potrzeby: (a) profilowania użytkowników, (b) reklamy ani podobnych celów handlowych ani (c) badania rynku w celu opracowania nowych funkcji, usług lub produktów ani na żadne inne potrzeby, chyba że takie używanie lub przetwarzanie jest zgodne z udokumentowanymi instrukcjami Klienta.
3. Powierzenie przetwarzania danych
Umowa powierzenia. Powierzenie przetwarzania danych odbywa się na drodze umownej. Microsoft stosuje standardową umowę, dokumenty „Postanowienia Dotyczące Usług Online" oraz „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft", które łącznie definiują relacje Klienta z Microsoft, w tym także proces powierzenia danych. ***Administrator i podmiot przetwarzający.*** Klient jest administratorem danych osobowych. Microsoft jest podmiotem przetwarzającym, za wyjątkiem zamkniętej czynności listy opisanych w dokumencie Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft" kiedy przyjmuje rolę administratora. Lista obejmuje: (1) fakturowanie i zarządzanie kontami; (2) rozliczanie wynagrodzeń (na przykład obliczanie prowizji dla pracowników i dodatków motywacyjnych dla partnerów); (3) sprawozdawczość wewnętrzna i modelowanie (na przykład prognozowanie, księgowanie przychodów, planowanie wydajności, realizacja strategii produktowych); (4) zwalczanie oszustw, cyberprzestępczości lub ataków cybernetycznych, które mogą mieć wpływ na Microsoft lub Produkty

Microsoft; (5) poprawa podstawowych funkcji związanych z dostępnością, prywatnością lub efektywnością energetyczną oraz (6) sprawozdawczość finansowa i przestrzeganie obowiązków prawnych.

Opis zobowiązań dla podmiotu przetwarzającego wynikające z przepisów RODO jakie bierze na siebie Microsoft znajduje się szczegółowo opisany w Załączniku „Postanowienia wynikające z unijnego ogólnego rozporządzenia o ochronie danych" w dokumencie „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft".

Podprzetwarzający. Microsoft może zaangażować podprzetwarzających. Microsoft ponosi odpowiedzialność za za przestrzeganie przez te podmioty obowiązków wynikających z dokumentów „Postanowienia Dotyczące Usług Online" oraz „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft". Lista podprzetwarzających jest dostępna dla Klienta, jest on także z uprzedzeniem powiadamiany o zaangażowaniu nowych podprzetwarzających oraz jest przygotowana procedura pozwalająca Klientowi zrezygnować z usługi w przypadku braku zgody na nowego podprzetwarzającego.

4. Lokalizacja danych

Lokalizacja: miejsce przechowywania danych wynika z wyboru regionu przez Klienta.
Microsoft przestrzega wymagań określonych w przepisach prawa ochrony danych przyjętych w krajach Europejskiego Obszaru Gospodarczego i Szwajcarii w zakresie zbierania, używania, przekazywania, zatrzymywania oraz innego przetwarzania Danych Osobowych. Wszystkie przypadki przekazywania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej są odpowiednio zabezpieczone zgodnie z art. 46 RODO oraz że takie przekazywanie i zabezpieczenia są dokumentowane zgodnie z art. 30 ust. 2 RODO.

Standardowe klauzule umowne. Załącznikiem do dokumentu „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft" są Standardowe Klauzule Umowne, które zapewniają bezpieczeństwo także w przypadku, gdyby doszło do przetwarzania danych osobowych poza EOG.

5. Bezpieczeństwo przetwarzania danych

Środki techniczne i organizacyjne: Microsoft wdraża i utrzymuje odpowiednie zabezpieczenia o charakterze technicznym i organizacyjnym w celu ochrony Danych Klienta i Danych Osobowych przed przypadkowymi lub niezgodnymi z prawem przypadkami uzyskiwania dostępu do nich, modyfikacji, ujawniania, utraty lub zniszczenia podczas ich przekazywania, przechowywania lub innego przetwarzania.

