RODO w czasie pandemii (materiał dla sektora edukacji)

Poniższe informacje nie stanowią opinii prawnej i mają wyłącznie charakter orientacyjny. Prosimy o dokonanie swojej analizy przed podjęciem decyzji co do sposobu postępowania.

I. Informacje ogólne

1. Czy w okresie pandemii w edukacji obowiązują przepisy RODO?

Tak, przepisy RODO obowiązują. Potwierdza to też oświadczenie przewodniczącej Europejskiej Rady Ochrony Danych (EDPB) ws. przetwarzania danych osobowych w kontekście pandemii COVID-19, które zostało także opublikowane 16 marca 2020 przez Urząd Ochrony Danych Osobowych. Andrea Jelinek powiedziała: *„Przepisy w zakresie ochrony danych (takie jak RODO) nie utrudniają działań podejmowanych w walce z pandemią koronawirusa. Chciałabym jednak podkreślić, że nawet w tych wyjątkowych czasach administrator musi zapewnić ochronę danych osobowych osób, których one dotyczą. W związku z tym należy wziąć pod uwagę szereg czynników, aby zagwarantować zgodne z prawem przetwarzanie danych osobowych.*"

Dodatkowo warto także przywołać zalecenia UODO w publikacji z 17 marca 2020 dotyczącej Ochrony Danych Osobowych podczas pracy zdalnej.

31 marca 2020 Urząd Ochrony Danych Osobowych opublikował także DOBRE PRAKTYKI POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH PODCZAS LEKCJI ONLINE, gdzie wskazał na co należy zwracać uwagę w celu zachowania właściwej ochrony danych w szkole.

2. Czy mogę stosować publiczną chmurę obliczeniową dla pracy zdalnej w edukacji i przetwarzać w niej dane osobowe?

Tak. Nie ma przeciwwskazań by przetwarzać dane osobowe w chmurze publicznej. Trzeba jednak wyraźnie powiedzieć, że różne są modele usług chmurowych. Warto zwrócić uwagę, czy dostawca usługi chmurowej generalnie działa jako przetwarzający dane osobowe przekazywane przez użytkowników. W takim przypadku, RODO wskazuje bardzo wyraźnie jakie warunki powinien spełniać dostawca usługi chmurowej - podmiot przetwarzający. Nie każda chmura i nie każdy dostawca wypełnia te wymagania, a wybór dostawcy należy do obowiązków administratora i to administrator ponosi odpowiedzialność za ten wybór.

3. Czy mogę przetwarzać dane osobowe dzieci w publicznej chmurze obliczeniowej?

Tak. RODO nakłada na administratora konieczność szczególnej staranności i ochrony w przypadku przetwarzania danych dzieci, ale nie wyklucza ani przetwarzania takich danych, ani możliwości przetwarzania ich w chmurze. Warto przywołać motyw (38) RODO:

(38) Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich. Zgoda osoby sprawującej władzę rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku.

Motyw ten bardzo wyraźnie wskazuje jakich usług chmurowych nie powinno stosować się w praktyce edukacyjnej – tych, w których dostawca wykorzystuje dane do celów marketingowych, tworzenia profili osobowych lub profili użytkownika. Trzeba koniecznie zwrócić na to uwagę, gdyż wiele darmowych i popularnych aplikacji konsumenckich bazuje na modelu usługa za dane i profiluje swoich użytkowników pod kątem późniejszego tworzenia profili dla reklamodawców (tj. dostawca staje się odrębnym administratorem przekazanych danych i może je wykorzystywać do swoich celów). Aplikacje takie nie powinny być stosowane w edukacji!

4. Czy mogę przetwarzać w chmurze publicznej szczególne kategorie danych osobowych?

Tak. UCHWAŁA NR 97 RADY MINISTRÓW z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa", czyli Uchwała WIIP, która dotyczy wszystkich podmiotów sektora finansów publicznych, przewiduje zastosowanie chmury publicznej również do systemów, w których będą przetwarzane szczególne kategorie danych osobowych (zwane popularnie „danymi wrażliwymi"). Nie każda chmura i nie każdy dostawca wypełnia wymagania, a wybór dostawcy należy do obowiązków administratora i to administrator ponosi odpowiedzialność za ten wybór.

5. Czy należy uzyskać zgodę na przetwarzanie danych?

Można oceniać, że powierzenie przetwarzania danych nie wymaga specjalnej zgody pracownika lub ucznia oraz jest dopuszczalne w zakresie, w którym placówka oświaty sama może przetwarzać dane osobowe. Przetwarzanie danych osobowych pracowników i uczniów przez placówki oświaty nie wymaga ich zgody w zakresie, w którym dana placówka upoważniona jest do ich przetwarzania na podstawie przepisów prawa, np. jako pracodawca lub w celu dokumentacji procesu przebiegu nauczania.

Przetwarzanie danych, w zakresie nieobjętym upoważnieniem wynikającym z przepisów prawa i w braku innych podstaw ich przetwarzania, wymagać może zgody. W takim przypadku, w celu wyrażenia zgody na przetwarzanie danych niezbędne jest posiadanie pełnej zdolności do czynności prawnych, którą co do zasady posiadają osoby pełnoletnie. Uczeń, który ukończył 18 lat i ma pełną zdolność do czynności prawnych może więc samodzielnie udzielić zgody na przetwarzanie jego danych osobowych. W przypadku osób niepełnoletnich co do zasady niezbędna będzie zgoda rodzica lub opiekuna. Należy wskazać, że osoba, która ukończyła 13 lat posiada ograniczoną zdolność do czynności prawnej i co do zasady, może dokonywać czynności prawnych za zgodą przedstawiciela ustawowego. Natomiast zgodnie z art. 8 ust. 1 RODO oraz polskimi przepisami, w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodę na przetwarzanie danych mogą wyrazić osoby, które ukończyły 16 lat. W przypadku dzieci młodszych zgodę musi wyrazić lub ją zaaprobować osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem. Z uwagi na wiele funkcjonalności oferowanych przez dostawców w ramach usług chmurowych bezpieczniej założyć ten wyższy próg wiekowy.

Zgoda może być wyrażona mailem lub przez e-Dziennik lub podczas logowania się do innego narzędzia, jakie szkoła przygotowała do kształcenia na odległość (np. poprzez zaznaczenie odpowiedniego „okienka"). W dalszej analizie należy rozważyć, czy zgoda ma charakter czasowy (konieczność realizowania obowiązku zapisanego w par. 7 Rozporządzenia z 20 marca) czy ostateczny.

6. Czy dane w chmurze publicznej stosowanej w edukacji muszą być przechowywane w Polsce?

Nie. Co więcej, art. 1 ust. 3 RODO wyraźnie wskazuje, że nie ogranicza się i nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

7. Na co zwrócić uwagę, jeśli dane osobowe są przetwarzane poza granicami Polski?

RODO w identyczny sposób traktuje przetwarzanie danych w Polsce oraz w krajach Europejskiego Obszaru Gospodarczego. Nie oznacza to, że dane nie mogą być przetwarzane poza tym obszarem, ale muszą być spełnione dodatkowe warunki np. decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony, zawarcie standardowych klauzul umownych (SCC) z dostawcą chmurowym. Mechanizm takiej ochrony jest opisany m.in. w art. 44-50 RODO. W telegraficznym skrócie przedstawiając SCC zobowiązują podmiot przetwarzający spoza EOG (importer danych) do zachowania takich reguł ochrony danych jakie wymagane są w Unii Europejskiej bez względu na to, gdzie odbywa się jakikolwiek proces przetwarzania.

8. Czy trzeba stosować Dekalog Chmuroluba?

Dekalog Chmuroluba został opublikowany w 2013 roku, na ponad pięć lat przed wejściem w życie RODO. „IT w Administracji" zamieściło odpowiedź rzecznika prasowego UODO, p. Adama Sanockiego, m.in. *„Informacja dotycząca dekalogu chmuroluba znajduje się na archiwalnych stronach GIODO (…). Materiał ten ma więc charakter archiwalny i nie może być traktowany jako aktualne stanowisko Prezesa Urzędu Ochrony Danych Osobowych".* Do zapoznania się z całym stanowiskiem odsyłamy do „IT w Administracji" (luty 2020).

II. Informacje dotyczące Microsoft

1. Gdzie znajdują się informacje regulujące umowne relacje pomiędzy administratorem a Microsoft?

Informacje dotyczące relacji między administratorem a Microsoft są określone przede wszystkim w dokumentach takich, jak Postanowienia Dotyczące Usług Online (tzw. **OST**) czy Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft (tzw. **DPA**). Administrator może zapoznać się z dokumentacją określającą jego relację z Microsoft również na stronie: www.microsoftvolumelicensing.com.

Na tej stronie znajduje się więcej przydatnych informacji np. jakie jednostki mają prawo korzystać z licencji edukacyjnych (patrz: Qualified Education User Definition) czy też warunki świadczenia serwisu (patrz: Online Services SLA).

2. Czy muszę mieć z Microsoft umowę podpisaną na papierze?

Nie. Umowa z Microsoft na świadczenie usług online (podobnie jak licencja na oprogramowanie) ma charakter standardowy i nie podlega negocjacjom. Powinienem odnotować, w celu rozliczalności procesu przetwarzania, te czynności jakie zostały dokonane w momencie uruchomienia usługi.

