Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft

Zakres zastosowania

Wymagania firmy Microsoft dotyczące ochrony danych przez dostawców („**DPR**”) obowiązują każdego dostawcę firmy Microsoft, który przetwarza dane osobowe lub dane poufne firmy Microsoft w związku z wykonywaniem swoich zobowiązań (takich jak dostarczanie usług, licencji oprogramowania, usług w chmurze) na podstawie warunków jego umowy z firmą Microsoft (np. warunków zamówienia zakupu lub umowy ramowej) (zwanych dalej „**Wykonaniem zobowiązań**”).

- W przypadku konfliktu między DPR a wymaganiami określonymi w umowach zawartych między dostawcą a Microsoft, DPR będą mieć moc wiążącą, chyba że dostawca wskaże na prawidłowe postanowienie w umowie, które zastąpi obowiązujący wymóg ochrony danych (w takim przypadku wiążące będą warunki umowy).
- W przypadku konfliktu między wymaganiami zawartymi w niniejszym dokumencie a jakimikolwiek wymaganiami prawnymi lub ustawowymi, wymagania prawne lub ustawowe będą miały moc wiążącą.
- Jeżeli dostawca firmy Microsoft działa jako Administrator danych osobowych, to mogą obowiązywać go obniżone wymogi DPR.
- W przypadku, gdy dostawca Microsoft nie przetwarza danych osobowych Microsoft, a jedynie dane poufne w odniesieniu do niniejszego DPR, mogą go obowiązywać obniżone wymagania.

Międzynarodowe transfery 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 zapewni zgodność z Wymaganiami dotyczącymi ochrony danych, łącznie ze Standardowymi klauzulami umownymi, lub, według uznania firmy Microsoft, innymi odpowiednimi mechanizmami międzynarodowego przekazywania danych zatwierdzonymi przez odpowiedni organ ochrony danych lub Komisję Europejską, w zależności od przypadku, i przyjętymi lub uzgodnionymi przez firmę Microsoft. Standardowe klauzule umowne zastępujące obecne, przyjęte przez (i) Komisję Europejską lub przyjęte przez Europejskiego Inspektora Ochrony Danych i zatwierdzone przez Komisję Europejską, (ii) Wielką Brytanię zgodnie z brytyjską ogólną federalną ustawą o ochronie danych, (iii) Szwajcarię zgodnie ze szwajcarską federalną ustawą o ochronie danych oraz (iv) klauzule regulujące międzynarodowe przekazywanie danych osobowych oficjalnie przyjęte przez rząd w innej jurysdykcji niż Szwajcaria, Wielka Brytania oraz jurysdykcjach obejmujących Unię Europejską/Europejski Obszar Gospodarczy, zostaną włączone do niniejszego dokumentu i będą wiążące dla dostawcy z dniem ich przyjęcia. Dostawca zagwarantuje również, że wszyscy podwykonawcy (określeni w standardowych klauzulach umownych) będą również przestrzegać wymagań DPR.

Główne definicje

Pojęcia użyte w niniejszym DPR mają następujące znaczenie. Lista przykładów następujących po słowach „w tym”, „takich jak”, „np.”, „na przykład” lub tym podobnych, stosowanych w całym niniejszym DPR, jest interpretowana jako obejmująca wyrażenia takie jak „bez ograniczeń” lub „ale nie tylko”, chyba że są one wyrażone słowami takimi jak „tylko” lub „wyłącznie”. Więcej definicji znajduje się w Słowniku pojęć na końcu niniejszego dokumentu.

„**Administrator danych**” - podmiot, który określa cele i sposoby przetwarzania danych osobowych. „Administrator” obejmuje firmę, administratora (zgodnie z definicją tego terminu w RODO) oraz równoważne terminy zawarte w przepisach o ochronie danych, w zależności od kontekstu.
Pliki **„Cookie”** to małe pliki tekstowe przechowywane na urządzeniach przez strony internetowe lub aplikacje, które zawierają informacje służące do rozpoznawania posiadacza danych lub urządzenia.

„Naruszenie ochrony danych” oznacza (1) naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieautoryzowanego ujawnienia lub dostępu do danych osobowych lub danych poufnych firmy Microsoft przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Dostawcę lub jego podwykonawców, lub (2) wystąpienie luki w zabezpieczeniach związanej z postępowaniem przez dostawcę z danymi osobowymi lub danymi poufnymi firmy Microsoft.

“**Posiadacz danych**” oznacza możliwą do zidentyfikowania osobę fizyczną, którą można zidentyfikować bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy, lub na podstawie jednego lub kilku szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

„Prawo posiadacza danych” oznacza prawo posiadacza danych do uzyskania dostępu, usunięcia, edycji, eksportu, ograniczenia lub wniesienia sprzeciwu wobec przetwarzania danych osobowych posiadacza danych przez Microsoft, jeżeli jest to wymagane przez obowiązujące prawo.

„**Prawo**” oznacza wszystkie stosowne przepisy, zasady, statuty, dekrety, decyzje, rozporządzenia, orzeczenia, kodeksy, akty, uchwały i wymagania dowolnego organu rządowego (federalnego, stanowego, lokalnego lub międzynarodowego) posiadającego właściwość sądowniczą. **„Niezgodne z prawem**” oznacza każde naruszenie obowiązującego prawa.