Microsoft udostępnia Klientowi wszelkie takie zasady wraz z opisami istniejących mechanizmów kontroli bezpieczeństwa dotyczących danej Usługi Online oraz innymi informacjami zasadnie wymaganymi przez Klienta w związku z procedurami i zasadami bezpieczeństwa Microsoft. Szczegóły dotyczące środków bezpieczeństwa są opisane w Aneksie A w dokumencie „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft".

Szyfrowanie danych. Dane są szyfrowane zarówno podczas przechowywania (ang. *at rest*) jak i podczas przesyłania (ang. *in transit*)

Personel Microsoft. Microsoft gwarantuje, że personel Microsoft zajmujący się przetwarzaniem Danych Klienta i Danych Osobowych

a) będzie przetwarzać takie dane wyłącznie na polecenie Klienta lub w sposób opisany w tym Dodatku dotyczącego Ochrony Danych
b) będzie zobowiązany do zachowania w poufności i zabezpieczenia wszelkich takich danych nawet po zakończeniu okresu zatrudnienia.

Microsoft przeprowadza dla swoich pracowników mających dostęp do Danych Klienta i Danych Osobowych okresowe, obowiązkowe szkolenia i kampanie informacyjne w zakresie bezpieczeństwa i prywatności danych zgodnie ze stosownymi Wymogami dotyczącymi Ochrony Danych i standardami branżowymi.

Stosowanie międzynarodowych norm bezpieczeństwa. Microsoft w dokumentach „Postanowienia Dotyczące Usług Online" oraz „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft" umownie deklaruje utrzymanie zgodności z normami ISO 27001, ISO 27002 oraz ISO 27018. Każda Podstawowa Usługa Online jest także zgodna ze standardami kontroli i normami wskazanymi w tabeli w Załączniku 1 do „Postanowień Dotyczących Usług Online". Audyty zgodności z normami są prowadzone przez niezależne firmy audytorskie przynajmniej dwa razy w roku

Microsoft na bieżąco publikuje na stronach portalu „Microsoft Service Trust Center" dodatkowe informacje o innych stosowanych normach, przeprowadzonych audytach, wynikach testów penetracyjnych i zasadach bezpieczeństwa przetwarzania danych (m.in. ISO 27701, ISO 20000, SOC 1, SOC 2, NIST 800-53). Niszczenie nośników następuje zgodnie z normą NIST 800-88.

Audyty bezpieczeństwa. Microsoft przeprowadza audyty zabezpieczeń komputerów, środowiska informatycznego i fizycznych centrów przetwarzania danych używanych przez Microsoft do przetwarzania Danych Klienta i Danych Osobowych w następujący sposób:

a) Jeśli standard lub norma zakładają przeprowadzanie audytów, audyt zostanie przeprowadzony przynajmniej raz w roku.

b) Każdy audyt zostanie przeprowadzony zgodnie ze standardami i przepisami urzędu regulacyjnego lub akredytacyjnego dla każdego obowiązującego standardu lub normy.

c) Każdy audyt zostanie przeprowadzony przez wykwalifikowanych, niezależnych audytorów zewnętrznych wybranych i opłaconych przez Microsoft.

Wyniki audytu są przedstawiane w formie raportu, który Microsoft udostępni na stronach portalu „Microsoft Service Trust Center". Raport z Audytu stanowi Informacje Poufne Microsoft i jednoznacznie przedstawia wszelkie istotne ustalenia poczynione przez audytora. Microsoft zobowiązuje się bezzwłocznie wyeliminować problemy wskazane w Raporcie z Audytu Microsoft zgodnie z zaleceniami audytora. Raport z Audytu Microsoft podlega ograniczeniom Microsoft i audytora dotyczącym poufności i rozpowszechniania.

Inne. Microsoft wypełnia wymagania dla Dostawcy Usług Cyfrowych dla wykorzystania w realizacji Usług Kluczowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa.

