SOŁTYSIŃSKI
KAWECKI
SZLĘZAK

PARTNERZY | OF COUNSEL
prof. zw. dr hab. STANISŁAW SOŁTYSIŃSKI
dr ANDRZEJ W. KAWECKI*
dr hab. ANDRZEJ SZLĘZAK
PIOTR ANDRZEJAK
ŁUKASZ BERAK
JAROSŁAW BIERONSKI
KRZYSZTOF CICHOCKI
ROBERT GAWAŁKIEWICZ
SZYMON GOGULSKI
KRZYSZTOF KANTON
TOMASZ KAŃSKI
TOMASZ KONOPKA
SŁAWOMIR ŁUCZAK
dr KATARZYNA MICHAŁOWSKA
JUSTYNA MŁODZIANOWSKA
prof. zw. dr hab. AURELIA NOWICKA
* Admitted also in New York

ul. Jasna 26 | 00-054 Warszawa
tel. +48 22 608 70 00 | fax +48 22 608 70 70
office@skslegal.pl

ul. Mickiewicza 35 | 60-837 Poznań
tel. +48 61 856 04 20 | fax +48 61 856 05 67
office.poznan@skslegal.pl

ul. Chorzowska 152 | 40-101 Katowice
Silesia Business Park | budynek A
tel. +48 32 731 59 86 | fax +48 32 731 59 90
office.katowice@skslegal.pl

pl. Solny 16 | 50-062 Wrocław
tel. +48 71 346 77 00 | fax +48 71 346 77 09
office.wroclaw@skslegal.pl

www.skslegal.pl

PARTNERZY | OF COUNSEL
dr MARCIN OLECHOWSKI
dr RUDOLF OSTRIHANSKY
ROCH PAŁUBICKI
KRZYSZTOF PAWLISZ
JANUSZ SIEKAŃSKI
JACEK SIŃSKI
dr hab. EWA SKRZYDŁO-TEFELSKA
DARIUSZ SKUZA
MIKOŁAJ SOWIŃSKI
SŁAWOMIR STAWCZYK
AGATA SZELIGA
SŁAWOMIR USS
RADOSŁAW WASZKIEWICZ
RAFAŁ WASZKIEWICZ
ZBYSZKO WIZNER

Do: Renata Zalewska, Microsoft Sp. z o.o.

Od: Agata Szeliga, Sołtysiński Kawecki & Szlęzak
dr Wojciech Iwański, Sołtysiński Kawecki & Szlęzak

Data: 11 maja 2017 r.

ANALIZA
dotycząca podstawowych uwarunkowań prawnych korzystania z wybranych usług online Microsoft przez podmioty sektora ubezpieczeniowego

Usługi online Microsoft umożliwiają Klientom powierzanie Microsoft przetwarzania danych zgodnie z polskim prawem, w szczególności z ustawą o działalności ubezpieczeniowej i reasekuracyjnej. Odpowiedzialność za sposób używania usług Microsoft oraz rodzaje powierzanych danych (w tym objętych tajemnicą ubezpieczeniową) ponosi Klient, który pozostaje administratorem danych i jedynym podmiotem, który decyduje, jakie dane i w jakim celu są powierzane do przetwarzania.

Niniejsze memorandum jest podzielone na dwie części: część ogólną (pkt 1) i szczegółową dotyczącą zgodności wybranych usług online z wymogami Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji (pkt 2) oraz możliwości zapewnienia przez zakład ubezpieczeń zgodności z przepisami o działalności ubezpieczeniowej i reasekuracyjnej z (pkt 3).

SOŁTYSIŃSKI KAWECKI SZLĘZAK

Spis treści

1. Informacje podstawowe

(1) Jakie postanowienia umowne mają zastosowanie do usług online Microsoft?

Usługi online Microsoft Azure (np. Usługa Synchronizacji Active Directory pomiędzy Office 365 i On Premise, Azure Site Recovery czy wykorzystanie Azure do przeliczania danych z AMI) oraz Microsoft Office 365 (Exchange Online lub SharePoint Online), dalej zwane „**usługami online**", są dostępne dla **(a)** klientów należących do programu licencjonowania grupowego, jak również **(b)** klientów będących stronami umowy subskrypcyjnej dotyczącej usług online Microsoft.

Usługi online Microsoft będą świadczone zgodnie z zasadami określonymi w następujących dokumentach:

a) Program licencjonowania grupowego	b) Umowa subskrypcyjna
• Umowa Business and Services Agreement (dalej **MBSA**) (włącznie z postanowieniami szczególnymi dla Polski) oraz umowa i rejestracja dla konkretnego programu licencjonowania grupowego (na przykład Enterprise Agreement lub Select Plus) lub Umowa Products and Services Agreement (dalej **MPSA**); oraz • Postanowienia dotyczące Usług Online (dostępne pod adresem http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46), dalej **OST**[1]; oraz • Umowa Dotycząca Poziomu Usług Online Świadczonych Przez Microsoft (dostępna pod adresem http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37), dalej **SLA**[2].	• Umowa subskrypcyjna dotycząca usług online firmy Microsoft (dostępna pod adresem https://azure.microsoft.com/pl-pl/support/legal/subscription-agreement/), dalej **Umowa Subskrypcyjna**; oraz • Postanowienia dotyczące Usług Online (dostępne pod adresemhttp://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46), dalej **OST**; oraz • Umowa Dotycząca Poziomu Usług Online Świadczonych Przez Microsoft (dostępna pod adresem http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37), dalej **SLA**[2].

Cechą usług *cloud computing* jest masowe oferowanie klientom określonych, ustandaryzowanych rozwiązań. W związku z powyższym, dostawcy takich usług, w tym Microsoft, przygotowują standardowe wzory umów oferowanych klientom, którzy są zainteresowani tego rodzaju usługami. Masowe oferowanie jednolitych rozwiązań pozwala na ograniczenie wynagrodzenia za świadczenie takich usług w porównaniu z klasyczną

[1] Wersja z dnia 1 maja 2017 r., OST są okresowo aktualizowane.
[2] Wersja z dnia 1 kwietnia 2017 r., SLA są okresowo aktualizowane.

umową outsourcingową, w której usługodawca świadczy usługę dostosowaną („skrojoną") pod konkretnego klienta. Świadczenie usług na podstawie standardowych wzorców umów nie jest stosowane wyłącznie przez dostawców usług informatycznych w modelu cloud computing, ale wszystkich dostawców usług opartych na infrastrukturze – usług dostawy energii elektrycznej, gazu, wody czy usług telekomunikacyjnych.

Jednakże ze względu na specyfikę świadczenia usług na rzecz podmiotów regulowanych, z podmiotami z sektora usług finansowych Microsoft zawiera dodatkowy Aneks do Programu Usług Finansowych (**Aneks Finansowy**) wprowadzający szczególne postanowienia mające na celu zapewnienie zgodności z wymogami regulacyjnymi.

Klient może zaakceptować treść ww. umów poprzez podpisanie formularza podpisów dotyczących programu, zawierającego listę umów zawieranych przez klienta i Microsoft. Spełnione więc są wymogi pisemnego oświadczenia woli. Ramy umowne korzystania z usług tworzą umowy i załączniki do nich wskazane w podpisanym formularzu oraz dokumenty dostępne online, przywołane w umowach, w szczególności wskazane powyżej OST i SLA.[3] Umowy są rządzone prawem irlandzkim.

Wskazane dokumenty mają charakter uniwersalny i ramowy – dotyczą różnych usług oferowanych przez Microsoft. Od decyzji Klienta zależy, które usługi online zostaną wdrożone.

(2) *Jaki podmiot świadczy usługi online?*

Podmiotem świadczącym na rzecz Klienta usługi online jest Microsoft Ireland Operations Limited, spółka prawa irlandzkiego (MIOL lub Microsoft). MIOL jest podmiotem zależnym Microsoft Corp., podmiotu notowanego na giełdzie NASDAQ.

(3) *Jakie dane osobowe mogą być przekazywane do Microsoft przez Klienta w ramach usług online?*

W ramach usług online, Klient przekazuje Microsoft dane zawierające tekst, dźwięki, filmy, obrazy oraz oprogramowanie (Dane Klienta). Dane Klienta mogą obejmować dane osobowe, tj. dane umożliwiające identyfikację konkretnej osoby, takie jak imię, nazwisko, adres, numer PESEL czy zdjęcie, w tym dane objęte tajemnicą ubezpieczeniową. Na przykład w ramach usług online Klient może przetwarzać dane swoich pracowników, kontrahentów, klientów (ubezpieczających, ubezpieczonych, uposażonych) oraz dane kontaktowe innych osób związanych z prowadzoną działalnością gospodarczą.

[3] Niezależnie od sposobu wykorzystania oprogramowania (lokalnego czy w ramach usług online), dla każdej z tych opcji zostały przygotowane odrębne regulacje dotyczące korzystania z takich usług lub oprogramowania („Prawo do używania produktów", dostępne na stronie www.microsoft.com/licensing/contracts), które nie są jednak istotne z punktu widzenia niniejszej analizy.

(4) Jakie przepisy prawa mają zastosowanie do korzystania przez zakłady ubezpieczeń z usług online?

- Ze względu na charakter usług online, kluczowym jest stwierdzenie możliwości zapewnienia przez zakład ubezpieczeń zgodności korzystania z nich z Wytycznymi dotyczącymi zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji z dnia 16 grudnia 2014 r. (**Wytyczne**), w szczególności dot. współpracy z zewnętrznymi dostawcami usług (Wytyczna 10).
- Dany zakład ubezpieczeń powinien przeanalizować, czy przeznaczenie i sposób korzystania przez niego z usług online jest zgodny z przepisami ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (**UDU**), w szczególności, w zakresie outsourcingu oraz ochrony tajemnicy ubezpieczeniowej.
- Przetwarzanie danych osobowych w ramach usług online podlega szczególnej ochronie prawnej w państwach Europejskiego Obszaru Gospodarczego – EOG (tj. państwach UE oraz Norwegii, Islandii i Liechtensteinu). Minimalny standard ochrony danych osobowych w państwach Unii Europejskiej określa obecnie dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, która została wdrożona w Polsce przez ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

(5) Microsoft jako podmiot przetwarzający dane w imieniu Klienta

Zakład ubezpieczeń, jako administrator, jest uprawniony do powierzenia przetwarzania danych osobowych na podstawie umowy innemu podmiotowi, który przetwarza dane w imieniu administratora w celu i w zakresie wyznaczonym w umowie. Zgodnie z MBSA, MPSA i OST, Klient powierza Microsoft przetwarzanie danych osobowych w imieniu Klienta. Zatem jeżeli np. Klient będzie korzystał z aplikacji do zarządzania zasobami ludzkimi na platformie Microsoft Azure, Microsoft będzie przetwarzał dane pracowników Klienta w imieniu Klienta. Klient pozostanie natomiast administratorem danych.

(6) Gdzie świadczone są usługi online

a) Wszystkie usługi są świadczone online w oparciu o publiczną chmurę obliczeniową. Biorąc pod uwagę lokalizacje centrów danych Microsoft, Microsoft podzielił świat na określone obszary geograficzne. Dla obszaru geograficznego obejmującego Europę centra danych położone są w Irlandii oraz w Holandii, a w odniesieniu do usługi Exchange Online również w Austrii i Finlandii.

b) Zgodnie z OST, w przypadku usług Office 365, jeżeli klient zaopatruje swojego dzierżawcę (*tenant*) w UE, tj. Klient skonfiguruje określoną usługę w celu jej wdrożenia w określonym obszarze (np. UE), dla tej usługi Microsoft zobowiązuje się przechowywać w tym obszarze następujące dane klienta w spoczynku (*at rest*, tj. nie podlegające transferowi): (1) zawartość skrzynki pocztowej Exchange Online (treść

wiadomości e-mail, wpisy w kalendarzu i zawartość załączników wiadomości e-mail) oraz (2) zawartość witryny SharePoint Online i przechowywane w niej pliki (czyli pliki z pakietu Microsoft Office Online). W związku z powyższym Klient będzie więc każdorazowo wiedział, na jakim obszarze przetwarzane będą jego dane i będzie mógł zdecydować o nieskorzystaniu z danej usługi, jeżeli zakład ubezpieczeń nie zgadza się na przetwarzanie danych poza wybranym obszarem.

c) W przypadku usług Azure, jeżeli Klient skonfiguruje określoną usługę w celu jej wdrożenia w określonym regionie geograficznym, dla tej usługi Microsoft zobowiązuje się przechowywać dane magazynowane Klienta we wskazanym regionie geograficznym. Pewne usługi mogą nie umożliwiać Klientowi konfigurowania ich pod kątem ich wdrożenia w określonym regionie geograficznym lub poza Stanami Zjednoczonymi i mogą przechowywać kopie zapasowe danych w innych miejscach, zgodnie z opisem dostępnym w Centrum zaufania Microsoft Azure (który Microsoft ma prawo okresowo aktualizować, choć Microsoft zobowiązuje się nie dodawać wyjątków dla istniejących usług w wersji ogólnej).

d) Podstawą przekazywania Danych Klienta poza terytorium państw EOG w ramach usług online jest umowa powierzenia przetwarzania danych pomiędzy Klientem a Microsoft, która jest zgodna ze standardowymi klauzulami umownymi (Załącznik nr 3 do OST – „Standardowe Klauzule Umowne (Podmioty Przetwarzające Dane)". Standardowe klauzule umowne, stanowiące załącznik do Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement (obecnie włączone do OST) zostały zaakceptowane przez Grupę Roboczą Artykułu 29 (organ złożony z przedstawicieli urzędów ds. ochrony danych osobowych w UE) jako zgodne z prawem ochrony danych osobowych UE (http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf).

e) Ponadto transfer danych osobowych do Stanów Zjednoczonych jest dopuszczalny w przypadku przyjęcia przez importera danych zasad ochrony danych w drodze samocertyfikacji w Departamencie Handlu USA i zobowiązania się do ich przestrzegania. Podstawą transferu w takim wypadku są przepisy decyzji wykonawczej Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA. W dniu 12 sierpnia 2016 r. Spółka Microsoft Corporation oraz jej wskazane spółki stowarzyszone uzyskały certyfikat Departamentu Handlu USA obejmujący swoim zakresem dane osobowe przekazywane w ramach usług online i zobowiązały się do przestrzegania zasad ochrony danych osobowych (https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK).

2. Pytania szczegółowe dotyczące usług online w świetle Wytycznych

(7) *Czy zakład ubezpieczeń ma możliwość szczegółowej oceny sytuacji ekonomiczno-finansowej Microsoft, zapewnianego przez niego poziomu bezpieczeństwa oraz jakości świadczonych usług (w miarę możliwości również na podstawie doświadczeń innych podmiotów)?*

Tak. Następujące okoliczności związane z usługami Microsoft mogą zostać wzięte pod uwagę przez zakład ubezpieczeń przy dokonywaniu takiej oceny:

- Microsoft jest liderem branży nowych technologii – dostawcą urządzeń i usług dla konsumentów oraz klientów instytucjonalnych i komercyjnych;
- aktualne dane finansowe grupy Microsoft dostępne są pod adresem http://www.microsoft.com/investor/default.aspx, a jednostkowe dane MIOL – za pośrednictwem irlandzkiego rejestru handlowego (https://search.cro.ie/company/CompanySearch.aspx);
- Microsoft jest usługodawcą o niekwestionowanej renomie. Wśród sztandarowych produktów oferowanych przez Microsoft jest system operacyjny Windows, dostępny również w wersjach na platformę mobilną – Windows Phone oraz platformę serwerową – Windows Server. Firma jest także liderem w zakresie rozwiązań dostarczanych w formie usług w modelu *cloud computing* i posiada kompleksową ofertę infrastruktury, platformy programistycznej oraz aplikacji w chmurze obliczeniowej. Kluczowe rozwiązania z tego obszaru to platforma Microsoft Azure oraz Office 365. Dbając o zapewnienie klientom bezpieczeństwa i poufności w tym środowisku, firma jako pierwszy duży dostawca wdrożyła międzynarodową normę poufności danych w chmurze ISO 27018. Przy tworzeniu usług online, Microsoft przestrzega zasad Security Development Lifecycle, które wymagają uwzględniania kwestii związanych z bezpieczeństwem i ochroną danych zarówno przy tworzeniu oprogramowania (*privacy by design*), jak i podczas funkcjonowania usługi (potwierdzają to posiadane certyfikacje ISO 27001 – por. dalej);
- Microsoft Corp. powstał w 1975 roku w USA i jest jedną z najbardziej wartościowych spółek publicznych z sektora IT notowanych na NASDAQ (MSFT), a polski oddział firmy istnieje od 1992 r. W swoich filiach na całym świecie Microsoft zatrudnia blisko 100 tys. specjalistów z różnych dziedzin, w tym ponad 500 osób w Polsce. Microsoft jest zaangażowany społecznie, dążąc do poszerzania kompetencji cyfrowych poprzez inwestycje w rozwój edukacji informatycznej, wsparcie początkujących przedsiębiorstw i organizacji pozarządowych. W 2014 firma przekazała na realizację tego celu w Polsce 478 milionów zł, docierając do 2000 nauczycieli, 38.000 uczniów i 79.000 studentów. Udzielone wsparcie technologiczne dla 2000 start-upów bezpośrednio przełożyło się na utworzenie 4000 miejsc pracy. Z kolei od 2001 r. ze wsparcia o łącznej wartości blisko 153 mln złotych skorzystało 6 tysięcy polskich organizacji trzeciego sektora;
- odpowiednie standardy zapewniające najwyższy poziom bezpieczeństwa danych zostały wskazane w OST (*Informacje dotyczące Bezpieczeństwa dla Usług Online*). Zgodnie z

postanowieniami OST Microsoft udostępnia klientowi Zasady Bezpieczeństwa Informacji oraz inne informacje dot. bezpieczeństwa (por. poniżej);

- najwyższą jakość świadczonych usług potwierdzają postanowienia SLA;
- Microsoft świadczy usługi na rzecz szeregu podmiotów z sektora finansowego, w tym bankowego i ubezpieczeniowego na świecie i w Polsce. Od wielu lat angażuje się aktywnie w dyskusje pomiędzy takimi podmiotami regulowanymi oraz organami nadzoru (w tym Komisją Nadzoru Finansowego; „**KNF**") dotyczące potwierdzania zgodności korzystania z usług Microsoft z regulacjami sektorowymi i oczekiwaniami regulatorów. W rezultacie zakład ubezpieczeń dokonując oceny ryzyka związanego ze skorzystaniem z usług online może liczyć na informacje i doświadczenia od innych uczestników rynku, a nawet samego organu nadzoru.

(8) *Jakie jest ryzyko związane z upadłością Microsoft usługodawcy zewnętrznego lub jego nagłym wycofaniem się ze współpracy z zakładem ubezpieczeń? Czy zakład ubezpieczeń będzie mógł stworzyć skuteczne plany awaryjne związane z wystąpieniem takich sytuacji?*

Ze względu na aktualną sytuację finansową grupy Microsoft, jak też powszechność dostępu do usług online, ryzyko upadłości usługodawcy lub jego nagłego wycofania się ze współpracy oceniane powinno być jako bardzo niskie. Zakład ubezpieczeń ma możliwość bieżącej weryfikacji sytuacji finansowej Microsoft w sposób opisany szczegółowo powyżej.

Na wypadek nagłego zaprzestania świadczenia usług lub na etapie powzięcia wiadomości o trudnościach w ich świadczeniu, dane zakładu ubezpieczeń przechowywane w chmurze zostaną niezwłocznie, ale nie później niż w terminie do 180 dni od dnia wygaśnięcia umowy lub zakończenia korzystania przez zakład ubezpieczeń z usług online przeniesione na nośniki zakładu ubezpieczeń wykorzystując zdalną transmisję lub zostaną przekopiowane z zaszyfrowanych nośników dostarczonych przez Microsoft do wskazanego centrum obliczeniowego zakładu ubezpieczeń. Techniczne aspekty zostają szczegółowo opisane na etapie wdrożenia rozwiązania.

(9) *Czy zakład ubezpieczeń może monitorować jakość usług online? Czy zakres, częstotliwość i metody monitorowania uwzględniają specyfikę świadczonych usług oraz ich istotność z perspektywy ciągłości i bezpieczeństwa działania zakładu ubezpieczeń?*

Zakład ubezpieczeń będzie posiadał szereg uprawnień do badania jakości świadczonych usług.

a) Jakość usług jest okresowo weryfikowana przez odpowiednich specjalistów:

- Microsoft realizuje coroczne audyty usług online, obejmujące audyty zabezpieczeń komputerów, środowiska informatycznego i fizycznych Centrów Danych, których szczegóły można znaleźć pod adresem http://www.microsoft.com/online/legal/v2/?docid=27. Na prośbę Klienta udostępniane są raporty z tych audytów.

- Centra danych oraz usługi są dodatkowo certyfikowane rocznie przez BSI (*British Standards Institute*) dla raportów ISO 27001:2013 i przez Deloitte dla SOC 1, SOC 2 i SOC 3. Oba audyty weryfikują dostęp do Centrów danych, obsługę wykonywaną przez dostawców i bezpieczeństwo ogólne. Szczegóły certyfikacji ISO znajdują się po linkiem GFS ISO/IEC 27001:2005 certificate. [4]

b) Jakość usług może być przez Klienta kontrolowana za pomocą Konsoli Office 365.

W panelu administracyjnym Office 365 jest pełna transparentność odnośnie działania usług w Office 365 Klienta. Przekazywane są na bieżąco informacje o stanie usługi oraz zaplanowanych pracach. Taki raport wyświetla informacje z ostatnich 30 dni działania (można go znaleźć pod adresem: https://portal.office.com/admin/default.aspx#ServiceStatusPage). Dodatkowo jest możliwość zasubskrybowania do powiadomień RSS odnośnie stanu usług.

W panelu administracyjnym Office 365 dostępnych jest szereg raportów dla administratorów zapewniający wgląd w użytkowanie usługi Office 365 w organizacji, np. z użycia: Aktywni użytkownicy, raporty inspekcji, wykrycie spamu i złośliwego oprogramowania.

Na liście raportów, widnieją także raporty, które są dedykowane do konkretnych usług, np. Exchange Online.

c) Jakość usług Azure może być przez Klienta kontrolowana za pomocą Konsoli Azure.

Integralną część platformy Azure stanowią usługi pomocy technicznej platformy Azure. Klient, w ramach zawartych umów z Microsoft, posiada plan pomocy technicznej dla platformy Azure.

Informacje o stanie systemu Azure, w tym stwierdzonych błędach, dostępne są także na stronie internetowej Microsoft (https://azure.microsoft.com/pl-pl/status/#history);

d) Dodatkowe narzędzia monitorowania zostały przewidziane w Aneksie Finansowym – por. powyżej.

(10) W przypadku, gdy zakład ubezpieczeń będzie wykorzystywał usługi online w sposób powodujący przetwarzanie danych o wysokim stopniu poufności lub istotności dla zakładu poza infrastrukturą teleinformatyczną zakładu:

– *Czy wprowadzone zostaną adekwatne mechanizmy kontrolne zapewniające poufność tych danych (np. poprzez ich szyfrowanie)?*

Microsoft wdrożył i zobowiązuje się utrzymywać i stosować odpowiednie zabezpieczenia o charakterze technicznym i organizacyjnym w celu ochrony Danych Klienta przed przypadkowymi, nieautoryzowanymi lub niezgodnymi z prawem przypadkami uzyskiwania

[4] http://www.bsigroup.com/en-US/Our-services/Certification/Certificate-and-Client-Directory-Search/Certificate-Client-Directory-Search-Results/?searchkey=standard%3dISO%252fIEC%2b27001%253a2005%26company%3dMicrosoft&licencenumber=IS%20533913

dostępu do nich, ich ujawniania, modyfikacji, utraty lub zniszczenia (s. 8 OST, „Bezpieczeństwo").

W celu zapewnienia bezpieczeństwa danych w chmurze Microsoft stosuje środki techniczne i organizacyjne opisane na s. 12-14 OST, a w szczególności:

(a) Monitorowane całodobowo zabezpieczenia fizyczne. Centra danych są fizycznie skonstruowane, zarządzane i monitorowane tak, aby chroniły dane i usługi przed nieautoryzowanym dostępem oraz zagrożeniami środowiskowymi.

(b) Monitorowanie i rejestrowanie. Zabezpieczenia są monitorowane przez scentralizowane systemy monitorowania, określania korelacji i analiz, które zarządzają dużymi ilościami informacji generowanych przez urządzenie znajdujące się w środowisku i gwarantują terminowe generowanie alertów. Ponadto dostępnych jest wiele poziomów monitorowania, rejestrowania i raportowania, dzięki którym klienci mają wgląd w bieżącą sytuację.

(c) Brak uprawnień ponadstandardowych. Personel Microsoft zajmujący się operacjami i świadczący pomoc techniczną domyślnie nie ma dostępu do danych klienta. W przypadku udzielenia takiego dostępu jest on starannie kontrolowany i rejestrowany. Centra danych uzyskują dostęp do systemów, które przechowują dane Klienta, w sposób ściśle kontrolowany za pośrednictwem procesów blokady.

(d) Izolacja. Usługi online używają izolacji sieci, aby zapobiegać niechcianej komunikacji między działami, a funkcje kontroli dostępu blokują użytkowników nieautoryzowanych. Maszyny wirtualne nie odbierają ruchu przychodzącego z Internetu, o ile klienci odpowiednio ich nie skonfigurują.

(e) Ochrona przed złośliwym oprogramowaniem. Microsoft przeprowadza kontrole chroniące przed złośliwym oprogramowaniem, które pomagają w uniemożliwieniu uzyskania nieupoważnionego dostępu do Danych Klienta przez takie oprogramowanie, w tym złośliwe oprogramowanie pochodzące z sieci publicznych.

(f) Wykrywanie włamań i ataków DDoS. Systemy wykrywania włamań i zapobiegania im oraz zapobiegania atakom typu odmowa usługi, regularne testy penetracyjne i narzędzia informatyki śledczej pomagają identyfikować i minimalizować zagrożenia.

(g) Komunikacja szyfrowana. Wbudowana od samego początku możliwość szyfrowania przez Klientów ich danych – oparta na Infrastrukturze Klucza Publicznego (Public Key Infrastructure, PKI), w ramach której Klient ma kontrolę nad kluczami kryptograficznymi. Microsoft oferuje również możliwość szyfrowania rozwiązaniem BitLocker.

(h) Tożsamość i dostęp. Usługa Active Directory systemu Azure umożliwia klientom zarządzanie dostępem do systemu Azure.

(i) Poprawki. Zintegrowane systemy wdrażania zarządzają dystrybucją i instalacją poprawek zabezpieczeń. Klienci mogą stosować podobne procesy zarządzania poprawkami dla maszyn wirtualnych wdrożonych w systemie Azure.

Ponadto Microsoft oferuje dodatkowe funkcjonalności usług online takie jak:

(a) Centrum zabezpieczeń Azure. Umożliwia zapobieganie zagrożeniom, wykrywanie ich i odpowiadanie na nie dzięki lepszemu wglądowi w zabezpieczenia zasobów platformy Azure i większej kontroli nad nimi. Szerzej zobacz https://azure.microsoft.com/pl-pl/services/security-center.

(b) Magazyn kluczy. Usługa Magazyn kluczy Azure umożliwia szyfrowanie kluczy i małych kluczy tajnych, takich jak hasła, za pomocą kluczy przechowywanych w sprzętowych modułach zabezpieczeń. W celu zapewnienia dodatkowej ochrony można importować lub generować klucze w sprzętowych modułach zabezpieczeń. W takiej sytuacji firma Microsoft będzie przetwarzać klucze w sprzętowych modułach zabezpieczeń zgodnych ze standardem FIPS 140-2 na poziomie 2 (sprzęt i oprogramowanie układowe). Usługa Magazyn kluczy jest zaprojektowana tak, że firma Microsoft nie zna kluczy Klienta ani nie może ich wyodrębnić. Użycie kluczy można monitorować i sprawdzać za pomocą funkcji rejestrowania platformy Azure. Szerzej zobacz https://azure.microsoft.com/pl-pl/services/key-vault.

(c) Microsoft Operations Management Suite (OMS). W ramach pakietu OMS dostępna jest funkcja analizy dzienników (log analysis), która pozwala zbierać, przechowywać i analizować dane dzienników chmury Azure oraz przekształcać je w czasie rzeczywistym w operacyjne dane analityczne ułatwiające podejmowanie bardziej świadomych decyzji biznesowych. Szerszej zobacz https://azure.microsoft.com/pl-pl/services/log-analytics.

(d) Usługa Multi-Factor Authentication. Usługa Azure Multi-Factor Authentication zabezpiecza dostęp do danych i aplikacji, a jednocześnie spełnia wymagania użytkowników dotyczące prostoty procesu logowania. Zapewnia ona silne uwierzytelnianie z szerokim zakresem prostych opcji weryfikacji obejmujących połączenia telefoniczne, wiadomości SMS i powiadomienia przez aplikacje mobilne, pozwalając użytkownikom na wybór odpowiadającej im metody. Szerzej zobacz https://azure.microsoft.com/pl-pl/services/multi-factor-authentication.

(e) Sieci wirtualne platformy Azure. Klienci mogą wybrać opcję przypisania wielu wdrożeń do izolowanej sieci wirtualnej i zezwolić tym wdrożeniom na wzajemne komunikowanie się za pomocą prywatnych adresów IP. Szerzej zobacz https://azure.microsoft.com/pl-pl/services/virtual-network.

(f) Połączenie prywatne. Klienci mogą używać usługi ExpressRoute do nawiązywania prywatnego połączenia z centrami danych systemu Azure, utrzymując swój ruch sieciowy poza Internetem. Szerzej zobacz https://azure.microsoft.com/pl-pl/services/expressroute.

Rozwiązanie BitLocker używa do szyfrowania pary kluczy. Samo szyfrowanie danych odbywa się kluczem symetrycznym (domyślnie 128-bit AES w trybie XTS dla aktualnej wersji Windows 10), natomiast sam klucz będzie już szyfrowany kolejnym kluczem, który

jest kluczem asynchronicznym. W przypadku szyfrowania asynchronicznego, bez posiadania obu kluczy nie jest możliwe odszyfrowanie danych.

Druga para klucza jest przechowywana w Active Directory Klienta i nie będzie opuszczała Klienta. W konsekwencji, mimo iż Microsoft jest dostawcą technologii Bitlocker, nie może on odszyfrować zaszyfrowanego wolumenu dyskowego, gdyż bycie autorem rozwiązania nie oznacza posiadania kluczy niezbędnych do odszyfrowania dysku.

Technologia Bitlocker jest powszechnie stosowana i uznawana za bezpieczną, a posiadane certyfikaty oraz audyty, jak też renoma usługodawcy minimalizują ryzyko związane z bezpieczeństwem informacji.

– *Czy zapewnione zostanie, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez Microsoft?*

Tak. Jeśli Microsoft dowie się o jakimkolwiek przypadku niezgodnego z prawem dostępu do Danych Klienta przechowywanych na sprzęcie Microsoft lub w placówce Microsoft lub nieautoryzowanego dostępu do sprzętu Microsoft lub placówki Microsoft, który skutkowałby utratą, ujawnieniem lub modyfikacją Danych Klienta (każde z osobna zwane „Naruszeniem Zabezpieczeń"), wówczas Microsoft bezzwłocznie (1) powiadomi Klienta o Naruszeniu Zabezpieczeń; (2) zbada dany przypadek Naruszenia Zabezpieczeń i przekaże Klientowi szczegółowe informacje na jego temat oraz (3) podejmie odpowiednie kroki w celu ograniczenia jego skutków i do zminimalizowania ewentualnych szkód wynikających z takiego Naruszenia Zabezpieczeń.

W przypadku każdego naruszenia bezpieczeństwa klasyfikowanego jako Naruszenie Zabezpieczeń Microsoft (poniżej) bezzwłocznie i w każdym przypadku nie później niż w ciągu 30 dni kalendarzowych wyśle stosowne powiadomienie. Powiadomienia o Naruszeniach Zabezpieczeń będą przekazywane do administratorów po stronie Klienta w sposób wybrany przez Microsoft, w tym pocztą elektroniczną. Klient ponosi wyłączną odpowiedzialność za zapewnienie, żeby administratorzy po jego stronie zamieszczali w poszczególnych odnośnych portalach usług online aktualne i dokładne informacje kontaktowe. Zobowiązanie Microsoft do zgłaszania Naruszeń Zabezpieczeń lub odpowiadania na nie na mocy niniejszego punktu nie stanowi potwierdzenia przez Microsoft przyjęcia jakiejkolwiek winy lub odpowiedzialności w związku z Naruszeniem Zabezpieczeń.

Klient musi bezzwłocznie informować Microsoft o wszelkich potencjalnych przypadkach niewłaściwego korzystania z kont lub poświadczeń uwierzytelniających oraz o wszelkich naruszeniach zabezpieczeń związanych z którąkolwiek z usług online.

Microsoft prowadzi rejestr naruszeń zabezpieczeń, w którym znajduje się opis naruszenia, czas i konsekwencje naruszenia, imię i nazwisko osoby zgłaszającej, imię i nazwisko osoby przyjmującej zgłoszenie oraz procedura odzyskiwania danych. (s. 8 i 14 OST).

– *Czy zakład ubezpieczeń będzie posiadać informacje o tym, w jakich lokalizacjach geograficznych dane te są przetwarzane oraz jakie przepisy prawa obowiązują tam w przedmiotowym zakresie, oraz zapewniona zostanie zgodność świadczonych usług w zakresie przetwarzania danych, z przepisami prawa obowiązującymi w Polsce?*

Jeżeli Klient skonfiguruje usługi online lub przydzieli zasoby swoim dzierżawcom w taki sposób, że jego dane magazynowane będą znajdowały się w EOG, dane te nie będą przekazywane poza EOG.

Należy jednak podkreślić, że z uwagi na specyfikę usług online (tj. wymóg ciągłego zapewniania usług wsparcia 24x7x365), nie jest możliwe ograniczenie podwykonawców jedynie do spółek z UE/EOG. Świadczenie usług wsparcia przez podwykonawców w praktyce nie wiąże się jednak z ich dostępem do zawartości danych Klienta. Jedynie w wyjątkowych sytuacjach, związanych z bardziej skomplikowanym wsparciem klienta (np. koniecznością bezpośredniej ingerencji w maila lub w załącznik do maila) może zachodzić konieczność przyznania podwykonawcy dostępu do zawartości danych Klienta. Microsoft zobowiązuje się w OST do korzystania z danych Klienta wyłącznie w celu świadczenia Klientowi usług online, w tym w celach powiązanych ze świadczeniem tych usług (s. 7 OST). W rezultacie, uzyskiwanie dostępu do tych danych w innych celach będzie stanowiło naruszenie umowy na świadczenie usług online.

Podwykonawcy spoza EOG otrzymują ewentualny dostęp do zawartości Danych Klienta na podstawie umowy powierzenia przetwarzania danych, zgodnej ze standardowymi klauzulami umownymi (Załącznik nr 3 do OST), którą Klient zawiera z Microsoft Corporation z siedzibą w Stanach Zjednoczonych. W przypadku transferu danych do Stanów Zjednoczonych dodatkową podstawą jest certyfikacja Departamentu Handlu USA zgodnie z decyzją wykonawczą Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA. W dniu 12 sierpnia 2016 r. spółka Microsoft Corporation oraz jej niektóre podmioty stowarzyszone uzyskały certyfikat Departamentu Handlu USA i zobowiązały się do przestrzegania zasad ochrony danych osobowych (https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK).

Dostęp do danych podmiotów spoza EOG w usługach Office 365

Informacje o tym kto może mieć dostęp do Danych Klienta i ich zawartości w ramach usług Office 365 dostępne są pod następującym adresem: https://www.microsoft.com/online/legal/v2/?docid=24&langid=pl-PL W usłudze Office 365, Microsoft zapewnia Klientom dodatkowe instrumenty zapewniające im kontrolę nad tym, kto uzyskuje dostęp do zawartości ich danych. W szczególności, Klient może uzyskać raporty dotyczące dostępu do danych Klienta przez Microsoft lub jego podwykonawców. W niektórych planach usług Office 365 Klient może również skorzystać z funkcjonalności Customer Lockobox Office 365, która przyznaje Klientowi uprawnienie do decydowania o tym, czy i kiedy może być przyznany dostęp do zawartości jego określonych danych w związku z usługami wsparcia (https://blogs.office.com/2015/04/21/announcing-customer-lockbox-for-office-365/ oraz https://support.office.com/en-us/article/Office-365-Customer-Lockbox-Requests-36f9cdd1-e64c-421b-a7e4-4a54d16440a2). Oznacza to, że Klient może

ogólnie zablokować dostęp do danych Klienta w związku z usługami wsparcia i zezwalać na taki dostęp jedynie w konkretnych sytuacjach. W takim przypadku, każdorazowo decyzja o udzieleniu zgody na dostęp wymaga zatwierdzenia przez administratora Klienta.

Dostęp do danych spoza EOG w usługach Azure

Informacje o tym kto może mieć dostęp do Danych Klienta i ich zawartości w ramach usług Azure są dostępne pod adresem https://www.microsoft.com/en-us/TrustCenter/Privacy/You-are-in-control-of-your-data#_You_control_access oraz WindowsAzurePrivacyOverview). Zgodnie z tymi postanowieniami, dostęp do danych Klienta (w tym ich zawartości) może mieć miejsce tylko jeśli jest to konieczne dla świadczenia usług wsparcia i pod nadzorem osób zarządzających. Taki dostęp jest kontrolowany oraz rejestrowany (za pomocą logów). Jeżeli prawo dostępu do danych nie jest już niezbędne, jest ono niezwłocznie cofane. Należy również podkreślić, że w przypadku usług Azure, lista podwykonawców świadczących usługi wsparcia, oprócz podmiotów z grupy Microsoft, jest bardzo ograniczona. Istotnie ogranicza to ryzyka związane z dostępem spoza EOG.

Dostęp do danych ze strony podmiotów trzecich

Microsoft nie ujawni Danych Klienta organom władzy publicznej, chyba że będzie to wymagane na mocy przepisów prawa. Jeśli organ władzy publicznej zażąda od Microsoft Danych Klienta, Microsoft podejmie próbę skierowania go z takim żądaniem bezpośrednio do Klienta. Jeśli Microsoft zostanie zmuszony do ujawnienia organowi władzy publicznej Danych Klienta, wówczas niezwłocznie powiadomi o tym Klienta i przekaże mu kopię takiego żądania, chyba że jest to zabronione przez przepisy prawa (s. 7 OST, akapit „Ujawnianie Danych Klienta").

Z chwilą otrzymania od jakiejkolwiek innej osoby trzeciej żądania ujawnienia Danych Klienta Microsoft niezwłocznie powiadomi o tym Klienta, chyba że jest to zabronione przez przepisy prawa. O ile przepisy prawa nie wymagają od Microsoft spełnienia takiego żądania, Microsoft zobowiązuje się odrzucać takie żądania. Jeśli żądanie będzie miało podstawę prawną, Microsoft podejmie próbę skierowania osoby trzeciej wysuwającej takie żądanie ujawnienia danych bezpośrednio do Klienta.

Microsoft nie zapewni żadnej osobie trzeciej: (a) bezpośredniego, pośredniego, nieograniczonego ani swobodnego dostępu do Danych Klienta; (b) kluczy szyfrowania platformy używanych do zabezpieczenia Danych Klienta ani możliwości złamania takiego szyfrowania ani (c) dostępu do Danych Klienta, jeżeli Microsoft będzie mieć świadomość, że dane te mają być użyte w celach innych niż wskazane w żądaniu przekazanym przez daną osobę trzecią (s. 7 OST akapit „Ujawnianie Danych Klienta").

W ramach świadczenia usług online dane osobowe przetwarzane są przez Microsoft i podwykonawców na zasadzie powierzenia przetwarzania danych. Administratorem danych, który decydujące o celach i środkach przetwarzania danych osobowych, pozostaje Klient. Żądania poprawienia, zmiany lub usunięcia danych powinny być kierowane przez osoby, których dane dotyczą, do administratora danych. Żądania skierowane do Microsoft lub podwykonawców będą przekazywane do Klienta.

– *Czy zapewnione zostaną skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia – wraz ze wszystkimi kopiami – przez Microsoft)?*

Tak. Najpóźniej 180 dni po wygaśnięciu lub zakończeniu używania przez Klienta dowolnej usługi online Microsoft wyłączy konto Klienta i usunie z niego Dane Klienta (s. 11 OST, „Prywatność"). Także w wypadku nagłego zaprzestania świadczenia usług lub na etapie powzięcia wiadomości o trudnościach w ich świadczeniu, dane zakładu ubezpieczeń przechowywane w chmurze zostaną niezwłocznie, ale nie później niż w terminie do 180 dni od dnia wygaśnięcia umowy lub zakończenia korzystania przez zakład ubezpieczeń z usług online przeniesione na nośniki zakładu ubezpieczeń wykorzystując zdalną transmisję lub zostaną przekopiowane z zaszyfrowanych nośników dostarczonych przez Microsoft do wskazanego centrum obliczeniowego zakładu ubezpieczeń. Techniczne aspekty zostają szczegółowo opisane na etapie wdrożenia rozwiązania.

Klient może także samodzielne usunąć swoje dane.

– *Czy Microsoft posiada certyfikaty w zakresie zgodności z uznanymi międzynarodowymi normami dotyczącymi bezpieczeństwa informacji (szczególnie w przypadku przetwarzania danych poza granicami Europejskiego Obszaru Gospodarczego)?*

Jak potwierdzono w OST (s. 14, „Informacje dotyczące Zasad Bezpieczeństwa dla Usług Online"), każda usługa online jest zgodna z zasadami zabezpieczeń danych („Zasady Bezpieczeństwa Informacji"), które są zgodne ze standardami kontroli i normami wskazanymi w poniższej tabeli.

Usługa Online	ISO 27001	ISO 27002 Kodeks postępowania	ISO 27018 Kodeks postępowania	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Usługi Office 365	Tak	Tak	Tak	Tak	Tak
Podstawowe Usługi Microsoft Dynamics 365	Tak	Tak	Tak	Tak*	Tak*
Podstawowe Usługi Microsoft Azure	Tak	Tak	Tak	Występują różnice**	Występują różnice**
Usługi Online Microsoft Intune	Tak	Tak	Tak	Tak	Tak
Usługi Microsoft Power BI	Tak	Tak	Tak	Nie	Nie

** Nie obejmuje usługi Microsoft Social Engagement.*

***Obecny zakres określono w raporcie z audytu i umieszczono w Centrum Zaufania Systemu Microsoft Azure.*

(11) Czy zakład ubezpieczeń będzie mógł sprawować kontrolę nad działalnością Microsoft w zakresie świadczonych przez niego usług?

W celu zagwarantowania należytej realizacji uprawnień kontrolnych, w Aneksie Finansowym przewidziano szereg uprawnień kontrolnych zakładu ubezpieczeń oraz UKNF.

UKNF będzie miał możliwość odbycia inspekcji w centrum przetwarzania danych oraz żądania od MIOL udostępniania dokumentów i informacji związanych ze świadczeniem usług online, a MIOL zobowiązuje się do pełnej współpracy z Urzędem w wymaganym zakresie. W Aneksie Finansowym Microsoft zobowiązuje się do umożliwienia organowi nadzoru, m.in., bezpośredniego skontrolowania usług online, z uwzględnieniem kontroli pomieszczeń i dostępu do informacji, akt, raportów i dokumentów dotyczących usług online. Uprawnienie do przeprowadzenia inspekcji przez organ nadzoru zostało więc zakreślone maksymalnie szeroko. Zakres tych uprawnień zasadniczo koresponduje z przyjętą praktyką rynkową dla umów outsourcingowych.

Uprawnienie to umożliwi także kontrolę działania podwykonawców. Ze względu na charakter usług oraz kwestie bezpieczeństwa, zdecydowana większość usług jest wykonywana przez podwykonawców w Centrach Danych Microsoft – z zachowaniem szczególnych zasad bezpieczeństwa i poufności wynikających z normy ISO 27001 oraz po zawarciu odpowiednich umów z podwykonawcami i objęciu ich procedurami bezpieczeństwa Microsoft (por., przede wszystkim, ust. A.15.1.1, A.15.1.2 praz A.15.2.2 Kontroli ISO 27001/13). Zgodnie z normą ISO 27018 (por. Kontrolę ISO 27018, ust. A.10.12), na podstawie zawartych umów, podwykonawcy zobowiązują się przestrzegać takich samych jak Microsoft standardów bezpieczeństwa wynikających, m.in., z przepisów prawa, standardów i rekomendacji.

W zakresie zapewnienia UKNF prawa do kontroli wykonywania powierzonych czynności, kontrola usług będzie możliwa na takiej samej zasadzie jak w przypadku jakichkolwiek innych usług IT świadczonych na terytorium EOG.[5]

(12) *Czy zakład ubezpieczeń będzie miał możliwość weryfikacji stosowanych przez Microsoft mechanizmów kontrolnych, w tym w zakresie środków ochrony i kontroli dostępu do pomieszczeń usługodawcy, w których odbywa się świadczenie usług na rzecz towarzystwa?*

W przypadku usług online, klienci standardowo nie mają możliwości przeprowadzenia kontroli w centrum danych z uwagi na kwestie bezpieczeństwa oraz charakter przetwarzania w chmurze (tj. personel centrum nie ma standardowo dostępu do danych Klientów i nie mógłby ich w toku kontroli udostępnić Klientowi).

W celu zagwarantowania możliwość weryfikacji stosowanych przez Microsoft mechanizmów kontrolnych:

[5] Pomimo zapewnienia przez Microsoft uprawnienia do kontroli na miejscu, żaden z regulatorów nie zdecydował się na przeprowadzenie samodzielnej kontroli Centrów Danych. Regulatorzy uzyskują raczej szczegółową wiedzę o funkcjonowaniu usług online, korzystając z prawa do żądania od Microsoft informacji i dokumentów, bezpośrednio lub za pośrednictwem podmiotów regulowanych. Szereg tego typu żądań było już kierowanych do Microsoft przez europejskich regulatorów. Według wiedzy Microsoft, szereg podmiotów regulowanych prowadziło dyskusje i przedstawiało wyjaśnienia regulatorom. Np. jedna z europejskich grup bankowych była zaangażowana w szereg tego typu dyskusji z kilkoma wiodącymi regulatorami europejskimi. Według wiedzy Microsoft, europejscy regulatorzy byli usatysfakcjonowani otrzymanymi informacjami i dokumentami.

- zgodnie z Aneksem Finansowym, Microsoft udostępni klientowi Raport z Audytu Microsoft, tak aby Klient mógł odpowiednio zweryfikować przestrzeganie przez Microsoft zobowiązań w zakresie bezpieczeństwa;

- klient może skorzystać z dodatkowych uprawnień kontrolnych przewidzianych w Aneksie Finansowym – w zakresie dostosowanym do indywidualnych potrzeb danego Klienta, w szczególności przyjętych w danym zakładzie ubezpieczeń zasad zarządzania ryzykiem;
- zgodnie z OST (str. 14), Microsoft może dostarczyć na żądanie wynik działania audytu SSAE 16.

(13) *Czy zakład ubezpieczeń będzie miał możliwość przeglądu wyników weryfikacji mechanizmów kontrolnych realizowanych – np. z wykorzystaniem standardu SSAE 16 – przez audyt wewnętrzny Microsoft lub niezależnych audytorów zewnętrznych?*

Tak. Zgodnie z OST (str. 14), Microsoft może dostarczyć na żądanie wynik działania audytu SSAE 16.

(14) *Czy umowa z Microsoft będzie określała:*

– *zakresy odpowiedzialności stron umowy?*

Zakres odpowiedzialności stanowi przedmiot postanowień (i) umowy MBSA: Rękojmie i gwarancje, Obrona przed roszczeniami z tytułu naruszenia lub przywłaszczenia praw oraz przed innymi roszczeniami osób trzecich, Ograniczenie odpowiedzialności oraz Odpowiedzialność za działania podwykonawców, (ii) OST (Załącznik 3 – Standardowe Klauzule Umowne (podmioty przetwarzające dane), Klauzula 6: Odpowiedzialność) oraz (iii) Aneksu Finansowego, który zmienia Umowę, w zakresie w nim określonym oraz (iv) umowy SLA (s. 6 i nast.).

Umowa MBSA wprowadza ograniczenie odpowiedzialności Microsoft za szkodę do wartości wynagrodzenia zapłaconego Microsoft w ostatnich 12 miesiącach świadczenia usług online. Wprowadzenie progu kwotowego odpowiedzialności odpowiada standardom rynkowym świadczenia usług IT, zwłaszcza usług w chmurze.

Umowa Subskrypcyjna, wprowadza tę samą zasadę oraz dodatkowe ograniczenie, zgodnie z którym, w żadnym przypadku łączna odpowiedzialność Microsoft nie przekroczy kwoty zapłaconej za usługi online w okresie subskrypcji.

– *zakres informacji i dokumentacji przekazywanych przez usługodawcę w związku ze świadczeniem usług,*

Informacje i dokumenty przekazywane przez Klienta do Microsoft w związku ze świadczeniem usług wskazane są w umowach (zob. definicję „danych Klienta", s. 4 OST).

– *zasady wymiany i ochrony informacji, w tym warunki nadawania pracownikom podmiotów zewnętrznych praw dostępu do informacji oraz zasobów środowiska*

teleinformatycznego, uwzględniające w szczególności obowiązujące przepisy prawa oraz regulacje towarzystwa w tym zakresie; w przypadku usługodawców posiadających dostęp do informacji o wysokim stopniu poufności, uregulowana powinna zostać również kwestia odpowiedzialności za zachowanie tajemnicy tych informacji w okresie wykonywania usług oraz po zakończeniu umowy,

Kwestie zachowania poufności uregulowane zostały szczegółowo w pkt. 3 umowy MBSA.

Zasady obchodzenia się z danymi Klienta, w tym ich wykorzystywania i ujawniania oraz nadawania uprawnień dostępu pracownikom Microsoft zostały uregulowane na str. 7-15 OST. Zostały tam także uregulowane obowiązki związane z zachowaniem poufności po zakończeniu umowy.

W zakresie przetwarzania danych, w tym obowiązków pracowników Microsoft, zasady wymiany i ochrony informacji, spełniające odpowiednie europejskie standardy zostały również zawarte w Standardowych Klauzulach Umownych (podmioty przetwarzające dane), stanowiących Załącznik 3 do OST.

Przeprowadzane audyty i posiadane Certyfikacje Office 365, a w szczególności ISO 27001-27013, 27018 oraz certyfikacje SOC 1,2,3 potwierdzają spełnienie przez Microsoft warunków bezpieczeństwa dostępu wszystkich osób (także podwykonawców zewnętrznych) do informacji, w tym informacji o wysokim stopniu poufności.

Każdy dostęp do informacji jest traktowany jako wyjątek i jest weryfikowany, monitorowany i audytowany (zarówno przez ISO jak i SSAE16). Usługa jest zarządzana i obsługiwana przez pracowników Microsoft, a w razie potrzeby przez podwykonawców, których zarządzanie jest prowadzone przez Microsoft. Wszyscy podwykonawcy mają podpisaną umowę z Microsoft, zgodnie z którą musi zostać zapewniony co najmniej ten sam poziom ochrony prywatności, jak w przypadku pracowników Microsoft; z kolei pracownicy Microsoft są zobowiązani do zachowania poufności. Jeżeli Klient skonfiguruje usługi online lub przydzieli zasoby swoim dzierżawcom w taki sposób, że jego dane będą znajdowały się poza EOG, dane te mogą być przekazywane poza EOG na podstawie umowy powierzenia przetwarzania danych, zgodnej ze standardowymi klauzulami umownymi (Załącznik nr 3 do OST), którą Klient zawiera z Microsoft Corp.

- *zasady związane z prawami do oprogramowania (w tym jego kodów źródłowych) w trakcie współpracy i po jej zakończeniu, w szczególności dostępu do kodów źródłowych w przypadku zaprzestania świadczenia usług wsparcia i rozwoju oprogramowania przez jego dostawcę (np. z wykorzystaniem usług depozytu kodów źródłowych),*

Zasady związane z prawami do korzystania oprogramowania stanowią przedmiot Umowy Enterprise, poszczególnych licencji na produkty oraz umowy MBSA. Usługi online są udostępniane na podstawie licencji subskrypcyjnych. Z uwagi na charakter usług online, które są standardowymi, masowo oferowanymi subskrypcjami, Microsoft nie udostępnia kodu źródłowego oprogramowania dot. usług online.

– *parametry dotyczące jakości świadczonych usług oraz sposoby ich monitorowania i egzekwowania,*

Parametry dotyczące jakości świadczonych usług stanowią przedmiot odrębnego SLA. Sposoby monitorowania jakości świadczonych usług zostały opisane powyżej.

Z punktu widzenia Microsoft, architektura usług online zapewnia wysoką dostępność każdego z elementów. Np. w ramach Exchange Online każda skrzynka jest replikowana na kilka serwerów fizycznych, w tym serwerów z obu ośrodków przetwarzania (w przypadku usług w Europie: Amsterdam i Dublin), oddzielonych od siebie o przynajmniej 100 km.

Biorąc pod uwagę możliwość wykorzystania zasobów w różnych częściach świata i strefach czasowych, Microsoft jest w stanie wdrażać zmiany i aktualizacje bez wpływu na dostępność usług dla zakładu ubezpieczeń. W rezultacie usługi online są dostępne w sposób niemal ciągły (poziom dostępności w ostatnim kwartale 2015 r. wyniósł 99,98%[6]). Szczegółowe informacje o dostępności usług są także dostępne indywidualnie, poprzez panel administracyjny Office 365 lub w ramach subskrypcji RSS.

Jeżeli przestoje okazałyby się konieczne, ewentualne ograniczenia dostępności dla środkowoeuropejskiej strefy czasowej to godz. 20:00 do 2:00 w nocy (a więc poza godzinami pracy zakładu ubezpieczeń). Zakład ubezpieczeń byłby każdorazowo uprzednio informowany o planowanym przestoju.

– *zasady i tryb obsługi zgłoszeń dotyczących problemów w zakresie świadczonych usług,*

Zasady zgłaszania problemów w zakresie świadczonych usług zostały wskazane w pkt. „Reklamacje" na str. 4 SLA. Pomoc techniczna dla usług online świadczona jest przez Microsoft zarówno za pośrednictwem internetu jak też telefonicznie – dostęp do niej jest intuicyjny z poziomu danej aplikacji. Ze względu na standardowy charakter usług, w większości przypadków wystarczającym będzie wsparcie w zakresie wystandaryzowanych problemów technicznych. Dodatkowo, klient ma możliwość skorzystania z specjalistycznego wsparcia na podstawie umów Microsoft Premier.

– *zasady i tryb dokonywania aktualizacji oprogramowania komponentów infrastruktury znajdujących się pod kontrolą dostawcy,*

Ze względu na specyfikę usług online, aplikacje oddane do użytku Klientów podlegają automatycznej aktualizacji dokonywanej przez Microsoft. W przypadku konieczności aktualizacji komponentów lokalnych, znajdą zastosowanie postanowienia OST (str. 5).

– *zasady współpracy w przypadku wystąpienia incydentu naruszenia bezpieczeństwa środowiska teleinformatycznego,*

Zasady postępowania w przypadku naruszenia bezpieczeństwa informacji zostały szczegółowo opisane w OST (str. 12 i n.; zob. również wyjaśnienia powyżej).

[6] Por. https://products.office.com/en-us/business/office-365-trust-center-operations

– *zasady w zakresie dalszego zlecania czynności podwykonawcom zewnętrznego dostawcy usług,*

Zgodnie z OST (s. 8 oraz 11), Microsoft może zaangażować podwykonawców do świadczenia pewnych usług ograniczonych lub dodatkowych w swoim imieniu. Lista podwykonawców i powierzanie im czynności są publikowane przez Microsoft pod adresem: http://www.microsoft.com/online/legal/v2/?docid=26

W związku z funkcjonowaniem usług online podzlecane mogą być jedynie czynności pomocnicze, nie mające zasadniczego znaczenia dla usług świadczonych przez Microsoft na rzecz zakładu ubezpieczeń – ich wykonanie nie ma wpływu na możliwość skorzystania przez zakład ubezpieczeń z usług online. Powierzenie przez Microsoft pewnych czynności pomocniczych nie będzie się wiązało z ich dostępem do danych zakładu ubezpieczeń, w tym danych objętych tajemnicą ubezpieczeniową. W przypadku Office 365, zasada ta będzie obowiązywała wszystkich podwykonawców wykonujących wszystkie rodzaje czynności pomocniczych, takich jak usługi sieciowe, utrzymanie sprzętu, wsparcie przy rozwiązywaniu problemów, czy wsparcie użytkownika (np. udzielanie porad użytkownikom przez telefon).

W zupełnie wyjątkowych sytuacjach związanych z bardziej skomplikowanym wsparciem klienta (np. koniecznością bezpośredniej ingerencji w załącznik do maila), wsparcie ze strony podwykonawcy mogłoby się wiązać z dostępem podwykonawcy do treści danych zakładu ubezpieczeń zawierających tajemnicę ubezpieczeniową. W takim przypadku dostęp podwykonawcy zawsze zależy od decyzji Klienta i to Klient może zdecydować o nieskorzystaniu z takiego wsparcia (co nie będzie miało wpływu na możliwość korzystania z usług online).

Korzystając z funkcjonalności Lockbox Office 365, Klient może bowiem bezpośrednio decydować o tym czy, kiedy i kto może ewentualnie uzyskać dostęp do zawartości jego danych w związku z usługami wsparcia (https://blogs.office.com/2015/04/21/announcing-customer-lockbox-for-office-365/ oraz https://support.office.com/en-us/article/Office-365-Customer-Lockbox-Requests-36f9cdd1-e64c-421b-a7e4-4a54d16440a2). Oznacza to, że Klient może ogólnie zablokować dostęp do danych klienta w związku z usługami wsparcia i zezwalać na taki dostęp jedynie w konkretnych sytuacjach. W rezultacie, decyzja o udzieleniu zgody na dostęp wymaga każdorazowo zatwierdzenia przez administratora sieci w zakładzie ubezpieczeń.

Jeżeli zachodziłaby opisana powyżej potrzeba udzielenia dostępu do konkretnej skrzynki mailowej, Klient może zaszyfrować zawarte w niej maile przed udzieleniem do niej dostępu Microsoft w ramach procedury Lockbox.

Zgodnie z umową MBSA Microsoft ponosi odpowiedzialność za działania podwykonawców.

– *kary umowne związane z nieprzestrzeganiem warunków umownych, w szczególności w zakresie bezpieczeństwa informacji przetwarzanych przez dostawcę usług.)*

Umowy nie przewidują kar umownych z tytułu ich naruszenia, jakkolwiek w przypadku naruszenia Umowy SLA, Klienci mogą skorzystać z obniżki wynagrodzenia.

3. Korzystanie z usługi online w świetle UDU

(15) Czy obowiązujące przepisy prawa zakazują korzystania z usług online przez zakłady ubezpieczeń lub pośredników ubezpieczeniowych?

Nie. Ani przepisy UDU, ani przepisy ustawy z dnia 22 maja 2003 r. o pośrednictwie ubezpieczeniowym nie stoją na przeszkodzie korzystania z usług online przez zakłady ubezpieczeń czy pośredników ubezpieczeniowych.

Z przypadku zakładów ubezpieczeń, korzystanie z usług online wymaga analizy z punktu widzenia zarządzania ryzykiem w kontekście outsourcingu oraz zasad ochrony danych objętych tajemnicą ubezpieczeniową.

(16) Czy usługi online stanowią outsourcing w rozumieniu UDU?

W naszej ocenie – nie. Począwszy od 2016 r., UDU przewiduje relatywnie wąską definicję outsourcingu. Zgodnie z art. 3 ust. 1 UDU, outsourcing oznacza umowę między zakładem ubezpieczeń a dostawcą usług, na podstawie której dostawca usług wykonuje proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez zakład ubezpieczeń, a także umowę, na podstawie której dostawca usług powierza wykonanie takiego procesu, usługi lub działania innym podmiotom, za pośrednictwem których wykonuje on dany proces, usługę lub działanie.

Usługi online stanowią specjalistyczne i wystandaryzowane usługi IT świadczone przez Microsoft szerokiemu kręgowi odbiorców. Tworzenie tego typu rozwiązań nie powinno być uznawane za „proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez zakład ubezpieczeń". Zakłady ubezpieczeń nie zajmują się (a nawet – nie mogą zajmować się) świadczeniem tego typu usług. Nie można też od nich racjonalnie oczekiwać, aby samodzielnie tworzyły tak zaawansowane procesy informatyczne.

Jednakże, według naszej wiedzy, KNF przyjmuje szersze, wychodzącą poza brzmienie UDU, rozumienie outsourcingu, zgodnie z którym usługi przetwarzania danych w chmurze mogą zostać zakwalifikowane jako outsourcing w rozumieniu UDU.

(17) Z czym łączy się potencjalna kwalifikacja usług online jako outsourcingu w rozumieniu UDU?

Kwalifikacja usług online jako outsourcingu łączy się przede wszystkim z koniecznością przeprowadzenia przez dany zakład ubezpieczeń analizy ryzyka związanego ze skorzystaniem z tych usług. Według naszej wiedzy, jest to kluczowy obowiązek, na który wskazuje KNF w przypadku chęci skorzystania z usług online przez zakład ubezpieczeń.

Dalsze obowiązki mogłyby ciążyć na zakładzie ubezpieczeń w przypadku uznania, że usługi online używane są przez dany zakład ubezpieczeń jako element systemu zarządzania (art. 73 i n. UDU). W naszej ocenie taka kwalifikacja jest mało prawdopodobna – nie można jej jednak wykluczyć w konkretnych przypadkach. Nawet jednak w przypadku przyjęcia takiej kwalifikacji, biorąc pod uwagę rozbudowane postanowienia Aneksu Finansowego oraz

uprawnienia kontrolne samego zakładu ubezpieczeń, usługi online powinny zostać uznane przez zakład ubezpieczeń za spełniające wymogi, o których mowa w art. 74 UDU.[7]

Ogólne postanowienia dotyczące odpowiedzialności Microsoft za nienależyte wykonanie usług online uregulowane zostały w umowie MBSA. Postanowienia umowy MBSA przewidują standardowe dla sektora IT wyłączenia odpowiedzialności. W kontekście art. 76 UDU należy jednak zwrócić uwagę, że ograniczenia te nie dotyczą roszczeń zgłaszanych przez niestowarzyszone osoby trzecie (np. klientów zakładu ubezpieczeń) wynikających z dostarczania usług online z naruszeniem ogólnych przepisów prawa, czy też szkód wyrządzonych z winy umyślnej.[8]

(18) Czy usługi online umożliwiają zgodność z wymogami sektorowymi dotyczącymi przestrzegania tajemnicy ubezpieczeniowej?

Tak. Zgodnie z art. 35 ust. 2 UDU, zakład ubezpieczeń może umożliwić dostęp do danych objętych tajemnicą ubezpieczeniową, m.in., podmiotowi przetwarzającemu na zlecenie zakładu ubezpieczeń dane dotyczące ubezpieczających, ubezpieczonych lub uprawnionych z umów ubezpieczenia oraz administrujących indywidualnymi kontami jednostek uczestnictwa w ubezpieczeniowym funduszu kapitałowym. Jak wskazano powyżej, zgodnie z MBSA, MPSA i OST, Klient powierza Microsoft przetwarzanie danych osobowych w imieniu Klienta.

W kontekście obowiązku zachowywania poufności określonych danych generowanych i przetwarzanych przez zakłady ubezpieczeń wskazujemy, że usługi online są świadczone zgodnie z zasadami bezpieczeństwa informacji opisanymi w odpowiedziach na pyt. (10)-(11) powyżej. W szczególności, dane Klienta przechowywane w chmurze w ramach usług online są chronione przed nieuprawnionym dostępem zarówno fizycznie, jak również w drodze szyfrowania przy użyciu funkcji *BitLocker*, umożliwiającej szyfrowanie na woluminach, czy też przy użyciu mechanizmów szyfrowania plików w Skype dla Firm, OneDrive dla Firm, oraz SharePoint Online. Szyfrowanie może odbywać zarówno za pomocą kluczy zarządzanych przez *Bitlocker*, jak również – w przypadku Szyfrowania Zaawansowanego w aplikacji Exchange Online oraz SharePoint Online – kluczy kontrolowanych przez Klienta.

---

[7] Zgodnie z tym przepisem „[o]utsourcing czynności ubezpieczeniowych lub reasekuracyjnych oraz funkcji należących do systemu zarządzania może odbywać się, pod warunkiem że:
1) dostawca usług będzie współpracował z organem nadzoru w zakresie powierzonych czynności lub funkcji;
2) zakład ubezpieczeń, zakład reasekuracji, podmiot uprawniony do badania sprawozdań finansowych zakładu ubezpieczeń i zakładu reasekuracji, podmiot uprawniony do badania sprawozdań o wypłacalności i kondycji finansowej zakładu ubezpieczeń i zakładu reasekuracji oraz organ nadzoru będą posiadać dostęp do danych związanych z powierzonymi czynnościami lub funkcjami;
3) organ nadzoru będzie miał możliwość przeprowadzania kontroli działalności i stanu majątkowego dostawcy usług w zakresie powierzonych czynności lub funkcji."

[8] Zapis dot. odpowiedzialności w MBSA mogą się różnić w zależności od wersji. Wskazany zapis pochodzi z umowy MBSA 2014. W aktualnej wersji Nov2015 zapis różni się jedynie nieznacznie i stanowi, że żadne ograniczenia ani wyłączenie nie będą miały zastosowania do odpowiedzialności stron z tytułu zobowiązań do obrony i zabezpieczenia. Zobowiązania do obrony uregulowane są w pkt. 6.a, który stanowi że Microsoft będzie bronić Klienta przed wszelkimi roszczeniami zgłaszanymi przez niestowarzyszone osoby trzecie (...) w związku ze świadczeniem przez Microsoft usługi online z naruszeniem przepisów obowiązujących wszystkich dostawców usług online.

Ponadto, treść danych Klienta przechowywanych w chmurze w ramach usług online co do zasady nie jest ujawniana Microsoft, jego podwykonawcom, czy też osobom trzecim (zob. odpowiedzi na pyt. (10) oraz (14) powyżej). Ujawnienie danych Klienta spółce Microsoft lub jej podwykonawcom może być wymagane wyjątkowo w związku ze świadczeniem Klientowi usług wsparcia, przy czym w ramach usług online Office 365 Microsoft oferuje również usługę *Customer Lockbox*, która pozwala Klientowi na bezpośrednie decydowanie o tym: czy, kto i przez jaki czas może ewentualnie uzyskać dostęp do zawartości określonych danych Klienta w związku z usługami wsparcia.

Poza powyższym, usługi online zawierają takie usługi jak Rights Management System (RMS), Information Rights Management (IRM), czy też Microsoft Azure Active Directory Rights Management (Microsoft Azure AD RM), które umożliwiają Klientowi definiowanie osób uprawnionych do uzyskiwania oraz przetwarzania określonych danych Klienta. Wskazane usługi umożliwiają Klientowi przestrzeganie wymogów poufności oraz realizację programów zgodności w drodze przyznawania dostępu do określonych danych Klienta przechowywanych w chmurze wyłącznie tym osobom, w przypadku których dostęp do danych jest wymagany z uwagi na zadania i obowiązki służbowe, jak również wyłączenie możliwości ujawniania danych w sposób dyskryminacyjny.

4. Zastrzeżenia

(1) Niniejsza analiza została przygotowana na zlecenie Microsoft sp. z o.o. w oparciu o dokumenty wskazane wyraźnie w pkt. 1 analizy i w wersji obowiązującej na dzień jej sporządzenia. W szczególności nie analizowaliśmy polityki bezpieczeństwa ani instrukcji zarządzania obowiązujących w spółkach z grupy Microsoft.

(2) Przedmiotem niniejszej analizy nie jest potwierdzenie zgodności oświadczeń, zobowiązań i informacji zawartych w dokumentach o których mowa w pkt. 1 analizy. Analiza jest ograniczona ściśle do kwestii prawa polskiego (w tym prawa UE), nie obejmując kwestii podlegających prawu obowiązującemu w jakiejkolwiek innej jurysdykcji.

(3) Ewentualne udostępnienie niniejszej analizy przez Microsoft Sp. z o.o. innym podmiotom nie stanowi świadczenia usług doradztwa prawnego podmiotom otrzymującym niniejszą analizę. Każdy otrzymujący przyjmuje do wiadomości, że powinien zasięgnąć niezależnej opinii prawnej dotyczących kwestii omawianych w analizie.

* * *

W przypadku jakichkolwiek pytań, uprzejmie prosimy o kontakt.

Z poważaniem,

Agata Szeliga
Partner, radca prawny

dr Wojciech Iwański
adwokat