3. Gdzie znajduje się umowa powierzenia danych?

Trzon umową powierzenia danych stanowią Postanowienia Dotyczące Usług Online (OST) oraz Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft (DPA).

4. Mamy naszą własną umowę powierzenia – czy Microsoft ją podpisze?

Nie. Umową powierzenia danych są dokumenty „Postanowienia Dotyczące Usług Online" (OST) oraz „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft" (DPA).

Trzeba pamiętać, że jednym z warunków właściwego wypełniania roli podmiotu przetwarzającego przez Microsoft jest konieczność przystosowywania się do zmieniających się wymagań prawnych, technicznych i organizacyjnych. Dzięki jednolitej standardowej umowie jest ma pewność, że w przypadku zmiany wymagań wszyscy klienci będą na pewno mieli zapewnione właściwe warunki przetwarzania danych. To wypełnienie wymagań zapisanych m.in. w motywie (81) oraz art. 28 i 32 rodo.

> *(81) Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. (…)*

5. **Czy muszę szukać w innych dokumentach niż DPA zapisów związanych z ochroną danych?**

Nie. Bardzo wyraźnie mówi o tym samo DPA:

> *W przypadku sprzeczności lub niezgodności między postanowieniami tego Dodatku dotyczącego Ochrony Danych a innymi postanowieniami zawartej przez Klienta umowy licencjonowania zbiorowego (w tym Postanowieniami dotyczącymi Produktów lub Postanowieniami dotyczącymi Usług Online) postanowienia tego Dodatku dotyczącego Ochrony Danych mają charakter rozstrzygający.*

6. **Czy zapisy OST i DPA mogą się zmienić w trakcie trwania umowy?**

Nie. Odpowiednie zapisy znajdują się w obu dokumentach.

OST:

> *Właściwe Aktualizacje i Postanowienia Dotyczące Usług Online*
>
> *W przypadku odnowienia lub zakupu przez Klienta nowej subskrypcji Usługi Online wiążące pozostaną obowiązujące wówczas Postanowienia Dotyczące Usług Online i nie ulegną one zmianie przez cały okres trwania uzyskanej przez Klienta subskrypcji danej Usługi Online.*

DPA:

> *Właściwy Dodatek dotyczący Ochrony Danych i aktualizacje*
>
> *W przypadku odnowienia lub zakupu przez Klienta nowej subskrypcji Usługi Online zastosowanie mają postanowienia obowiązującego wówczas Dodatku dotyczącego Ochrony Danych i nie ulegną one zmianie przez cały okres obowiązywania uzyskanej przez Klienta subskrypcji takiej Usługi Online*

7. **Kto jest właścicielem danych podczas przetwarzania w chmurze Microsoft?**

Osoba zawierająca umowę z Microsoft (Klient) zachowuje wszelkie prawa, tytuł prawny i interes prawny do danych Klienta (w tym plików zawierających tekst, dźwięki, filmy i obrazy oraz oprogramowanie) przekazane Microsoft przez Klienta (lub w jego imieniu) w wyniku korzystania z usług online.

8. **Jaką rolę ma Microsoft w procesie przetwarzania danych osobowych?**

Microsoft jest podmiotem przetwarzającym dane osobowe, z wyjątkiem sytuacji, (a) w której administrator występuje jako podmiot przetwarzający Dane Osobowe, zaś Microsoft jest dalszym przetwarzającym, lub (b) gdy szczegółowe postanowienia dokumentacji np. Postanowień dotyczących usług online, stanowią inaczej. Microsoft działa jako administrator w przypadku fakturowania i zarządzania kontami, rozliczania wynagrodzeń (na przykład obliczania prowizji dla pracowników i dodatków motywacyjnych dla partnerów) czy zwalczania oszustw, cyberprzestępczości lub ataków cybernetycznych, które mogą mieć wpływ na Microsoft lub Produkty Microsoft. Wszystkie informacje znajdują się w dokumencie DPA „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft”

9. **Gdzie znajduje się opis zobowiązań Microsoft jako podmiotu przetwarzającego?**

Opis zobowiązań Microsoft znajduje się w dokumencie DPA „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft", w szczególności w Załączniku 3 POSTANOWIENIA WYNIKAJĄCE Z UNIJNEGO OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH, jak również w Załączniku 1 do Postanowień Dotyczących Usług Online (OST).

10. **Czy Microsoft wykorzystuje podprzetwarzających i czy jest dostępna ich lista?**

Tak. Microsoft ponosi odpowiedzialność za przestrzeganie przez Podmioty Podprzetwarzające Microsoft obowiązków Microsoft wynikających z tego Dodatku dotyczącego Ochrony Danych (DPA). Podprzetwarzający będzie mógł uzyskiwać dostęp do Danych Klienta lub Danych Osobowych i używać ich wyłącznie w celu świadczenia usług zleconych mu przez Microsoft i nie będzie mógł korzystać z Danych Klienta ani Danych Osobowych w żadnym innym celu. Microsoft zapewni, że Podmioty Podprzetwarzające są związane pisemnymi umowami wymagającymi od nich zapewnienia co najmniej tego samego stopnia ochrony danych, jaki jest wymagany od Microsoft na mocy tego Dodatku dotyczącego Ochrony Danych. Microsoft zgadza się nadzorować Podmioty Podprzetwarzające w celu zapewnienia, że wspomniane zobowiązania umowne zostaną dotrzymane. Pozostałe szczegółowe zapisy znajdują się w dokumencie „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft" (DPA).

Lista podprzetwarzających znajduje się na stronach Microsoft Service Trust Portal, w sekcji Data Protection Resources.

11. **Gdzie są przechowywane moje dane?**

W chwili uruchomienia usługi Klient wybiera region, w którym będą przechowywane jego dane. W Załączniku 1 do Postanowień Dotyczących Usług Online wskazano zasady i procedury bezpieczeństwa dotyczące Podstawowych Usług Online, jak również miejsce przechowywania danych magazynowych Klienta (tzw. danych w spoczynku) w przypadku Podstawowych Usług Online. Bardziej szczegółowe informacje o miejscu przechowywania danych magazynowych można znaleźć na stronie https://products.office.com/en-us/where-is-your-data-located i https://products.office.com/pl-pl/where-is-your-data-located#office-ContentAreaHeadingTemplate-bkjgypc

12. **Czy Microsoft stosuje Standardowe Klauzule Umowne?**

Tak. Microsoft stosuje standardowe klauzule umowne w modelu administrator (Klient) – przetwarzający (Microsoft Corporation). Ich treść jest zawarta w Załączniku nr 2 do Dodatku dotyczącego Ochrony Danych w ramach Usług Online Microsoft (DPA).

13. **Co się dzieje z moimi danymi po zakończeniu usługi chmurowej Microsoft?**

Microsoft zatrzyma 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. Klient może w tym czasie sam usunąć dane lub przenieść je do innych usług. 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 Dodatku dotyczącego Ochrony Danych. Inne zasady mogą obowiązywać w przypadku wersji próbnych.

14. **Jakie jest prawo właściwe?**

Prawem właściwym dla umowy jest standardowo prawo irlandzkie. Standardowe Klauzule Umowne podlegają prawu państwa członkowskiego, w którym Administrator prowadzi działalność.

15. **Gdzie można znaleźć więcej informacji na środków stosowanych przez Microsoft dla ochrony danych?**

Opis środków stosowanych przez Microsoft dla zapewnienia bezpieczeństwa danych stanowi element „Dodatku dotyczącego Ochrony Danych w ramach Usług Online Microsoft" (DPA). Aneks A do wskazanego Dodatku zawiera dokładny opis stosowanych przez Microsoft środków ochrony danych.

Poza tym, Microsoft prowadzi regularne audyty zabezpieczeń komputerów, środowiska informatycznego i fizycznych centrów przetwarzania danych. Wyniki tych audytów są ujmowane w formie raportów („Raport z Audytu Microsoft"), dostępnych pod adresem: https://servicetrust.microsoft.com/ (Microsoft Service Trust Portal). Poza Raportami z Audytów, znajduje się tam również szereg innych informacji dotyczących usług online Microsoft, w tym środków bezpieczeństwa, przetwarzania danych osobowych. Informacje dotyczą m.in. certyfikatów i raportów związanych z normami ISO 27001, 27018 czy 22301, spełaniania wymogów standardów SOC 1 i SOC 2, raportów z testów penetracyjnych i wielu innych.

16. **Czy po okresie pandemii powinienem zakończyć eksploatację rozwiązania chmurowego Microsoft stosowanego do edukacji online?**

Nie. Usługi chmurowe Microsoft pozwalają na wypełnienie wymagań ochrony danych zarówno w szczególnym okresie związanym z pandemią, jak i w normalnych warunkach prowadzenia edukacji.

Analizowane dokumenty: Wśród dokumentów są w szczególności 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), czyli rodo, 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, 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, a także UCHWAŁA NR 97 RADY MINISTRÓW z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa", czyli Uchwała WIIP.