Narzędzia dodatkowe i administracyjne. Microsoft udostępnia Klientowi narzędzia administracyjne i pomocnicze pozwalające na odpowiednie zabezpieczanie, monitorowanie i raportowanie procesów przetwarzania danych osobowych. Narzędzia te pozwalają na stworzenie przez Klienta adekwatnych rejestrów czynności przetwarzania, monitorowania bezpieczeństwa i używania usług chmurowych, podnoszenia bezpieczeństwa systemu, realizacji praw osób, których dane dotyczą, a nawet całościowej analizy wypełniania wymagań RODO. Dostępność narzędzia mogą się różnić w zależności od wybranej wersji licencji. Przykładami takich narzędzi mogą być:

- E-discovery – pozwalające na identyfikację danych osobowych w nieustrukturyzowanych zbiorach danych, np. wśród plików tworzonych przez aplikacje Office; w szczególności przydatny przy realizacji żądań osób, których dane dotyczą
- Azure Information Protection – system klasyfikowania danych i możliwości odpowiedniego działania z tymi danymi; realizacja wymagań z art. 5 RODO
- Advanced Threat Protection – zabezpieczenie przed przesyłaniem niebezpiecznych plików lub linków do odbiorców, ochrona przed atakami phishingowymi

- Data Loss Protection – zabezpieczenie przed nieautoryzowanym wysłaniem danych osobowych;
- Compliance Manager – narzędzie do zarządzania całością wymagań dotyczących ochrony danych osobowych w organizacji

6. Powiadomienie o naruszeniu zabezpieczeń

W przypadku każdego przypadku naruszenia bezpieczeństwa klasyfikowanego jako Naruszenie Zabezpieczeń Microsoft bezzwłocznie i w każdym przypadku nie później niż w ciągu 72 godzin wyśle stosowne powiadomienie.

7. Zarządzanie ciągłością działania

Microsoft posiada plany awaryjne dla placówek, w których są zlokalizowane systemy informatyczne Microsoft przetwarzające Dane Klienta. Nadmiarowa pamięć masowa Microsoft i procedury Microsoft dotyczące odzyskiwania danych, umożliwiają podjęcie próby rekonstrukcji Danych Klienta w ich oryginalnym lub ostatnio zreplikowanym stanie, w jakim znajdowały się przed ich utratą lub zniszczeniem.

Microsoft posiada certyfikaty ISO 22301 dla wykazania prawidłowego procesu ciągłości działania w swoich usługach.

8. Usuwanie danych i zakończenie usługi

Przez cały czas obowiązywania subskrypcji, Klient w każdej chwili może uzyskiwać dostęp do Danych Klienta przechowywanych w danej Usłudze Online. Ponadto może dane wyodrębniać i usuwać. Microsoft zatrzymuje Dane Klienta zapisane w Usługach Online na koncie o ograniczonej funkcjonalności przez 90 dni od daty wygaśnięcia lub wypowiedzenia uzyskanej przez Klienta subskrypcji w celu umożliwienia Klientowi odzyskania danych. Po upływie tego 90-dniowego okresu zatrzymania Microsoft wyłączy konto Klienta i usunie Dane Klienta i Dane Osobowe w ciągu dodatkowych 90 dni, (chyba że na mocy przepisów prawa właściwego dozwolone lub wymagane jest zatrzymanie tych danych lub Microsoft jest do tego upoważniony na mocy tego Dodatku dotyczącego Ochrony Danych).

9. Obowiązki Klienta

Klient ponosi wyłączną odpowiedzialność za ustalenie w niezależny sposób, czy środki techniczne i organizacyjne dotyczące Usługi Online spełniają jego wymagania, w tym pozwalają wykonać obowiązki Klienta w zakresie bezpieczeństwa na mocy właściwych Wymogów dotyczących Ochrony Danych. Klient przyznaje i zgadza się, że (uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania Danych Osobowych, a także ryzyko, jakie stwarza ono dla poszczególnych osób) procedury i zasady bezpieczeństwa wdrożone i utrzymywane przez dostawcę zapewniają stopień bezpieczeństwa odpowiadający ryzyku związanemu z Danymi Osobowymi administrowanymi przez Klienta. Klient jest odpowiedzialny za wdrażanie i utrzymywanie środków ochrony prywatności i zabezpieczeń dla pochodzących od Klienta składników lub elementów sterujących.