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

„Dane osobowe firmy Microsoft” oznaczają wszelkie dane osobowe przetwarzane przez firmę Microsoft lub w jej imieniu.

„Dane osobowe” oznaczają wszelkie informacje odnoszące się do posiadacza danych oraz wszelkie inne informacje, które zgodnie z prawem stanowią „dane osobowe”.

„Przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub danych poufnych firmy Microsoft w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, rejestrowanie, 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.

„Podmiot przetwarzający” oznacza podmiot, który przetwarza dane osobowe w imieniu innego podmiotu i obejmuje dostawcę usług, podmiot przetwarzający (zgodnie z definicją tego terminu w RODO) oraz równoważne terminy znajdujące się w przepisach o ochronie danych, w zależności od kontekstu.

„Podwykonawca” oznacza stronę trzecią, której dostawca przekazuje swoje zobowiązania w związku z umową określającą ich wykonywanie, w tym podmiot powiązany z dostawcą, który nie zawiera umów bezpośrednio z firmą Microsoft.

„Podrzędny podmiot przetwarzający” oznacza stronę trzecią, której firma Microsoft zleciła wykonanie zobowiązań, przy czym wykonywanie zobowiązań obejmuje przetwarzanie danych osobowych firmy Microsoft, w odniesieniu do których firma Microsoft jest podmiotem przetwarzającym.

Odpowiedź dostawcy

Dostawcy co roku potwierdzają zgodność z tymi wymaganiami, korzystając z usługi online administrowanej przez firmę Microsoft. Prosimy zapoznać się z Przewodnikiem po programie SSPA, aby dowiedzieć się, jak zarządza się zgodnością z wymaganiami w Microsoft.

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	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 w odniesieniu do danych poufnych i danych osobowych firmy Microsoft, w tym zakaz sprzedaży danych osobowych firmy Microsoft oraz przetwarzania danych osobowych firmy Microsoft poza bezpośrednimi relacjami biznesowymi między firmą Microsoft a dostawcą. W przypadku firm pełniących funkcję podmiotów przetwarzających lub podrzędnych podmiotów przetwarzających, w związku z wykonywaniem zobowiązań w odniesieniu do danych osobowych firmy Microsoft, umowa musi obejmować przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych firmy Microsoft, kategorie posiadaczy danych oraz obowiązki i prawa firmy Microsoft.	Dostawca musi przedstawić odpowiednią umowę zawartą z Microsoft. W przypadku podmiotów przetwarzających i podrzędnych podmiotów przetwarzających opisy przetwarzania są zawarte w odpowiedniej umowie (*np*. w wykazie zakresu prac lub w zamówieniach zakupu). Uwaga: W przypadku firm z zamówieniami zakupu w toku odpowiedni opis działań dotyczących przetwarzania może zostać dodany później podczas dokonywania zakupów.
2	W przypadku, gdy firma Microsoft potwierdzi, że dana osoba została zatrudniona jako podrzędny podmiot przetwarzający, dostawca powinien zawrzeć stosowne umowy o ochronie danych osobowych z firmą Microsoft. Uwaga: Microsoft zamieści informację o wyznaczeniu takiej osoby jako podrzędnego podmiotu przetwarzającego w jej profilu w stosownym czasie.	Standardowe klauzule umowne, aneks dotyczący danych klienta online oraz aneks dotyczący przetwarzania danych przy świadczeniu profesjonalnych usług przez dostawców i partnerów.
3	Wyznaczenie osoby lub grupy osób w firmie, która będzie ponosić odpowiedzialność za zapewnienie zgodności z wymaganiami DPR.	Należy podać stanowisko osoby lub grupy odpowiedzialnej za zapewnienie, że dostawca przestrzega wymagań DPR. Dokument opisujący uprawnienia i obowiązki tej osoby lub grupy, której rolą jest zapewnienie bezpieczeństwa i ochrony danych osobowych.

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	Część A: Zarządzanie (ciąg dalszy)	
4	Opracowanie, utrzymywanie i przeprowadzanie corocznych szkoleń w zakresie ochrony danych osobowych i bezpieczeństwa dla pracowników, którzy będą mieli dostęp do danych osobowych przetwarzanych przez dostawcę w związku z wykonywaniem zobowiązań lub przetwarzaniem danych poufnych firmy Microsoft. Jeżeli firma nie ma przygotowanych materiałów, może skorzystać z tego konspektu scenorysu i dostosować go do wymogów firmy dostawcy. Uwaga: Personel dostawcy może być zobowiązany do ukończenia dodatkowych szkoleń prowadzonych przez oddziały firmy Microsoft.	Roczne rejestry obecności są dostępne i mogą być udostępnione firmie Microsoft na jej prośbę. Treść szkoleniowa obejmuje zasady bezpieczeństwa i ochrony danych osobowych. Dokumentacja zgodności z wymaganiami dotyczącymi szkoleń będzie zawierała dowody przeprowadzenia szkoleń związanych z wymogami prawnymi w zakresie ochrony danych osobowych, zobowiązaniami w zakresie bezpieczeństwa oraz obowiązującymi wymogami i zobowiązaniami umownymi.
5	Przetwarzanie danych osobowych firmy Microsoft tylko zgodnie z udokumentowanymi instrukcjami firmy Microsoft dotyczącymi na przykład scenariuszy 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 lub podrzędny podmiot przetwarzający (dostawca) poinformuje administratora (firmę Microsoft) o takim wymogu prawnym przed takim przetwarzaniem, jeżeli te przepisy prawa nie zabraniają ujawniania tych informacji ze względu na ważny interes publiczny).	Dostawca sporządza i przechowuje wszystkie udokumentowane instrukcje firmy Microsoft (np. umowę, wykaz prac lub zamówienie zakupu) w formie elektronicznej, w lokalizacji łatwo dostępnej dla jego pracowników i wykonawców uczestniczących w wykonywaniu zobowiązań.
	Część B: Powiadomienie	
6	Dostawca jest zobowiązany do stosowania zasad ochrony danych osobowych firmy Microsoft w przypadku zbierania danych osobowych jej imieniu. Zasady ochrony danych osobowych powinny być zrozumiałe i dostępne dla posiadaczy takich danych, aby ułatwiać im podjęcie decyzji o przesłaniu ich danych osobowych do dostawcy. Uwaga: Jeżeli firma jest administratorem zajmującym się przetwarzaniem danych osobowych, to powinna opublikować własne zasady ochrony takich danych.	Dostawca wykorzystuje fwdlink, aby uzyskać dostęp do aktualnych, opublikowanych zasad ochrony danych osobowych Microsoft. Zasady ochrony danych osobowych są publikowane w każdym kontekście, w którym będą zbierane dane osobowe użytkownika. W razie potrzeby zostanie udostępniona ich wersja offline przed zebraniem danych osobowych. Zasady ochrony danych osobowych w wersji offline to

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
		najnowsza opublikowana wersja z odpowiednią datą. W przypadku usług dla pracowników firmy Microsoft stosowane są zasady ochrony danych osobowych firmy Microsoft.
7	Dostawcy zbierający dane osobowe firmy Microsoft podczas rozmów telefonicznych lub na podstawie nagranych rozmów telefonicznych powinni być przygotowani do omówienia z posiadaczami danych zasad zbierania, przetwarzania, wykorzystywania i przechowywania ich danych osobowych.	Skrypt nagrań głosowych opisuje, w jaki sposób dane osobowe firmy Microsoft są przetwarzane i obejmuje: ▪ zbieranie ▪ wykorzystywanie ▪ przechowywanie
	Część C: Wybór i zgoda	
8	W odpowiednich przypadkach dostawca powinien uzyskać i zarejestrować zgodę posiadacza danych na wszystkie swoje działania dotyczące przetwarzania (w tym nowe i zaktualizowane działania dotyczące przetwarzania) przed rozpoczęciem zbierania danych osobowych posiadacza danych. Dostawca monitoruje skuteczność zarządzania preferencjami, aby zapewnić, że czas na zmianę preferencji jest zgodny z najbardziej restrykcyjnymi obowiązującymi wymaganiami prawnymi.	Dostawca może wykazać, w jaki sposób posiadacz danych może udzielić zgodę na przetwarzanie, a zakres zgody obejmuje wszystkie działania dostawcy dotyczące przetwarzania w odniesieniu do danych osobowych posiadacza danych. Dostawca może wykazać, w jaki sposób posiadacz danych może wycofać zgodę na działania dotyczące przetwarzania. Dostawca może wykazać, w jaki sposób sprawdzane są preferencje przed rozpoczęciem nowych czynności przetwarzania. Uwaga: Dowodem mogą być zrzuty ekranu interakcji użytkownika, eksperymenty z usługą lub możliwość wyświetlenia dokumentacji technicznej.
9	Dostawcy tworzący i zarządzający witrynami internetowymi i/lub aplikacjami albo stronami, na których widnieje marka Microsoft powinni przekazać posiadaczom danych wyraźne powiadomienie i możliwość wyboru opcji korzystania z plików cookie zgodnie ze swoimi zobowiązaniami zawartymi w zasadach ochrony danych osobowych Microsoft i miejscowymi wymogami prawnymi. O ile zawierająca umowę jednostka biznesowa nie zwróci się z odpowiednim żądaniem, do zarządzania kontrolą wyboru dostawcy powinni stosować standardowy baner wyprodukowany przez zespół 1ES.	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, nie mogą mieć one 13-miesięcznej daty ważności od momentu odwiedzenia witryny przez użytkownika. Sprawdzenie zgodności z obowiązującym Prawem EU, np.: ▪ użycie konwencji oznaczania „Ochrona danych osobowych i pliki cookie” w odniesieniu do zasad ochrony danych osobowych,

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	Wymóg ten obowiązuje, gdy witryny są skierowane do użytkowników znajdujących się w Unii Europejskiej lub na Europejskim Obszarze Gospodarczym i innych regionach, w których obowiązują przepisy dotyczące ochrony danych osobowych, oraz wszędzie tam, gdzie jest używane oświadczenie firmy Microsoft o ochronie danych osobowych. Uwaga: Sponsorzy biznesowi firmy Microsoft są zobowiązani do zarejestrowania witryn firmy Microsoft w wewnętrznym portalu zgodności w sieci na stronie (http://aka.ms/wcp) w celu skatalogowania i zarządzania spisem plików cookie.	▪ zapewnienie uzyskania zgody od użytkownika przed użyciem plików cookie do celów innych niż niezbędne, takich jak reklamowe, oraz ▪ wygaśnięcie zgody lub jej ponownie uzyskanie nie rzadziej niż raz na 6 miesięcy.
	Część D: Zbieranie	
10	Dostawca powinien monitorować zbieranie danych osobowych lub danych poufnych firmy Microsoft w celu zapewnienia, 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. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
11	Przed zebraniem danych od dzieci (zgodnie z definicją obowiązującą w jurysdykcji sądowej) dostawca powinien uzyskać na to zgodę zgodnie z lokalnymi przepisami dotyczącymi ochrony danych osobowych.	Dostawca może przekazać dokumentację wykazującą zgodę rodzica lub opiekuna. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
	Część E: Przechowywanie	
12	Zagwarantowanie, że dane osobowe i dane poufne firmy Microsoft nie są przechowywanie dłużej niż jest to wymagane do wykonania zobowiązań, chyba że dalsze przechowywanie danych osobowych 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). Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
13	Zapewnienie, że według wyłącznego uznania firmy Microsoft dane osobowe i poufne firmy Microsoft będące w posiadaniu dostawcy lub pozostające pod jego kontrolą zostaną zwrócone firmie Microsoft lub zniszczone po zakończeniu wykonania zobowiązania lub na żądanie firmy Microsoft.	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 dostawcy.

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	Należy ustanowić w aplikacjach procesy gwarantujące bezpieczne usunięcie danych, gdy dane zostaną usunięte z aplikacji przez użytkownika lub po spełnieniu określonych warunków, takich jak określony czas przechowywania danych. Gdy konieczne będzie zniszczenie danych osobowych lub danych poufnych firmy Microsoft, dostawca powinien spalić, zetrzeć na proszek lub podrzeć zasoby fizyczne zawierające dane osobowe i/lub dane poufne firmy Microsoft w sposób uniemożliwiający ich odczytanie lub odtworzenie.	
	Część F: Posiadacze danych	
	Posiadacze danych mają pewne prawa wynikające z przepisów prawa, takie jak prawo uzyskania dostępu, usunięcia, edycji, eksportu, ograniczenia lub wniesienia sprzeciwu wobec przetwarzania ich danych osobowych (**„Prawa posiadaczy danych”**). Gdy posiadacz danych egzekwuje swoje prawa dotyczące jego danych osobowych przetwarzanych w firmie Microsoft zgodnie z prawem, dostawca musi umożliwić firmie Microsoft wykonanie następujących czynności lub wykonać te czynności w imieniu firmy Microsoft:	
14	Wspierać firmę Microsoft przy użyciu odpowiednich środków technicznych i organizacyjnych w celu wywiązania się ze swoich zobowiązań dotyczących odpowiadania bez nieuzasadnionej zwłoki na żądania posiadaczy danych pragnących wyegzekwować swoje prawa. Jeżeli firma Microsoft nie zdecydowała inaczej, dostawca będzie kierować wszystkich posiadaczy danych, którzy bezpośrednio się z nim skontaktują, do firmy Microsoft w celu wyegzekwowania ich praw.	Dostawca będzie posiadał udokumentowany dowód stosowania procesów i procedur ułatwiających egzekwowanie praw posiadaczy danych. Dostawca będzie posiadał udokumentowany dowód na przeprowadzenie testów. Dowody będą udostępniane na prośbę firmy Microsoft.
15	Przesyłając odpowiedź bezpośrednio do posiadacza danych oraz w przypadku, gdy dostawca zapewnia samoobsługowy mechanizm online, dostawca będzie dysponować procesami i procedurami umożliwiającymi identyfikację posiadaczy danych zgłaszających żądanie.	Dostawca udokumentował metodę stosowaną do identyfikacji posiadaczy danych w firmie Microsoft. Dostawca dostarczy dokumentację dowodową firmie Microsoft na jej prośbę.

16	Na wniosek firmy Microsoft o zlokalizowanie danych osobowych dotyczących danego posiadacza takich danych w Microsoft, które nie są dostępne za pośrednictwem samoobsługowego mechanizmu online, dostawca podejmie uzasadnione starania w celu zlokalizowania żądanych danych i będzie prowadził rejestr potwierdzający przeprowadzenie wyszukiwania w tym zakresie.	Dostawca będzie posiadał udokumentowany dowód na stosowanie procedur w celu ustalenia, czy są przechowywane dane osobowe firmy Microsoft i przekaże go firmie Microsoft na jej prośbę. Dostawca prowadzi rejestr wykazujący działania podjęte w celu spełnienia żądań wynikających z praw posiadaczy danych. Dokumentacja zawiera: ▪ datę i godzinę żądania, ▪ działania podjęte w odpowiedzi na żądanie oraz informacje o tym, kiedy poinformowano firmę Microsoft. Dostawca dostarczy dokumentację dowodową firmie Microsoft na jej prośbę.
17	Dostawca będzie informować posiadaczy danych o wszystkich krokach, które powinni wykonać w celu uzyskania dostępu do swoich danych osobowych w firmie Microsoft lub egzekwowania w inny sposób swoich praw dotyczących tych danych.	Dostawca będzie posiadał udokumentowany dowód komunikacji oraz stosowania procedur dostępu do danych osobowych firmy Microsoft. Dostawca będzie posiadał udokumentowany dowód i dostarczy go firmie Microsoft na jej prośbę.
18	Rejestrować datę i godzinę zgłoszenia żądań dotyczących praw posiadaczy danych i działania podejmowane przez dostawcę w odpowiedzi na takie żądania. Przekazać posiadaczowi danych, którego żądanie zostało odrzucone na wniosek firmy Microsoft, pisemne wyjaśnienie. Udostępnić rejestr wniosków posiadaczy danych firmie Microsoft na jej prośbę.	Dostawca prowadzi rejestr żądań dostępu/usunięcia danych osobowych i dokumentuje zmiany wprowadzane do danych osobowych firmy Microsoft. Dostawca dokumentuje wypadki odrzucenia żądań i przechowuje dowody weryfikacji i zatwierdzenia przez firmę Microsoft. Dostawca przekaże dowód prowadzenia rejestru żądań i odmów dostępu do danych osobowych firmy Microsoft.
19	Dostawca powinien umożliwić firmie Microsoft lub uzyskać kopię żądanych danych osobowych Microsoft dla uwierzytelnionego posiadacza danych w odpowiednim formacie drukowanym, elektronicznym lub ustnym.	Dostawca przekaże dane osobowe Microsoft posiadaczowi danych w formie, która będzie zrozumiała i wygodna dla niego jak i dla dostawcy.
20	Dostawca powinien podjąć uzasadnione środki ostrożności, aby zapewnić, że dane osobowe udostępnione Microsoft lub uwierzytelnionemu posiadaczowi danych, nie będą mogły zostać wykorzystane do identyfikacji innej osoby.	Dostawca będzie posiadał udokumentowany dowód stosowania procedur związanych ze środkami ostrożności podejmowanymi w celu uniknięcia zidentyfikowania posiadacza danych, w sposób niezgodny z warunkami Umowy. Dostawca dostarczy dokumentację dowodową firmie Microsoft na jej prośbę.

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
21	Jeśli posiadacz danych uzna, że jego dane osobowe nie są kompletne i prawidłowe, dostawca powinien zgłosić ten problem do firmy Microsoft i współpracować z firmą Microsoft w celu rozwiązania go.	Dostawca dokumentuje przypadki braku zgody i przekazuje informację o tym do firmy Microsoft. Dostawca dostarczy dokumentację dowodową firmie Microsoft na jej prośbę.
	Część G: Podwykonawcy	
	Jeżeli dostawca zamierza skorzystać z pomocy podwykonawcy w związku z przetwarzaniem danych osobowych lub danych poufnych firmy Microsoft, powinien:	
22	Powiadomić Microsoft przed zleceniem usług podwykonawstwa lub wprowadzeniem jakichkolwiek zmian odnośnie dodania lub zastąpienia podwykonawców. Uwaga: dostawca powinien przyjąć to zobowiązanie, nawet jeśli obecnie nie zatrudnia żadnych podwykonawców, ale może zatrudniać ich w przyszłości.	Sprawdzenie, czy dane osobowe firmy Microsoft są przetwarzane wyłącznie przez firmy znane firmie Microsoft zgodnie z wymaganiami odpowiednich umów (np. wykazem zakresu prac, załącznikiem, zleceniem zakupu) lub zarejestrowane w bazie danych SSPA. Dostawca może opublikować listę swoich podwykonawców online i zamieścić link do strony w bazie danych SSPA.
23	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. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
24	Jeśli firma Microsoft jest administratorem danych osobowych, należy zagwarantować, że podwykonawca wykorzystuje dane osobowe firmy Microsoft zgodnie z deklarowanymi przez posiadacza danych preferencjami dotyczącymi kontaktu z nim.	Wykazanie, w jaki sposób preferencje posiadacza danych są wykorzystywane przez podwykonawców. Udostępnienie dokumentacji dodatkowej (np. zrzutu ekranu, umowy SLA, SOW itp.) zawierającej okres uznawania zmiany preferencji przez podwykonawcę.
25	Ograniczyć przetwarzanie danych osobowych lub danych poufnych firmy Microsoft przez podwykonawców do celów niezbędnych do realizacji umowy dostawcy z firmą Microsoft.	Dostawca może udostępnić dokumentację wykazującą, że dane osobowe Microsoft przekazywane podwykonawcy są wymagane do wykonywania zobowiązań. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
26	Sprawdzać skargi wskazujące na nieautoryzowane lub	Dostawca może przedstawić systemy i procesy służące

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	niezgodne z prawem przetwarzanie danych osobowych firmy Microsoft.	do rozwiązywania skarg dotyczących nieupoważnionego wykorzystania lub ujawnienia danych osobowych firmy Microsoft przez podwykonawcę. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
27	Niezwłocznie powiadomić firmę Microsoft o wykryciu przetwarzania przez podwykonawcę danych osobowych lub danych poufnych firmy Microsoft do celu innego niż związanego z wykonywaniem zobowiązań.	Dostawca udostępnił instrukcje i środki umożliwiające podwykonawcy zgłaszanie niewłaściwego użycia danych firmy Microsoft. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
28	W przypadku, gdy dostawca zbiera dane osobowe od stron trzecich w imieniu Microsoft, powinien sprawdzić, czy zasady i praktyki ochrony danych stron trzecich są zgodne z umową dostawcy z Microsoft i DPR.	Dostawca może dostarczyć dokumentację dotyczącą przeprowadzonego badania due diligence w odniesieniu do polityk i praktyk ochrony danych osób trzecich. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
29	Niezwłocznie podjąć działania w celu złagodzenia wszelkich rzeczywistych lub potencjalnych szkód spowodowanych przez podwykonawcę w związku z nieautoryzowanym lub niezgodnym z prawem przetwarzaniem przez niego danych osobowych oraz poufnych Microsoft.	Dostawca powinien przechowywać dokumentację dowodową planu i procedury oraz na żądanie dostarczyć dowód takiej dokumentacji do firmy Microsoft.
	Część H: Jakość	
30	Dostawca powinien zapewnić integralność wszystkich danych osobowych firmy Microsoft, tak aby były one dokładne, kompletne i adekwatne oraz zgodnie z deklarowanym celem ich przetwarzania.	Dostawca może wykazać stosowanie procedur sprawdzania poprawności danych osobowych firmy Microsoft podczas ich zbierania, tworzenia i aktualizowania. Dostawca może wykazać stosowanie procedur monitorowania i pobierania próbek w celu weryfikowania dokładności danych na bieżąco oraz wprowadzania niezbędnych korekt. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
	Część I: Monitorowanie i egzekwowanie	

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
31	Dostawca stosuje plan reagowania na zdarzenia, który wymaga powiadomienia przez niego firmy Microsoft zgodnie z wymaganiami umownymi lub bez nieuzasadnionej zwłoki w zależności od tego, co nastąpi wcześniej, po uzyskaniu informacji o naruszeniu ochrony danych. Dostawca powinien, na prośbę lub polecenie firmy Microsoft, współpracować z firmą Microsoft przy dochodzeniu dotyczącym zdarzenia lub ograniczaniu/usuwaniu jego skutków, łącznie z udostępnieniem firmie Microsoft danych, informacji, dostępu do personelu dostawcy lub sprzętu niezbędnego do przeprowadzenia analizy kryminalistycznej. Uwaga: Dostawca powinien zapoznać się z Przewodnikiem po programie SSPA, aby dowiedzieć się, jak należy powiadomić firmę Microsoft o wystąpieniu zdarzenia.	Dostawca stosuje plan reagowania na zdarzenia obejmujący powiadomienie klientów (firmy Microsoft) zgodnie z opisem w tej części. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
32	Wdrożenie planu naprawy i monitorowanie rozwiązywania każdego naruszenia ochrony danych w celu zagwarantowania, że odpowiednie działania zaradcze są podejmowane na czas.	Dostawca posiada udokumentowane procedury, które podejmie w celu odpowiedzi na naruszenie ochrony danych i rozwiązania tego problemu. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.
33	Jeśli firma Microsoft jest administratorem swoich danych osobowych, należy ustanowić formalny proces obsługi skarg w celu rozpatrywania wszystkich skarg związanych z ochroną danych osobowych w Microsoft.	Dostawca stosuje środki przyjmowania skarg dotyczących danych osobowych firmy Microsoft i posiada udokumentowaną procedurę rozpatrywania takich skarg. Dostawca przekaże dokumentację dowodową firmie Microsoft na jej prośbę.

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	Część J: Bezpieczeństwo	
	Dostawca powinien stworzyć, wdrożyć i prowadzić program bezpieczeństwa informacji, który uwzględnia	Ważny certyfikat ISO 27001 jest dopuszczalnym zamiennikiem części J. Aby zastosować ten zamiennik,

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	zasady i procedury gwarantujące bezpieczeństwo i ochronę danych osobowych oraz danych poufnych firmy Microsoft, zgodnie z zalecanymi praktykami branżowymi i przepisami prawa. Program bezpieczeństwa wdrożony przez dostawcę powinien być zgodny z poniższymi standardami (wymagania 34–50).	należy skontaktować się z zespołem SSPA. Uwaga: Dostawca będzie musiał udostępnić taki certyfikat.
34	Wykonywanie corocznej oceny zabezpieczeń sieciowych, obejmującej następujące działania: ▪ przegląd najważniejszych zmian w środowisku, takich jak nowy składnik systemu, topologia sieci, reguły zapory; ▪ wyszukiwanie luk w zabezpieczeniach oraz ▪ prowadzenie dzienników zmian.	Dostawca udokumentował oceny sieci, dzienniki zmian i wyniki wyszukiwania luk w zabezpieczeniach. Wymagane dzienniki zmian muszą śledzić zmiany, zawierać informacje o przyczynie zmiany, a także imię i nazwisko oraz stanowisko wyznaczonej osoby zatwierdzającej.
35	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 wykaże, że stosuje zasady dotyczące urządzeń przenośnych w przypadku, gdy przetwarzanie danych osobowych lub poufnych danych osobowych Microsoft będzie wymagać użycia urządzenia przenośnego.
36	Wszystkie zasoby używane do wspomagania wykonywania zobowiązań powinny zostać zarejestrowane i posiadać właściciela możliwego do identyfikacji. Dostawca jest zobowiązany do prowadzenia wykazu tych zasobów informacyjnych, określenia dozwolonych i autoryzowanych metod ich użycia oraz zapewnienia odpowiedniego poziomu ich ochrony 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 handlowej oraz ▪ rejestr utylizacji nośników używanych do przechowywania danych, gdy nie będą już one potrzebne.
37	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, ▪ niezawodne parametry do wyboru poświadczeń używanych do uwierzytelniania oraz ▪ dezaktywację kont użytkowników w ciągu 48 godzin po zakończeniu zatrudnienia ▪ silne kontrole haseł, które wymuszają długość i

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
		złożoność hasła oraz zapobiegają ponownemu jego użyciu Dostawca wykazuje, że stworzył proces przeglądu dostępu użytkowników do danych osobowych oraz danych poufnych firmy Microsoft z uwzględnieniem zasady najniższego poziomu uprawnień. Proces powinien uwzględniać: ▪ wyraźnie zdefiniowane role użytkownika, ▪ procedury przeglądu i uzasadniania zezwalania na dostęp do ról oraz ▪ sprawdzanie, czy udokumentowano uzasadnienie przyłączenia do grup/ról użytkowników uprawnionych do dostępu do danych firmy Microsoft.
38	Zdefiniowanie i wdrożenie procedur zarządzania poprawkami, które przypisują wyższy priorytet poprawkom 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.
39	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 oraz 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.	Istnieje dokumentacja wykazująca aktywne stosowanie oprogramowania antywirusowego i oprogramowania chroniącego przed złośliwym kodem. Uwaga: To wymaganie dotyczy wszystkich systemów operacyjnych.

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	Uwaga: Dotyczy to wszystkich systemów operacyjnych, w tym systemu Linux.	
40	Dostawcy tworzący oprogramowanie dla firmy Microsoft muszą stosować w procesie tworzenia zasady „uwzględnienia bezpieczeństwa w fazie projektowania”.	Dokumenty specyfikacji technicznej dostawcy obejmują punkty kontrolne w celu sprawdzania bezpieczeństwa w ramach cykli tworzenia.
41	Wdrożenie programu Ochrony przed utratą danych („**DLP**”) w celu zapobiegania nieuprawnionemu dostępowi, utracie danych i innym nieautoryzowanym działaniom. Dane powinny zostać prawidłowo sklasyfikowane, oznaczone i chronione, a dostawca powinien 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; ▪ określenie procesu reagowania na zdarzenia i zarządzania nimi, który należy wykonać po wykryciu naruszeń ochrony danych ▪ komunikacja (ze wszystkimi pracownikami i podwykonawcami dostawcy, którzy zostali wyłączeni z wykonywania zobowiązań przez dostawcę) w	Udokumentowane wdrożenie programu DLP z procedurami zapobiegania nieautoryzowanemu dostępowi, utracie i innym nieautoryzowanym działaniom (i spełniającego wymagania minimalne w zakresie wszystkich elementów określonych w tym punkcie).

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	zakresie nieautoryzowanego pobierania i wykorzystywania danych osobowych lub danych poufnych firmy Microsoft.	
	Część J: Bezpieczeństwo (ciąg dalszy)	
42	Niezwłoczne powiadamianie kierownictwa wyższego szczebla i firmy Microsoft o wynikach dochodzenia przez zespół reagowania na incydenty.	Powinny być stosowane systemy i procedury powiadamiania firmy Microsoft o wynikach dochodzenia prowadzonego przez zespół reagowania na zdarzenia.
43	Administratorzy systemów, personel operacyjny, kierownictwo i strony trzecie powinni brać udział w corocznym szkoleniu z zakresu zabezpieczeń.	Opracowanie programu szkoleń w zakresie zabezpieczeń, który uwzględnia: ▪ coroczne szkolenie dla zespołu reagowania na zdarzenia oraz ▪ symulowane zdarzenia i automatyczne mechanizmy umożliwiające efektywne reagowanie w sytuacjach kryzysowych. ▪ Informowanie o metodach zapobiegania zdarzeniom (np. eliminacji ryzyka związanego z pobieraniem złośliwego oprogramowania).
44	Dostawca powinien 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 udokumentowane procedury reagowania i odzyskiwania, szczegółowo opisujące, w jaki sposób organizacja będzie zarządzać zdarzeniem zakłócającym i utrzyma bezpieczeństwo informacji na z góry określonym poziomie w oparciu o zatwierdzone przez kierownictwo cele ciągłości bezpieczeństwa informacji. Dostawca może wykazać zdefiniowanie i wdrożenie procedur umożliwiających okresowe wykonywanie kopii zapasowych, bezpieczne przechowywanie i efektywne odzyskiwanie danych o znaczeniu krytycznym.
45	Opracowanie i przetestowanie planów zapewnienia ciągłości działalności biznesowej i odzyskiwania awaryjnego.	Plan odzyskiwania awaryjnego powinien obejmować: ▪ Zdefiniowane kryteria w celu ustalenia, 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,

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
		umożliwiającą odzyskanie aplikacji przed upływem 72 godzin przez inżyniera, który nie zna systemu. ▪ Coroczne (lub przeprowadzane częściej) testy i przeglądy planów odzyskiwania awaryjnego w celu zapewnienia realizacji celów takiego odzyskiwania.
	Część J: Bezpieczeństwo (ciąg dalszy)	
46	Uwierzytelnianie tożsamości osoby przed udzieleniem jej dostępu do danych osobowych lub danych poufnych firmy Microsoft oraz zapewnienie, że dostęp jest ograniczony do zakresu działalności danej osoby dozwolonego w celu wykonywania zobowiązań.	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 uwierzytelnianie oparte na telefonie. Udokumentowany program bezpieczeństwa informacji obejmujący proces zapewniający, że dostęp wszystkich pracowników i podwykonawców dostawcy do danych osobowych lub danych poufnych firmy Microsoft nie jest większy ani dłuższy niż konieczny w celu wykonywania zobowiązań.
47	Dostawca musi chronić wszystkie dane przetwarzane w związku z wykonywaniem swoich zobowiązań, które są 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 również inny równoważny standard branżowy. Dostawca powinien nie zgadzać się na przesyłanie danych osobowych lub danych poufnych firmy Microsoft nieszyfrowanymi kanałami.	Należy zdefiniować i egzekwować proces tworzenia, stosowania i wymiany certyfikatów TLS lub innych.
48	Wszystkie urządzenia dostawcy (laptopy, stacje robocze itp.), uzyskujące dostęp do danych osobowych lub danych poufnych firmy Microsoft albo przetwarzające te dane, powinny 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.

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
	Część J: Bezpieczeństwo (ciąg dalszy)	
49	Stosowanie systemów i procedur (zgodnie z bieżącymi standardami branżowymi, takimi jak opisane w **NIST 800-111**) do szyfrowania magazynowanych (przechowywanych) danych osobowych oraz danych poufnych firmy Microsoft, obejmujących: ▪ dane uwierzytelniające (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 oznaczenia 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 lub usługi OneDrive); ▪ materiały dotyczące nieogłoszonych produktów firmy Microsoft; ▪ data 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); ▪ nazwisko panieńskie matki	Należy sprawdzić, czy dane osobowe i dane poufne firmy Microsoft są szyfrowane podczas magazynowania.
50	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 posiadaczy danych osobowych lub niewłaściwego użycia ich danych.

#	Wymagania dotyczące ochrony danych osobowych przez dostawców Microsoft	Dowód zgodności
		Uwaga: Dane zanonimizowane różnią się od danych pseudonimizowanych. Dane zanonimizowane to informacje, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, gdzie nie można zidentyfikować lub nie można już zidentyfikować posiadacza danych osobowych.

Słownik pojęć

„Upoważniony przedstawiciel” to osoba posiadająca odpowiednie uprawnienia do podpisywania umów w imieniu firmy. Osoba ta posiada wymaganą wiedzę na temat bezpieczeństwa i ochrony danych osobowych lub konsultuje się z ekspertem przed złożeniem odpowiedzi na działanie programu SSPA. Ponadto, poprzez dodanie swojego imienia i nazwiska do formularza SSPA, zaświadcza, że zapoznała się z wymaganiami DPR.

„EUDPR” oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii Europejskiej i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE.

„Freelancer” oznacza osoby wykonujące zadania lub usługi na żądanie, które są zamawiane za pośrednictwem platform cyfrowych lub w inny sposób.

„RODO” oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

„Wymagania dotyczące ochrony danych osobowych” oznaczają rozporządzenia RODO, EUDPR, lokalne prawa UE/EOG w dziedzinie ochrony danych, kalifornijską ustawę o ochronie danych osobowych konsumentów, Kodeks Cywilny Stanu

Kalifornia § 1798.100 i nast. (CCPA — California Consumer Privacy Act), brytyjską ustawę o ochronie danych osobowych z 2018 roku (UK Data Protection Act) oraz wszelkie powiązane lub późniejsze prawa, rozporządzenia i inne wymagania prawne obowiązujące w Wielkiej Brytanii, a także wszelkie obowiązujące prawa, rozporządzenia i inne wymagania prawne odnoszące się do (a) ochrony i bezpieczeństwa danych osobowych; lub (b) wykorzystywania, zbierania, zatrzymywania, przechowywania, zabezpieczania, ujawniania, przekazywania, usuwania i innego przetwarzania danych osobowych.

„Wzorcowe klauzule UE" oraz „Standardowe klauzule umowne" oznaczają (i) standardowe klauzule ochrony danych dotyczące przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w państwach trzecich, które nie zapewniają odpowiedniego poziomu ochrony danych, jak opisano w art. 46 RODO i zatwierdzono decyzją Komisji Europejskiej (UE) nr 2021/914/WE z dnia 4 czerwca 2021 r.; (ii) wszelkie klauzule zastępujące obecne, przyjęte przez (a) Komisję Europejską (b) Europejskiego Inspektora Ochrony Danych i zatwierdzone przez Komisję Europejską (c) Wielką Brytanię zgodnie z brytyjską ogólną federalną ustawą o ochronie danych, (d) Szwajcarię zgodnie ze szwajcarską federalną ustawą o ochronie danych lub (e) przez rząd w jurysdykcji innej niż Szwajcaria, Wielka Brytania oraz jurysdykcje obejmujące Unię Europejską / Europejski Obszar Gospodarczy, w których klauzule regulujące międzynarodowe przekazywanie danych osobowych, zostają włączone i obowiązują dostawcę z dniem ich przyjęcia.

„**Hosting witryn internetowych**" Usługa hostingu witryn internetowych to usługa online, która tworzy lub utrzymuje witryny internetowe w imieniu Microsoft w domenie Microsoft, tj. dostawca przekazuje wszystkie materiały i usługi wymagane do utworzenia i utrzymania witryny oraz udostępnia ją w Internecie. „Dostawca usług hostingowych" lub „host sieciowy" to dostawca, który zapewnia narzędzia i usługi potrzebne do przeglądania witryny lub strony internetowej w Internecie, takie jak pliki cookie lub sygnalizatory sieci Web do celów reklamowych.