Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców

Zakres zastosowania

Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców („**DPR**”) obowiązują każdego dostawcę firmy Microsoft, który Przetwarza Dane osobowe firmy Microsoft lub Dane poufne firmy Microsoft w związku z wykonywaniem zobowiązań przez tego dostawcę (np. dostarczanie usług, licencji oprogramowania, usług w chmurze) na podstawie warunków jego umowy z firmą Microsoft (np. warunków Zamówienia zakupu, umowy ramowej) („**Wykonanie zobowiązań**” lub „**Wykonywanie zobowiązań**”).

- W przypadku konfliktu wymagań zawartych w niniejszym dokumencie z wymaganiami określonymi w umowach między dostawcą a firmą Microsoft wyższy priorytet mają wymagania DPR, chyba że dany dostawca określi w formularzu atestu zgodności z wymaganiami DPR odpowiednie postanowienia umowy, które powodują konflikt z odpowiednią częścią wymagań DPR (w takim przypadku wyższy priorytet mają warunki umowy).
- W przypadku konfliktu między wymaganiami zawartymi w niniejszym dokumencie a jakimikolwiek wymaganiami prawnymi lub ustawowymi wyższy priorytet mają wymagania prawne lub ustawowe.
- Jeżeli dostawca firmy Microsoft działa jako Administrator w odniesieniu do niniejszych wymagań DPR, tylko wymagania w części J Bezpieczeństwo i części A Zarządzanie mają zastosowanie do działań związanych z Przetwarzaniem przez tego dostawcę.
- W przypadku gdy dostawca firmy Microsoft nie przetwarza Danych osobowych firmy Microsoft, a tylko Dane poufne firmy Microsoft, w odniesieniu do niniejszych wymagań DPR, tylko wymagania w części A Zarządzanie, części E Przechowywanie i części J Bezpieczeństwo mają zastosowanie do Przetwarzania przez tego dostawcę Danych poufnych firmy Microsoft.

Międzynarodowe przekazywanie danych

Bez ograniczania innych zobowiązań, dostawca nie będzie przeprowadzał międzynarodowego przekazywania Danych osobowych firmy Microsoft, jeśli firma Microsoft nie wyraziła wcześniej zgody w formie pisemnej, oraz w każdym przypadku dostawca spełni wymagania dotyczące ochrony danych określone przez dowolne standardowe warunki umowy, wiążące reguły korporacyjne lub inne programy zatwierdzone przez dowolny organ ochrony danych, Europejską Radę Ochrony Danych lub Komisję Europejską i przyjęte lub uzgodnione przez firmę Microsoft, w szczególności przez zawarte między UE i Stanami Zjednoczonymi oraz Szwajcarią i Stanami Zjednoczonymi porozumienie Privacy Shield i ogólne rozporządzenie o ochronie danych UE. Dostawca zobowiązuje się do powiadamiania firmy Microsoft o wszelkiej swojej niezdolności do zapewnienia poziomu ochrony wymaganego przez zasady Privacy Shield. Dostawca powinien także zapewnić, że każdy podwykonawca (zgodnie z definicją w ust. 1(d) standardowych klauzul umownych z 2010 roku opublikowanych jako załącznik do decyzji Komisji Europejskiej C(2010)593) spełnia te wymagania.

Najważniejsze definicje

Poniższe pojęcia użyte w niniejszych wymaganiach DPR mają znaczenie podane poniżej. Przykłady występujące po wyrażeniach „w tym”, „takie jak”, „np.”, „na przykład” lub podobne użyte w niniejszych wymaganiach DPR należy interpretować jak zawierające wyrażenie „szczególnie” lub „w szczególności”, chyba że użyto słów takich jak „tylko” lub „wyłącznie”.

„**Administrator**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby Przetwarzania Danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w Prawie Unii Europejskiej („**UE**”) lub państwa członkowskiego, to również w Prawie Unii lub w Prawie

państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

„**Dane osobowe firmy Microsoft**” oznaczają wszelkie Dane osobowe Przetwarzane przez firmę Microsoft lub w jej imieniu.

„**Dane osobowe**” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („**Osoba, której dane dotyczą**”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

„**Dane poufne firmy Microsoft**” to wszelkie informacje, których ujawnienie poprzez naruszenie poufności lub integralności może spowodować znaczne straty finansowe firmy Microsoft lub znaczny uszczerbek dla jej reputacji. Dotyczy to produktów sprzętowych i programowych firmy Microsoft, wewnętrznych aplikacji biznesowych, przedpremierowych materiałów marketingowych, kluczy licencji produktów i dokumentacji technicznej związanej z produktami i usługami firmy Microsoft.

„**Naruszenie ochrony danych**” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub Niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych lub Danych poufnych firmy Microsoft przesyłanych, przechowywanych lub w inny sposób Przetwarzanych.

„**Podmiot przetwarzający**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który Przetwarza Dane osobowe w imieniu Administratora.

„**Prawo Osoby, której dane dotyczą**” oznacza prawo Osoby, której dane dotyczą do uzyskania dostępu, usunięcia, edycji, eksportu, ograniczenia lub wniesienia sprzeciwu wobec Przetwarzania Danych osobowych firmy Microsoft tej Osoby, której dane dotyczą, jeżeli jest to wymagane przez Prawo.

„**Prawo**” oznacza wszystkie odpowiednie przepisy, zasady, statuty, dekrety, decyzje, rozporządzenia, rozporządzenia regulacyjne, kodeksy, akty, rezolucje i wymagania dowolnego organu rządowego (federalnego, stanowego, lokalnego lub międzynarodowego) posiadającego właściwość. „**Niezgodne z prawem**” oznacza każde naruszenie Prawa.

„**Przetwarzanie**” oznacza operację lub zestaw operacji wykonywanych na Danych osobowych lub Danych poufnych firmy Microsoft w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Pojęcia „Przetwarzanie” i „Przetworzone” będą miały jednakowe znaczenie.

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część A: Zarządzanie		
1	Każda odpowiednia umowa między firmą Microsoft a dostawcą (np. umowa ramowa, wykaz zakresu prac, zamówienia zakupu i inne zamówienia) zawiera informacje o ochronie danych związanej z prywatnością i bezpieczeństwem odpowiednio w odniesieniu do Danych poufnych i Danych osobowych firmy Microsoft. W przypadku firm pełniących funkcję Podmiotów przetwarzających umowa musi obejmować przedmiot i czas trwania Przetwarzania, charakter i cel Przetwarzania, rodzaj Danych osobowych firmy Microsoft oraz kategorie Osób, których dane dotyczą, obowiązki i prawa firmy Microsoft.	Dostawca musi przedstawić odpowiednią umowę między firmą Microsoft a Dostawcą. W przypadku Podmiotów przetwarzających opisy Przetwarzania są zawarte w odpowiedniej umowie (*np.* wykazie zakresu prac, zamówieniach zakupu). Uwaga: W przypadku firm z zamówienia zakupu w toku odpowiedni opis działań dotyczących Przetwarzania może zostać dodany później podczas dokonywania zakupów.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
2	Wyznaczenie osoby lub grupy osób w firmie, która będzie ponosić odpowiedzialność za zapewnienie zgodności z wymaganiami DPR.	Imię i nazwisko osoby lub nazwa grupy odpowiedzialnej za zapewnienie zgodności z Wymagania firmy Microsoft dotyczącymi ochrony danych przez dostawców. Dokument opisujący uprawnienia i obowiązki tej osoby lub grupy pełniącej rolę dotyczącą ochrony prywatności i/lub bezpieczeństwa.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
3	Opracowanie, utrzymywanie i przeprowadzanie corocznych szkoleń w zakresie ochrony prywatności i bezpieczeństwa dla pracowników, którzy będą mieli dostęp do Danych osobowych lub Danych poufnych firmy Microsoft. Jeżeli firma nie ma przygotowanych materiałów, może skorzystać z tego konspektu scenorysu i dostosować go zgodnie z wymaganiami firmy.	Dostępne są roczne dane na temat obecności. Zawartość szkoleniowa obejmuje zasady ochrony prywatności i bezpieczeństwa.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część A: Zarządzanie (cd.)		
4	Przetwarzanie Danych osobowych firmy Microsoft tylko zgodnie z udokumentowanymi instrukcjami firmy Microsoft dotyczącymi na przykład przesyłania Danych osobowych firmy Microsoft do kraju trzeciego lub organizacji międzynarodowej, z wyjątkiem okoliczności, w których jest to wymagane przez przepisy Prawa (w takim wypadku przed rozpoczęciem Przetwarzania Podmiot przetwarzający (dostawca) poinformuje administratora (firmę Microsoft) o tym wymaganiu prawnym, jeżeli te przepisy Prawa nie zabraniają ujawniania tych informacji ze względu na ważny interes publiczny.	Udokumentowane dowody istnienia instrukcji, na przykład w formie zapisów w umowie (np. wykaz zakresu prac lub zlecenie zakupu) albo zarejestrowane w systemie elektronicznym używanym do Wykonywania zobowiązań.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część B: Powiadamianie		
5	Dostawca jest zobowiązany do stosowania Zasad zachowania poufności informacji firmy Microsoft w przypadku zbierania Danych osobowych w imieniu firmy Microsoft. Zasady zachowania poufności informacji muszą być zrozumiałe i dostępne dla Osób, których dane dotyczą, aby ułatwiać im podjęcie decyzji o przesłaniu ich Danych osobowych do dostawcy. Uwaga: Jeżeli firma jest Administratorem działań dotyczących Przetwarzania, musi opublikować własne zasady zachowania poufności informacji. *Aby uzyskać dostęp do odpowiednich powiadomień firmy Microsoft, należy wysłać wiadomość na adres SSPAHelp@microsoft.com.*	Dostawca wykorzystuje fwdlink do aktualnych, opublikowanych Zasad zachowania poufności informacji firmy Microsoft. Zasady zachowania poufności informacji są publikowane w każdym kontekście, w którym będą zbierane Dane osobowe użytkownika. Jeżeli jest to konieczne, wersja offline jest dostępna i udostępniana przed zebraniem danych. Zasady zachowania poufności informacji w wersji offline to najnowsza opublikowana wersja z odpowiednią datą. W przypadku usług dla pracowników firmy Microsoft stosowane jest Powiadomienie firmy Microsoft o ochronie danych.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
6	Dostawcy zbierający Dane osobowe firmy Microsoft podczas rozmów telefonicznych lub na podstawie nagranych rozmów telefonicznych muszą być przygotowani do omówienia z Osobami, których dane dotyczą obowiązujących zasad zbierania, przetwarzania, wykorzystywania i przechowywania danych.	Skrypt nagrań głosowych opisuje, w jaki sposób Dane osobowe firmy Microsoft są Przetwarzane i obejmuje: ▪ gromadzenie, ▪ wykorzystanie i ▪ przechowywanie.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część C: Wybór i zgoda		
7	Jeżeli wyrażenie zgody jest prawnie wymagane do Przetwarzania danych, dostawca musi uzyskać i zarejestrować zgodę Osoby, której dane dotyczą, na wszystkie swoje działania dotyczące Przetwarzania (w tym nowe i zaktualizowane działania dotyczące Przetwarzania) przed rozpoczęciem zbierania Danych osobowych tej Osoby, której dane dotyczą.	Dostawca może wykazać sposób udzielenia przez Osobę, której dane dotyczą, zgody na Przetwarzanie a zakres zgody obejmuje wszystkie działania dostawcy dotyczące Przetwarzania w odniesieniu do Danych osobowych Osoby, której dane dotyczą. Dostawca może wykazać, w jaki sposób Osoba, której dane dotyczą, wycofuje zgodę na działania dotyczące Przetwarzania. Dostawca może wykazać, w jaki sposób sprawdzane są preferencje przed rozpoczęciem nowych działań dotyczących Przetwarzania. Dostawca monitoruje skuteczność zarządzania preferencjami, aby zapewnić, że czas na zmianę jest zgodny z najbardziej restrykcyjnymi obowiązującymi wymaganiami prawnymi. Uwaga: Dowodem mogą być zrzuty ekranu interakcji użytkownika, eksperymenty z usługą lub możliwość wyświetlenia dokumentacji technicznej.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część C: Wybór i zgoda (cd.)		
8	Pliki cookie są małymi plikami tekstowymi zapisywanymi na urządzeniach przez witryny internetowe i/lub aplikacje, które zawierają informacje używane do identyfikowania Osoby, której dane dotyczą, lub urządzenia. Dostawcy tworzący witryny internetowe i aplikacje firmy Microsoft i/lub zarządzający nimi muszą zapewnić Osobom, których dane dotyczą, wyraźne powiadomienie i możliwość wyboru opcji korzystania z plików cookie. Dostawcy tworzący witryny internetowe i/lub aplikacje firmy Microsoft oraz zarządzający nimi muszą zagwarantować, że pliki cookie są używane zgodnie z deklaracjami w Zasadach zachowania poufności informacji firmy Microsoft i lokalnymi zobowiązaniami prawnymi, takimi jak przepisy ustanowione przez UE.	Cel użycia każdego pliku cookie musi być udokumentowany z uwzględnieniem typu stosowanego pliku cookie. ▪ Nie wolno używać trwałych plików cookie, jeżeli pliki cookie dotyczące sesji są wystarczające. ▪ Jeżeli używane są trwałe pliki cookie, ich data ważności nie może upływać za więcej niż 2 lata od momentu odwiedzenia witryny przez użytkownika. W przypadku użytkowników w UE okres ważności trwałego pliku cookie nie może przekraczać 13 miesięcy. Sprawdzenie zgodności z obowiązującym Prawem EU, np. ▪ użycie konwencji oznaczania „Ochrona prywatności i pliki cookie” w odniesieniu do zasad zachowania poufności informacji i ▪ zapewnienie uzyskania zgody od użytkownika przed użyciem plików cookie do celów innych niż niezbędne, takich jak reklamowe.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część D: Zbieranie		
9	Dostawca musi monitorować zbieranie Danych osobowych i/lub Danych poufnych firmy Microsoft w celu upewnienia się, że zbierane są tylko dane wymagane do Wykonania zobowiązań.	Dostawca może udostępnić dokumentację wykazującą, że zbierane Dane osobowe i/lub Dane poufne firmy Microsoft są wymagane do Wykonania zobowiązań.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
10	Jeżeli dostawca zbiera Dane osobowe od stron trzecich w imieniu firmy Microsoft, musi upewnić się, że zasady i procedury ochrony danych stosowane przez strony trzecie są zgodne z umową zawartą przez dostawcę z firmą Microsoft i wymaganiami DPR.	Dostawca może udostępnić dokumentację przeprowadzenia analizy należytej staranności w odniesieniu do zasad i praktyk stron trzecich w zakresie ochrony danych.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
11	Przed rozpoczęciem zbierania Danych osobowych firmy Microsoft przy użyciu oprogramowania zainstalowanego lub uruchamianego na urządzeniu Osoby, której dane dotyczą, należy udokumentować konieczność zbierania tych danych w formie wiążącej umowy dostawcy z firmą Microsoft.	Umowa z firmą Microsoft dotycząca użycia uruchamianego oprogramowania na urządzeniu Osoby, której dane dotyczą, jest określona w realizowanej umowie.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
12	Przed rozpoczęciem zbierania poufnych Danych osobowych firmy Microsoft (danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych, danych dotyczących zdrowia lub seksualności albo orientacji seksualnej osoby fizycznej) należy udokumentować konieczność zbierania Danych osobowych firmy Microsoft w formie wiążącej umowy dostawcy z firmą Microsoft.	Konieczność zbierania poufnych Danych osobowych firmy Microsoft jest określona w realizowanej umowie z firmą Microsoft.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część E: Przechowywanie		
13	Zagwarantowanie, że Dane osobowe i Dane poufne firmy Microsoft nie są przechowywanie dłużej niż jest to wymagane do Wykonania zobowiązań, chyba że kontynuowanie przechowywania Danych osobowych i/lub Danych poufnych firmy Microsoft jest wymagane przez Prawo.	Dostawca postępuje zgodnie z udokumentowanymi zasadami przechowywania danych albo wymaganiami określonymi przez firmę Microsoft w umowie (np. wykazie zakresu prac lub zleceniu zakupu).	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
14	Zagwarantowanie, że zgodnie z decyzją firmy Microsoft Dane osobowe i Dane poufne firmy Microsoft, które pozostają w dyspozycji lub pod kontrolą dostawcy, są zwracane firmie Microsoft lub niszczone po zakończeniu Wykonania zobowiązań albo na żądanie firmy Microsoft. Należy ustanowić w aplikacjach procesy gwarantujące bezpieczne usunięcie danych, gdy dane są usuwane z aplikacji przez użytkownika lub po spełnieniu określonych warunków, takich jak określony czas trwania przechowywania danych. Gdy konieczne jest zniszczenie Danych osobowych lub Danych poufnych firmy Microsoft, dostawca musi spalić, rozdrobnić lub podrzeć zasoby fizyczne zawierające Dane osobowe i/lub Dane poufne firmy Microsoft w sposób uniemożliwiający ich odczytanie lub odtworzenie.	Prowadzenie rejestru usuwania Danych osobowych i Danych poufnych firmy Microsoft (może to obejmować zwrot do firmy Microsoft w celu zniszczenia). Jeżeli zniszczenie jest konieczne lub wymagane przez firmę Microsoft, należy udostępnić certyfikat zniszczenia podpisany przez dyrektora ze strony dostawcy.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część F: Osoby, których dane dotyczą		
	Osoby, których dane dotyczą, mają prawo uzyskania dostępu, usunięcia, edycji, eksportu, ograniczenia lub wniesienia sprzeciwu wobec Przetwarzania ich Danych osobowych („**Prawa Osób, których dane dotyczą**"). Gdy Osoba, której dane dotyczą, egzekwuje swoje prawa dotyczące jej Danych osobowych firmy Microsoft, wynikające z przepisów Prawa, dostawca musi:		
15	Wspierać firmę Microsoft przy użyciu odpowiednich środków technicznych i organizacyjnych, w jak najszerszym zakresie, w celu wywiązania się ze swoich zobowiązań dotyczących odpowiadania na żądania Osób, których dane dotyczą, egzekwujących swoje Prawa Osób, których dane dotyczą.	Dostępne są procesy i procedury ułatwiające egzekwowanie Praw Osób, których dane dotyczą.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
16	Odpowiadać bez nieuzasadnionej zwłoki na wszelkie żądania związane z Prawami Osób, których dane dotyczą.	Dostawca przeprowadza okresowe testy w celu upewnienia się, że może zapewnić egzekwowanie Praw Osób, których dane dotyczą.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
17	Jeżeli firma Microsoft nie zdecydowała inaczej, dostawca będzie kierować wszystkie kontaktujące się z nim bezpośrednio Osoby, których dane dotyczą, do firmy Microsoft w celu egzekwowania ich Praw Osób, których dane dotyczą. Dostawca będzie informować Osoby, których dane dotyczą, o wszystkich krokach, które dana osoba musi wykonać w celu uzyskania dostępu do swoich Danych osobowych firmy Microsoft lub egzekwowania w inny sposób swoich praw dotyczących tych danych. *Aby uzyskać więcej informacji na temat tego wymagania, należy przesłać odpowiednie zapytanie na adres SSPAHelp@microsoft.com.*	Dostawca informuje o procedurze uzyskiwania dostępu do Danych osobowych, a także dostępnych metodach aktualizowania tych danych.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
18	Przesyłając odpowiedź bezpośrednio do Osoby, której dane dotyczą, sprawdzić tożsamość Osoby, której dane dotyczą, zgłaszającej żądanie.	Dostawca udokumentował metodę stosowaną do identyfikacji Osób, których dane dotyczą, firmy Microsoft.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część F: Osoby, których dane dotyczą (cd.)		
	Po uwierzytelnieniu Osoby, której dane dotyczą, dostawca musi:		
19	Ustalić, czy Dane osobowe firmy Microsoft, związane z Osobą, której dane dotyczą, są przechowywane lub kontrolowane przez dostawcę.	Dostawca stosuje procedury umożliwiające ustalenie, czy Dane osobowe są przechowywane przez dostawcę.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
20	Podjąć uzasadnione działania w celu zlokalizowania żądanych Danych osobowych firmy Microsoft i prowadzić rejestr potwierdzający przeprowadzenie wyszukiwania w odpowiednim zakresie.	Dostawca prowadzi rejestr wykazujący działania podjęte w celu spełnienia żądań wynikających z Praw Osób, których dane dotyczą. Dokumentacja zawiera: ▪ datę i godzinę żądania, ▪ działania podjęte w odpowiedzi na żądanie oraz ▪ informacje o tym, kiedy poinformowano firmę Microsoft.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
21	Rejestrować datę i godzinę zgłoszenia żądania dotyczącego Praw Osób, których dane dotyczą, i działania podejmowane przez dostawcę w odpowiedzi na takie żądania. Udostępnić rejestr żądań Osób, których dane dotyczą, firmie Microsoft na jej prośbę.	Dostawca prowadzi rejestr żądań dostępu i dokumentuje zmiany wprowadzane w Danych osobowych.	
	Po uwierzytelnieniu Osoby, której dane dotyczą, i sprawdzeniu przez dostawcę, że dostępne są żądane Dane osobowe firmy Microsoft, dostawca musi:		
22	W przypadku żądania kopii Danych osobowych udostępnienie Osobie, której dane dotyczą, jej Danych osobowych firmy Microsoft w odpowiedniej formie drukowanej, elektronicznej lub ustnej.	Dostawca dostarcza Osobie, której dane dotyczą, jej Dane osobowe w formie, która jest zrozumiała i wygodna dla Osoby, której dane dotyczą, i dostawcy.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część F: Osoby, których dane dotyczą (cd.)		
23	Przekazanie Osobie, której dane dotyczą i której żądanie zostało odrzucone na zlecenie firmy Microsoft, pisemne wyjaśnienie zgodne z odpowiednimi instrukcjami udostępnionymi uprzednio przez firmę Microsoft. *Aby uzyskać więcej informacji na temat tego wymagania, należy przesłać odpowiednie zapytanie na adres SSPAHelp@microsoft.com.*	Dostawca dokumentuje wypadki odrzucenia żądań i przechowuje dowody weryfikacji i zatwierdzenia przez firmę Microsoft.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
24	Dostawca musi stosować uzasadnione środki ostrożności, aby uniemożliwić użycie Danych osobowych firmy Microsoft, udostępnionych Osobom, których dane dotyczą, do identyfikacji innej osoby.	Dostawca musi wykazać, że podejmuje uzasadnione środki bezpieczeństwa uniemożliwiające zidentyfikowanie innych osób na podstawie udostępnionych informacji (np. zakaz kopiowania całej strony w przypadku występowania żądanych Danych osobowych Osoby, której dane dotyczą, tylko w jednym wierszu).	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
25	Jeżeli Osoba, której dane dotyczą, i dostawca nie mogą uzgodnić, czy Dane osobowe firmy Microsoft są kompletne i dokładne, dostawca powinien zgłosić ten problem do firmy Microsoft i współpracować z firmą Microsoft w celu rozwiązania tego problemu. *Aby uzyskać więcej informacji na temat tego wymagania, należy przesłać odpowiednie zapytanie na adres SSPAHelp@microsoft.com.*	Dostawca dokumentuje przypadki braku zgody i przekazuje informacje o problemach do firmy Microsoft.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część G: Ujawnianie danych stronom trzecim		
	Jeżeli dostawca zamierza skorzystać z pomocy podwykonawcy związanej z Przetwarzaniem Danych osobowych lub Danych poufnych firmy Microsoft, musi:		
26	Uzyskać wyraźną pisemną zgodę firmy Microsoft przed zleceniem podwykonawcom świadczenia usług albo wprowadzeniem zmian związanych z dodaniem lub zmianą podwykonawców. *Aby uzyskać więcej informacji na temat tego wymagania, należy przesłać odpowiednie zapytanie na adres SSPAHelp@microsoft.com.*	Sprawdzenie, czy Dane osobowe firmy Microsoft są Przetwarzane wyłącznie przez firmy znane firmie Microsoft zgodnie z wymaganiami odpowiednich umów (np. wykazem zakresu prac, dodatkiem, zleceniem zakupu) lub zarejestrowane w bazie danych SSPA.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
27	Dokumentować charakter i zakres Danych osobowych oraz Danych poufnych firmy Microsoft, Przetwarzanych przez podwykonawców, w celu zapewnienia, że zbierane są tylko informacje wymagane do Wykonania zobowiązań.	Dostawca prowadzi dokumentację dotyczącą Danych osobowych oraz Danych poufnych firmy Microsoft ujawnianych lub przekazywanych podwykonawcom.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
28	Zagwarantować, że podwykonawca wykorzystuje Dane osobowe firmy Microsoft zgodnie z deklarowanymi przez Osobę, której dane dotyczą, preferencjami dotyczącymi kontaktowania się z nim.	Wykazanie, w jaki sposób preferencje Osoby, której dane dotyczą, firmy Microsoft są wykorzystywane przez podwykonawców. Udostępnienie dokumentacji dodatkowej zawierającej okres uznawania zmiany preferencji przez podwykonawcę.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
29	Ograniczyć Przetwarzanie Danych osobowych firmy Microsoft przez podwykonawców do celów niezbędnych do realizacji umowy dostawcy z firmą Microsoft.	Dostawca może udostępnić dokumentację wykazującą, że zbierane Dane osobowe firmy Microsoft są wymagane do Wykonywania zobowiązań.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
30	Sprawdzać skargi wskazujące na nieautoryzowane lub Niezgodne z prawem Przetwarzanie Danych osobowych firmy Microsoft.	Dostawca może przedstawić systemy i procesy przetwarzania skarg dotyczących nieupoważnionego wykorzystania lub ujawnienia Danych osobowych	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*

		firmy Microsoft przez podwykonawcę.	
Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
Część G: Ujawnianie danych stronom trzecim (cd.)			
31	Niezwłocznie powiadomić firmę Microsoft o wykryciu Przetwarzania przez podwykonawcę Danych osobowych lub Danych poufnych firmy Microsoft do celu innego niż związany z Wykonywaniem zobowiązań.	Dostawca udostępnił instrukcje i środki umożliwiające podwykonawcy zgłaszanie niewłaściwego użycia danych firmy Microsoft.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
32	Niezwłocznie podejmować działania w celu ograniczenia rzeczywistych lub potencjalnych szkód wynikających z nieautoryzowanego lub Niezgodnego z prawem Przetwarzania Danych osobowych oraz Danych poufnych firmy Microsoft przez podwykonawcę.	Dostawca może wykazać stosowanie planu i procedur na wypadek niewłaściwego użycia Danych osobowych i Danych poufnych firmy Microsoft przez podwykonawcę.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*
Część H: Jakość			
33	Dostawca musi zapewnić integralność wszystkich Danych osobowych firmy Microsoft, tak aby były one dokładne, kompletne i adekwatne, zgodnie z deklarowanym celem Przetwarzania tych danych.	Dostawca może wykazać stosowanie procedur sprawdzania poprawności Danych osobowych firmy Microsoft podczas ich zbierania, tworzenia i aktualizowania. Dostawca może wykazać stosowanie procedur ciągłego monitorowania i próbkowania w celu weryfikowania dokładności danych oraz wprowadzania niezbędnych korekt.	*<Spełnione> <Niespełnione> <Nie ma zastosowania> <Konflikt prawny> <Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część I: Monitorowanie i egzekwowanie		
34	Dostawca stosuje plan reagowania na incydenty, który wymaga powiadomienia przez Dostawcę firmy Microsoft bez nieuzasadnionej zwłoki po uzyskaniu informacji o Naruszeniu ochrony danych lub luce w zabezpieczeniach dotyczącej postępowania przez dostawcę z Danymi osobowymi lub Danymi poufnymi firmy Microsoft. *Aby zgłosić incydent, należy wysłać wiadomość na adres SSPAHelp@microsoft.com.*	Dostawca stosuje plan reagowania na incydenty obejmujący powiadomienie klientów (firmy Microsoft) zgodnie z opisem w tej części.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
35	Powstrzymanie się od publikowania informacji dla prasy lub innych powszechnie dostępnych powiadomień, dotyczących Naruszenia ochrony Danych osobowych lub Danych poufnych firmy Microsoft, bez uzyskania zezwolenia od firmy Microsoft, z wyjątkiem okoliczności, w których jest to wyraźnie wymagane przez Prawo.	Dostawca zobowiązuje się do spełnienia tego wymagania w przypadku incydentu.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
36	Wdrożenie planu działań zaradczych i monitorowanie rozwiązywania problemów z Naruszeniami ochrony danych i lukami w zabezpieczeniach związanych z Danymi osobowymi lub Danymi poufnymi firmy Microsoft w celu upewnienia się, że odpowiednie działania zaradcze są podejmowane na czas.	Dostawca stosuje udokumentowane procedury w celu eliminacji Naruszenia ochrony danych.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
37	Ustanowienie formalnego procesu obsługi skarg w celu rozpatrywania wszystkich skarg związanych z ochroną Danych osobowych firmy Microsoft.	Dostawca stosuje środki przyjmowania skarg dotyczących Danych osobowych firmy Microsoft i udokumentowaną procedurę rozpatrywania tych skarg.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo		
	Dostawca musi ustanowić, wdrożyć i prowadzić program bezpieczeństwa informacji, który uwzględnia zasady i procedury gwarantujące nieustanną ochronę Danych osobowych oraz Danych poufnych firmy Microsoft, zgodnie z zalecanymi procedurami branżowymi i przepisami Prawa. Program bezpieczeństwa wdrożony przez dostawcę musi być zgodny z poniższymi standardami (wymagania 38–56).	Zabezpieczenia mogą obejmować więcej zagadnień niż wymienione, jeżeli jest to konieczne do zachowania zgodności z przepisami (np. HIPAA, GLBA) lub wymaganiami określonymi w umowach. Prawidłowy raport ISO 27001 lub SOC 2 z zabezpieczeniami jest dopuszczalnym zamiennikiem części J. Aby zastosować ten zamiennik, należy skorzystać z adresu kontaktowego SSPAHelp@microsoft.com. Uwaga: Należy udostępnić dokumentację opisującą zakres tych certyfikatów/raportów.	
38	Wykonywanie corocznej oceny zabezpieczeń sieciowych, obejmującej następujące działania: ▪ przegląd najważniejszych zmian w środowisku, takich jak nowy składnik systemu, topologia sieci, reguły zapory; ▪ przeprowadzanie skanowań w poszukiwaniu luk w zabezpieczeniach oraz ▪ prowadzenie dzienników zmian.	Dostawca udokumentował oceny sieci, dzienniki zmian i wyniki skanowania. Wymagane dzienniki zmian muszą śledzić zmiany, zawierać informacje o przyczynie zmiany, a także imię i nazwisko oraz stanowisko wyznaczonej osoby zatwierdzającej.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
39	Dostawca definiuje, publikuje i wdraża zasady dotyczące urządzeń przenośnych, które zabezpieczają i ograniczają użycie Danych osobowych lub Danych poufnych firmy Microsoft, udostępnianych lub używanych na urządzeniu przenośnym.	Dostawca wykazuje stosowanie zgodnych zasad dotyczących urządzeń przenośnych, jeżeli Przetwarzanie Danych osobowych lub Danych poufnych firmy Microsoft wymaga stosowania urządzeń przenośnych.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
40	Wszystkie zasoby używane do wspomagania Wykonywania zobowiązań muszą być uwzględnione, a ich właściciel powinien być zidentyfikowany. Dostawca jest zobowiązany do prowadzenia wykazu tych zasobów informacyjnych, określenia dozwolonych i autoryzowanych metod użycia tych zasobów oraz zapewnienia odpowiedniego poziomu ochrony zasobów przez cały cykl użytkowania.	Wykaz zasobów używanych do wspomagania Wykonywania zobowiązań. Wykaz tych zasobów powinien zawierać następujące informacje: ▪ lokalizacja urządzenia; ▪ klasyfikacja danych przechowywanych w zasobie; ▪ rejestr odzyskiwania zasobów po zakończeniu zatrudnienia lub umowy biznesowej oraz ▪ rejestr utylizacji zbędnych nośników używanych do przechowywania danych.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
41	Ustanowienie i utrzymanie procedur zarządzania prawami dostępu w celu zapobiegania nieautoryzowanemu dostępowi do Danych osobowych lub Danych poufnych firmy Microsoft pozostających pod kontrolą dostawcy.	Dostawca wykazuje wdrożenie planu zarządzania prawami dostępu, który obejmuje następujące elementy: ▪ procedury kontroli dostępu; ▪ procedury identyfikacji; ▪ procedury blokowania po próbach uzyskania dostępu zakończonych niepowodzeniem; ▪ resetowanie haseł tak często, jak jest to konieczne, jednak przynajmniej co 90 dni; ▪ niezawodne parametry do wyboru poświadczeń używanych do uwierzytelniania oraz ▪ dezaktywację kont użytkowników nie później niż 48 godzin po zakończeniu zatrudnienia. Dostawca wykazuje ustanowienie procesu przeglądu dostępu użytkowników do Danych osobowych oraz Danych poufnych firmy Microsoft z uwzględnieniem zasady najniższego poziomu uprawnień. Proces powinien uwzględniać: ▪ jednoznacznie zdefiniowane role użytkowników; ▪ procedury przeglądu i uzasadniania zezwalania na dostęp do ról oraz ▪ sprawdzanie, czy udokumentowano uzasadnienie przyłączenia do grup/ról użytkowników z rolami uprawnionymi do dostępu do danych firmy Microsoft.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
42	Zdefiniowanie i wdrożenie procedur zarządzania poprawkami, które przypisują wyższy priorytet do poprawek zabezpieczeń dla systemów używanych do Przetwarzania Danych osobowych lub Danych poufnych firmy Microsoft. Procedury te obejmują: ▪ zdefiniowane podejście do oceny ryzyka w celu określenia priorytetów poprawek zabezpieczeń; ▪ możliwość obsługi i wdrażania poprawek awaryjnych; ▪ możliwość stosowania w odniesieniu do systemu operacyjnego i oprogramowania serwera, takiego jak serwer aplikacji i oprogramowanie baz danych; ▪ dokumentowanie ryzyka ograniczanego przez poprawkę i śledzenie wszelkich wyjątków oraz ▪ wymagania dotyczące wycofania oprogramowania, które nie jest już obsługiwane przez producenta.	Dostawca może wykazać wdrożenie procedury zarządzania poprawkami, która spełnia to wymaganie i obejmuje co najmniej następujące elementy: ▪ Przypisanie ważności w celu określenia priorytetu. (Definicje ważności są udokumentowane). ▪ Udokumentowana procedura wdrażania poprawek awaryjnych. ▪ Sprawdzenie, czy nie są używane systemy operacyjne, dla których producent nie oferuje już pomocy technicznej. ▪ Dokumentację zarządzania poprawkami, która zawiera zatwierdzenia i wyjątki.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
43	Zainstalowanie oprogramowania antywirusowego i oprogramowania chroniącego przed złośliwym kodem w przypadku całego sprzętu podłączonego do sieci, używanego do Przetwarzania Danych osobowych oraz Danych poufnych firmy Microsoft, w tym serwerów czy komputerów produkcyjnych i szkoleniowych, w celu zapewnienia ochrony przed potencjalnie szkodliwymi wirusami i złośliwymi aplikacjami. Aktualizowanie definicji oprogramowania antywirusowego i oprogramowania chroniącego przed złośliwym kodem co najmniej raz dziennie lub zgodnie z zaleceniami dostawcy tego oprogramowania. Uwaga: Dotyczy to wszystkich systemów operacyjnych, w tym systemu Linux.	Istnieje dokumentacja wykazująca aktywne stosowanie oprogramowania antywirusowego i oprogramowania chroniącego przed złośliwym kodem. Uwaga: To wymaganie dotyczy wszystkich systemów operacyjnych.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
44	Dostawcy tworzący oprogramowanie dla firmy Microsoft muszą stosować w procesie tworzenia zasady „uwzględnienia bezpieczeństwa w fazie projektowania”.	Dokumenty specyfikacji technicznej dostawcy obejmują punkty kontrolne sprawdzania bezpieczeństwa w ramach cykli tworzenia.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
45	Wdrożenie programu Ochrony przed utratą danych („**DLP**"). Dane muszą zostać prawidłowo sklasyfikowane, oznaczone i chronione, a dostawca musi monitorować używane systemy informacyjne służące do Przetwarzania Danych osobowych lub Danych poufnych firmy Microsoft pod kątem nieuprawnionego dostępu, utraty i innych nieautoryzowanych działań. Program DLP ma następujące wymagania minimalne: ▪ użycie zgodnych ze standardem branżowym hostowanych, sieciowych i chmurowych systemów wykrywania nieuprawnionego dostępu („**IDS**", Intrusion Detection Systems), jeżeli przechowywane są Dane osobowe lub Dane poufne firmy Microsoft; ▪ wdrożenie zaawansowanych systemów ochrony przed nieuprawnionym dostępem („**IPS**", Intrusion Protection Systems) skonfigurowanych pod kątem monitorowania i aktywnego zapobiegania utracie danych; ▪ w przypadku nieuprawnionego dostępu analizowanie systemu w celu eliminacji również pozostałych luk w zabezpieczeniach; ▪ opisanie wymaganych procedur systemu monitorowania narzędzi do wykrywania nieuprawnionego dostępu oraz ▪ określenie procesu reagowania na incydenty i zarządzania nimi, który należy wykonać po wykryciu Naruszeń ochrony danych.	Udokumentowane wdrożenie systemu IDS/IPS z procedurami kierowania działaniami po wykryciu luki w zabezpieczeniach lub Naruszenia ochrony danych.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
46	Niezwłoczne powiadamianie kierownictwa wyższego szczebla i firmy Microsoft o wynikach dochodzenia przez zespół reagowania na incydenty. *Aby poinformować firmę Microsoft, należy skorzystać z adresu SSPAHelp@microsoft.com.*	Muszą być stosowane systemy i procedury powiadamiania firmy Microsoft o wynikach dochodzenia prowadzonego przez zespół reagowania na incydenty.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
47	Administratorzy systemów, personel operacyjny, kierownictwo i strony trzecie muszą brać udział w corocznym szkoleniu w zakresie zabezpieczeń.	Opracowanie programu szkoleń w zakresie zabezpieczeń, który uwzględnia: ▪ coroczne szkolenie dla zespołu reagowania na incydenty oraz ▪ symulowane zdarzenia i automatyczne mechanizmy umożliwiające efektywne reagowanie w sytuacjach kryzysowych. Informowanie o metodach zapobiegania incydentom (np. eliminacji ryzyka związanego z pobieraniem złośliwego oprogramowania).	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
48	Dostawca musi zagwarantować, że procesy planowania wykonywania kopii zapasowych zapewniają ochronę Danych osobowych oraz Danych poufnych firmy Microsoft przed nieautoryzowanym użyciem, dostępem, ujawnieniem, modyfikacją i zniszczeniem.	Dostawca może wykazać udokumentowanie procedur reagowania i odzyskiwania z uwzględnieniem szczegółowego opisu zarządzania przez organizację po wystąpieniu destrukcyjnego zdarzenia i metod utrzymania wstępnie określonego poziomu bezpieczeństwa informacji organizacji zgodnie z wymaganiami dotyczącymi ciągłości ochrony, określonymi przez kierownictwo. Dostawca może wykazać zdefiniowanie i wdrożenie procedur umożliwiających okresowe wykonywanie kopii zapasowych, bezpieczne przechowywanie i efektywne odzyskiwanie danych o znaczeniu krytycznym.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
49	Opracowanie i przetestowanie planów zapewnienia ciągłości działalności biznesowej i odzyskiwania awaryjnego.	Plan odzyskiwania awaryjnego musi obejmować wszystkie poniższe elementy: ▪ Zdefiniowane kryteria ustalania, czy system ma kluczowe znaczenie dla funkcjonowania firmy dostawcy. ▪ Listę systemów o kluczowym znaczeniu, ustaloną zgodnie ze zdefiniowanymi kryteriami, które należy odzyskać po wystąpieniu awarii. ▪ Zdefiniowaną procedurę awaryjnego odzyskiwania poszczególnych systemów o kluczowym znaczeniu, umożliwiającą odzyskanie aplikacji przed upływem 72 godzin przez inżyniera, który nie zna systemu. ▪ Coroczne (lub wykonywane częściej) testy i przeglądy planów odzyskiwania awaryjnego w celu zapewnienia realizacji celów odzyskiwania.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
50	Uwierzytelnianie tożsamości osoby przed udzieleniem jej dostępu do Danych osobowych lub Danych poufnych firmy Microsoft.	Zagwarantowanie, że identyfikatory użytkowników są unikatowe i powiązane z metodami uwierzytelniania zgodnymi ze standardami branżowymi, takimi jak usługa Azure Active Directory. Przed rozszerzeniem zakresu dostępu (przyznaniem uprawnień administracyjnych lub innego podwyższonego poziomu uprawnień) powinien być wymagany drugi składnik uwierzytelnienia, taki jak karta inteligentna lub uwierzytelnienie oparte na telefonie.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
51	Dostawca musi chronić Dane osobowe oraz Dane poufne firmy Microsoft przesyłane w sieciach, szyfrując je przy użyciu protokołu TLS („**Transport Layer Security**”) lub IPsec („**Internet Protocol Security**”). Te metody opisano w dokumentacji NIST 800-52 i NIST 800-57. Można stosować inny równoważny standard branżowy. Dostawca musi odmawiać przesyłania Danych osobowych lub Danych poufnych firmy Microsoft nieszyfrowanymi kanałami.	Należy zdefiniować i wdrożyć proces tworzenia, stosowania i wymiany certyfikatów TLS lub innych.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
52	Wszystkie urządzenia dostawcy (laptopy, stacje robocze itp.), uzyskujące dostęp do Danych osobowych lub Danych poufnych firmy Microsoft albo przetwarzające te dane, muszą stosować szyfrowanie dysków.	Należy szyfrować wszystkie urządzenia, używane do przetwarzania Danych osobowych lub Danych poufnych firmy Microsoft, przy użyciu funkcji Bitlocker lub innej równoważnej metody szyfrowania dysków.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
53	Stosowanie systemów i procedur (zgodnie z bieżącymi standardami branżowymi, takimi jak NIST 800-111) do szyfrowania magazynowanych (przechowywanych) Danych osobowych i/lub Danych poufnych firmy Microsoft, obejmujących: ▪ poświadczenia (np. nazwę użytkownika/hasło); ▪ dane instrumentów płatniczych (np. numery kart kredytowych i kont bankowych); ▪ dane osobowe dotyczące imigracji; ▪ dane profilów medycznych (np. numery kartoteki medycznej albo markery lub identyfikatory biometryczne, takie jak DNA, odciski palców, siatkówki i tęczówki oka, wzorce głosu, wzorce twarzy i wymiary dłoni używane w celu uwierzytelniania); ▪ numery identyfikacyjne nadane przez administrację państwową (np. numery PESEL lub numery prawa jazdy); ▪ dane należące do klientów firmy Microsoft (np. korzystających z usługi SharePoint, dokumentów usługi O365, usługi OneDrive); ▪ materiały dotyczące nieogłoszonych produktów firmy Microsoft; ▪ datę urodzenia; ▪ informacje o profilu dzieci; ▪ dane geograficzne dostępne w czasie rzeczywistym; ▪ adres zamieszkania (niesłużbowy); ▪ prywatne (niesłużbowe) numery telefonów; ▪ wyznanie; ▪ poglądy polityczne; ▪ orientację seksualną / preferencje seksualne; ▪ odpowiedzi na pytania zabezpieczające (np. uwierzytelnianie dwuskładnikowe, resetowanie hasła): o nazwisko panieńskie matki.	Należy sprawdzić, czy Dane osobowe i Dane poufne firmy Microsoft podane w tym wierszu są szyfrowane podczas magazynowania.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
54	W przypadku przetwarzania kart kredytowych w imieniu firmy Microsoft postępowanie zgodnie ze standardami określonymi przez wydawcę karty.	Coroczne potwierdzanie zgodności przez przedstawienie certyfikatu „**PCI-DSS**” (Payment Card Industry Data Services Standard). *Certyfikaty PCI DSS należy przesyłać do zespołu programu SSPA. W przypadku pytań*	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*

		należy skorzystać z adresu SSPAHelp@microsoft.com.	

Nr	Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców	Dowód zgodności	Odpowiedź
	Część J: Bezpieczeństwo (cd.)		
55	Dostawca musi przechowywać zasoby fizyczne firmy Microsoft w środowisku z kontrolowanym dostępem.	Muszą być stosowane systemy i procedury zarządzania fizycznym dostępem do cyfrowych, drukowanych, archiwalnych i zapasowych kopii danych firmy Microsoft. Przenoszenie odpowiedzialności musi być monitorowane podczas przekazywania i niszczenia nośników fizycznych zawierających dane firmy Microsoft.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*
56	Zapewnienie anonimowości wszystkich Danych osobowych firmy Microsoft używanych w środowisku projektowym lub testowym.	Nie należy wykorzystywać Danych osobowych firmy Microsoft w środowiskach projektowych ani testowych. W przeciwnym wypadku należy zapewnić ich anonimowość w celu uniemożliwienia identyfikacji Osób, których dane dotyczą, lub niewłaściwego użycia Danych osobowych. Uwaga: Dane zanonimizowane różnią się od danych pseudonimizowanych. Dane zanonimizowane to informacje, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, a osoby, której dane osobowe dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować.	*<Spełnione>* *<Niespełnione>* *<Nie ma zastosowania>* *<Konflikt prawny>* *<Konflikt umów>*