Skrócona lista kontrolna		
Lp.	**Pytanie**	**Odpowiedź**
1.	Podmiot świadczący usługę chmurową jest zarejestrowany w kraju UE	TAK
2.	Umowa jest zawarta w języku polskim	TAK
3.	Powierzenie przetwarzania danych osobowych ma formę pisemną	TAK
4.	Umowa nie ulega zmianom w trakcie jej trwania	TAK
5.	Szkoła (administrator) ma pełną kontrolę, podmiot świadczący usługę chmurową wypełnia rolę podmiotu przetwarzającego	TAK/TAK
6.	Dane są zlokalizowane na terenie Polski/UE	NIE/TAK
7.	Zagwarantowane szyfrowanie danych w spoczynku/podczas transmisji	TAK/TAK
8.	Podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych	TAK
9.	Personel mający dostęp do danych Klienta podlega obowiązkowi zachowania poufności	TAK
10.	Podmiot przetwarzający stosuje odpowiednie środki techniczne i organizacyjne w celu ochrony danych. Środki te są zgodne z wymaganiami określonymi w normach ISO 27001, ISO 27002, ISO 27018 ISO 27017, ISO 22301	TAK
11.	Podmiot przetwarzający regularnie poddaje się zewnętrznej kontroli niezależnych audytorów, co jest potwierdzone certyfikatami	TAK
12.	Uwzględniając charakter przetwarzania oraz dostępne informacje, podmiot przetwarzający pomaga Klientowi wywiązać się z obowiązków określonych w art. 32–36 RODO	TAK
13.	Podmiot przetwarzający regularne testuje i oceniania skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. (Art. 32 ust. 1)	TAK
14.	Podmiot przetwarzający korzysta z usług podwykonawców, którzy zostali przez niego zweryfikowani pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych, a lista podwykonawców jest dostępna dla administratora	TAK/TAK
15.	Po zakończeniu świadczenia usług związanych z przetwarzaniem i zależnie od decyzji Klienta, podmiot przetwarzający usuwa albo zwraca Klientowi wszelkie Dane Osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie Danych Osobowych	TAK

Wnioski

Zastosowanie rozwiązania Microsoft Office 365 w procesie zdalnego nauczania obciążone jest niewielkim ryzykiem związanym z przetwarzaniem danych osobowych z wykorzystaniem tego narzędzia. Dostawca rozwiązania jest firmą wiarygodną, od lat obecną na wielką skalę na rynku polskim i światowym, a jednocześnie przykłada należytą uwagę do wymagań ochrony danych osobowych. Szkoła pozostaje administratorem i ma pełną kontrolę nad danymi, także w przypadku zakończenia usługi. Microsoft – pełniący rolę podmiotu przetwarzającego - reprezentuje przedsiębiorstwo z kraju Unii Europejskiej, zaś standardowa umowa jest w języku polskim.

Poziom bezpieczeństwa w części chmurowej w wersji standardowej jest wyższy niż możliwy do uzyskania we własnej infrastrukturze, a co więcej będzie dostosowywany do dalszych wymagań bezpieczeństwa bez żadnych dodatkowych nakładów po stronie szkoły. Co więcej, możliwe jest zastosowanie dodatkowych narzędzi lub korzystanie w niezbędnym zakresie z wyższych licencji produktu tak aby to bezpieczeństwo jeszcze podnieść. Narzędzia jakimi dysponuje administrator podniosą rozliczalność procesu przetwarzania danych osobowych i możliwości reagowania na żądania osób, których dane dotyczą.

Przygotowana analiza zagrożeń oraz niniejsza analiza ryzyka pozwalają stwierdzić, że z pomocą opisanego produktu można usunąć lub znacznie zredukować zagrożenia w procesie zdalnego nauczania.

Data:	Podpisy: