Microsoft Procurement

Przewodnik po programie zapewnienia bezpieczeństwa i ochrony prywatności dla dostawców (Supplier Security & Privacy Assurance – SSPA)

Wersja 8

Czerwiec 2022 r.

Wprowadzenie

W firmie Microsoft jesteśmy przekonani, że prawo do prywatności jest prawem podstawowym. Zgodnie z naszą misją wspierania rozwoju każdej osoby i organizacji na całym świecie codziennie dążymy do pozyskania i utrzymania zaufania naszych klientów.

Skuteczne procedury dotyczące ochrony prywatności i zapewnienia bezpieczeństwa są niezwykle ważne dla realizacji naszej misji oraz stanowią niezbędny element w celu zapewnienia zaufania ze strony klientów i zgodności z różnymi przepisami na ternie kilku jurysdykcji. Standardy uwzględnione w zasadach firmy Microsoft dotyczących ochrony prywatności i zapewnienia bezpieczeństwa odzwierciedlają wyznawane przez naszą firmę wartości i są wymagane od naszych dostawców (takich jak twoja firma), którzy przetwarzają Dane firmy Microsoft w naszym imieniu.

Program zapewnienia bezpieczeństwa i ochrony prywatności - Supplier Security and Privacy Assurance (**„SSPA")**jest korporacyjnym programem firmy Microsoft umożliwiającym przekazywanie naszym dostawcom podstawowych instrukcji dotyczących przetwarzania danych firmy Microsoft w formie Wymagań firmy Microsoft dotyczących ochrony danych przez dostawców („**DPR**"), które można pobrać ze strony internetowej SSPA on Microsoft.com/Procurement. Należy pamiętać o możliwej konieczności spełnienia przez dostawców dodatkowych wymagań na poziomie organizacyjnym uzgodnionych i przekazanych poza programem SSPA przez grupę Microsoft odpowiedzialną za kontakty z dostawcą

Kluczowe pojęcia związane z programem SSPA zdefiniowano w wymaganiach DPR. Aby dowiedzieć się więcej o samym programie, przeczytaj nasze najczęściej zadawane pytania - Frequently Asked Questions (FAQs) – i skontaktuj się z naszym globalnym zespołem, pisząc na adres SSPAHelp@microsoft.com.

Omówienie programu SSPA

Program SSPA powstał w ramach partnerstwa między działami Procurement, Corporate External and Legal Affairs oraz Corporate Security firmy Microsoft w celu zapewnienia przestrzegania zasad ochrony prywatności i zapewnienia bezpieczeństwa przez naszych dostawców.

Program SSPA obejmuje wszystkich dostawców z całego świata, którzy przetwarzają Dane osobowe i/lub Dane poufne firmy Microsoft w związku z wykonywaniem przez nich zobowiązań (np. dostarczanie usług, licencji oprogramowania, usług w chmurze) na podstawie warunków ich umowy z firmą Microsoft (np. warunków zamówienia zakupu, umowy ramowej) („**Wykonanie zobowiązań**" lub „**Wykonywanie zobowiązań**").

Program SSPA umożliwia dostawcy dokonanie wyborów Profili przetwarzania danych zgodnych z towarami i/lub usługami objętymi umowami. Wybory te aktywują związane z nimi wymagania do przekazania firmie Microsoft niezbędnych poświadczeń zgodności.

Wszyscy zarejestrowani dostawcy będą corocznie przeprowadzać samodzielną atestację

zgodności z wymaganiami DPR. Twój Profil przetwarzania danych określa, czy zostanie wprowadzony pełny zestaw wymagań DPR czy tylko ich podzbiór. Od dostawców, którzy przetwarzają dane traktowane przez firmę Microsoft jako dane podwyższonego ryzyka może być oczekiwane spełnienie dodatkowych wymagań, takich jak przeprowadzenie niezależnej weryfikacji zgodności. Dostawcy, którzy znajdują się w opublikowanym wykazie podrzędnych podmiotów przetwarzających firmy Microsoft będą również zobowiązani do przedstawienia niezależnej weryfikacji zgodności.

Ważne: Na podstawie działań związanych z zapewnianiem zgodności jest określany status SSPA — Zielony (zgodność) lub Czerwony (brak zgodności). Narzędzia zakupowe firmy Microsoft sprawdzają, czy status SSPA to Zielony (w przypadku każdego dostawcy objętego programem SSPA) przed zezwoleniem na kontynuację przedsięwzięcia.

Diagram procesu SSPA — rejestracja nowego dostawcy

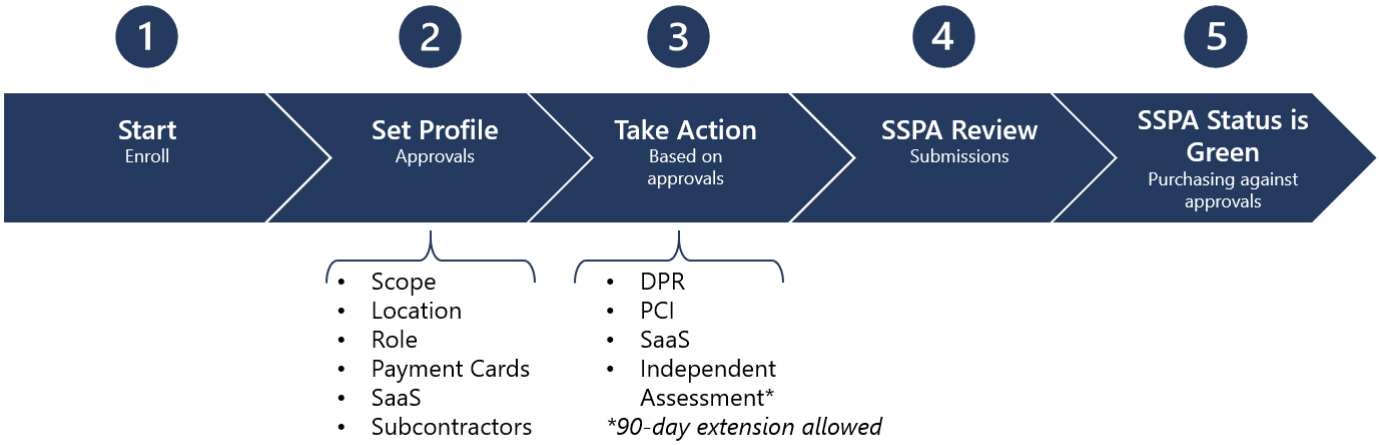
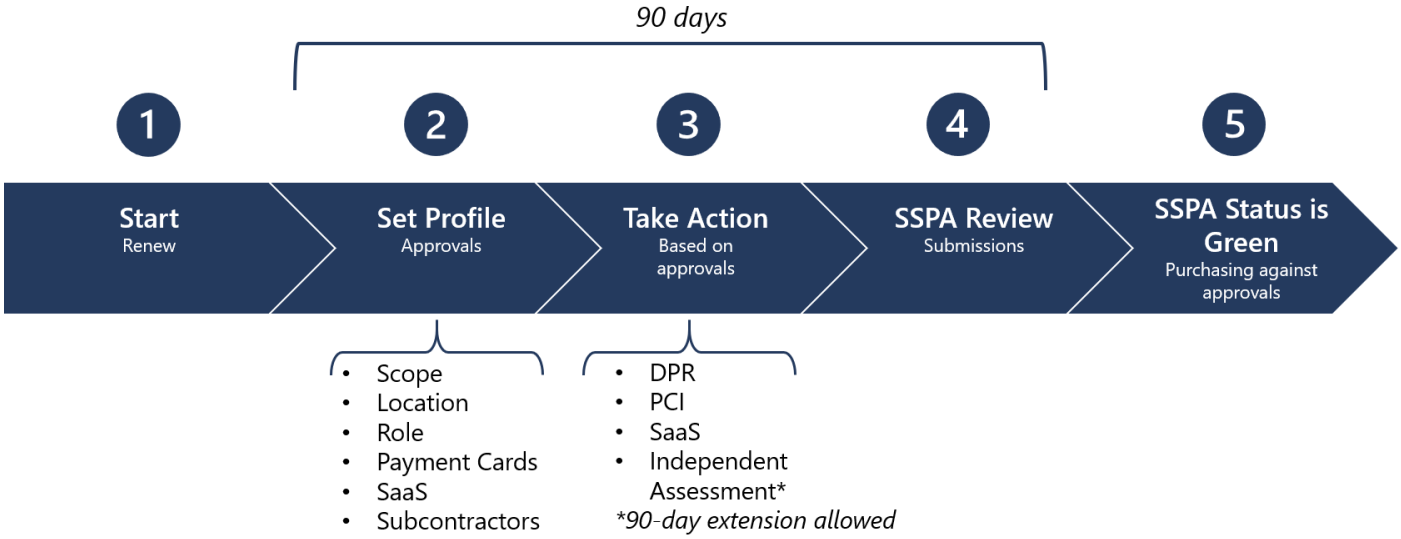


Diagram procesu SSPA — coroczne odnowienie dostawcy



Zakres programu SSPA

Aby ustalić, czy dostawca przetwarza Dane osobowe i/lub Dane poufne firmy Microsoft, zapoznaj się z listą przykładów w poniższych tabelach. Należy pamiętać, że są to jedynie przykłady, a nie kompletna lista.

Uwaga: Właściciel przedsięwzięcia biznesowego firmy Microsoft może wystąpić o rejestrację w przypadkach niewystępujących na tej liście, biorąc pod uwagę poufny charakter przetwarzanych danych.

Dane osobowe według typu danych

Przykłady obejmują w szczególności:

Dane poufne
Dane dotyczące dzieci
Dane genetyczne, biometryczne lub dane o stanie zdrowia
Informacje dotyczące pochodzenia rasowego lub etnicznego
Informacje dotyczące przekonań religijnych, politycznych i filozoficznych oraz przynależności do organizacji
Informacje dotyczące przynależności do związków zawodowych
Informacje dotyczące aktywności lub orientacji seksualnej
Status imigracyjny (wiza, pozwolenie na pracę itp.)
Numery identyfikacyjne przypisane przez administrację państwową (numery paszportu, prawa jazdy, wizy, ubezpieczenia społecznego, PESEL)
Dokładne dane o lokalizacji użytkownika (do 300 metrów)
Numery osobistych rachunków bankowych
Numery i daty ważności kart kredytowych
Dane dotyczące treści klienta
Dokumenty, zdjęcia, filmy, muzyka itp.
Recenzje i/lub oceny wprowadzone w produkcie bądź usłudze
Odpowiedzi na pytania ankietowe
Historia przeglądania, zainteresowania i ulubione
Tekst zapisany odręcznie lub z użyciem klawiatury i wypowiedzi (głos/audio i/lub czat/bot)
Dane dotyczące poświadczeń (hasła, wskazówki dotyczące haseł, nazwy użytkownika, dane biometryczne używane do identyfikacji)
Dane klienta związane ze sprawą pomocy technicznej

Dane przechwytywane i generowane
Niedokładne dane o lokalizacji
Adres IP
Preferencje i personalizacja urządzeń
Użycie usług w witrynach internetowych, śledzenie kliknięć na stronach internetowych
Dane z mediów społecznościowych, graf relacji społecznościowych
Dane dotyczące aktywności uzyskane z podłączonych urządzeń, takich jak monitory fitness
Dane kontaktowe takie jak imię i nazwisko, adres, numer telefonu, adres e-mail, data urodzenia oraz kontakty zależne i alarmowe
Dane dotyczące oceny oszustwa i ryzyka, badania informacji o przeszłości osoby
Szczegóły dotyczące ubezpieczeń, emerytur, rent i innych świadczeń
Życiorysy kandydatów, uwagi/opinie związane z rozmowami kwalifikacyjnymi
Metadata and telemetry
Dane dotyczące kont
Dane dotyczące instrumentów płatniczych
Numer i data ważności karty kredytowej
Kod banku
Numer rachunku bankowego
Wnioski o kredyt lub linię kredytową
Dokumenty i identyfikatory podatkowe
Dane dotyczące inwestycji lub wydatków
Firmowe karty płatnicze
Pseudonimizowane informacje o użytkowniku końcowym (EUPI) (Identyfikatory utworzone przez firmę Microsoft w celu identyfikacji użytkowników produktów i usług firmy Microsoft)
Unikatowy identyfikator globalny (GUID)
Identyfikator użytkownika lub unikatowy identyfikator usługi Passport (PUID)
Skrót danych osobowych użytkownika końcowego (EUII)
Identyfikatory sesji
Identyfikatory urządzeń
Dane diagnostyczne
Dane dziennika

Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

Dane poufne firmy Microsoft wg klasy danych

Przykłady obejmują w szczególności:

Ściśle poufne
Informacje dotyczące opracowywania, testowania lub wytwarzania bądź powiązane z opracowywaniem, testowaniem lub wytwarzaniem Produktów firmy Microsoft lub składników Produktów firmy Microsoft *Oprogramowanie, usługi online, usługi oraz sprzęt sprzedawane komercyjnie za pośrednictwem dowolnego kanału uznaje się za „**Produkt firmy Microsoft**”.*
Przedpremierowe materiały marketingowe dotyczące urządzeń firmy Microsoft
Nieogłoszone korporacyjne dane finansowe firmy Microsoft podlegające przepisom komisji papierów wartościowych i giełd (SEC)
Poufne
Klucze licencji produktów firmy Microsoft udostępniane w jej imieniu w związku z dystrybucją dowolną metodą
Informacje dotyczące opracowywania lub testowania bądź powiązane z opracowywaniem lub testowaniem wewnętrznych aplikacji biznesowych (LOB) firmy Microsoft
Przedpremierowe materiały marketingowe dotyczące oprogramowania i usług firmy Microsoft, takich jak Office, SQL, Azure itd.
Dokumentacja pisemna, projektowa, elektroniczna lub drukowana dotycząca wszelkich usług lub produktów firmy Microsoft, na przykład urządzeń (podręczniki procesów lub procedur, dane konfiguracyjne itp.)

Ważne: Właściciel przedsięwzięcia biznesowego firmy Microsoft może wymagać udziału w programie także w przypadku przetwarzania danych, których nie ma na tej liście.

Profil przetwarzania danych

Dostawcy firmy Microsoft mają pełną kontrolę nad swoim profilem przetwarzania danych SSPA.

Dzięki temu mogą decydować, do których przedsięwzięć chcą się kwalifikować. Zwracaj szczególną uwagę na dokonywane wybory i przemyśl działania związane z zapewnieniem zgodności, które trzeba podjąć w celu uzyskania zatwierdzenia. **Patrz „Wymagania dotyczące poświadczania zgodności” poniżej i Dodatek A.**

Grupy biznesowe firmy Microsoft będą mogły współpracować z dostawcami tylko wówczas, gdy działalność związana z przetwarzaniem danych będzie zgodna z zatwierdzeniami uzyskanymi przez dostawcę.

Dostawcy będą mogli aktualizować swój Profil przetwarzania danych w dowolnym momencie w ciągu roku, **o ile nie będzie otwartych zadań**. Po dokonaniu zmiany zostanie podjęta odpowiednia operacja, która musi zostać zakończona przed uzyskaniem zatwierdzeń. Istniejące,

uzyskane zatwierdzenia będą obowiązywały do czasu spełnienia nowo wydanych wymagań.

Jeśli nowo podjęte zadania nie zostaną zrealizowane w ciągu dozwolonego okresu 90 dni, status SSPA zmieni się na Czerwony, a konto będzie zagrożone dezaktywacją w systemach rozrachunków z dostawcami firmy Microsoft.

Zatwierdzenia przetwarzania danych	
1	Zakres przetwarzania danych ▪ Poufne ▪ Osobowe, Poufne
2	Miejsce przetwarzania danych ▪ W firmie Microsoft lub u Klienta ▪ U Dostawcy
3	Rola w procesie przetwarzania danych ▪ Administrator (niezależny Administrator lub Współadministrator) ▪ Podmiot przetwarzający ▪ Podrzędny podmiot przetwarzający (wyznaczony przez Microsoft)
4	Przetwarzanie kart płatniczych ▪ Tak ▪ Nie dotyczy
5	Oprogramowanie jako usługa ▪ Tak ▪ Nie dotyczy
6	Korzystanie z podwykonawców ▪ Tak ▪ Nie dotyczy

Kwestie związane z zatwierdzeniami

Zakres przetwarzania danych

Poufne

Wybierz to zatwierdzenie, jeśli wykonywanie zobowiązań przez dostawcę będzie obejmować Przetwarzanie tylko Danych poufnych firmy Microsoft. Zapoznaj się z definicjami zawartymi w wymaganiach DPR.

Wybranie tego zatwierdzenia uniemożliwi ci uczestniczenie w przedsięwzięciach związanych z przetwarzaniem Danych osobowych.

Osobowe, Poufne

Wybierz to zatwierdzenie, jeśli wykonywanie zobowiązań przez dostawcę będzie obejmować Przetwarzanie Danych osobowych i Danych poufnych firmy Microsoft.

Miejsce przetwarzania

W firmie Microsoft lub u klienta

Wybierz to zatwierdzenie, jeśli wykonywanie zobowiązań przez dostawcę uwzględnia Przetwarzanie danych w obrębie środowiska sieciowego firmy Microsoft, w którym personel używa poświadczeń dostępu @microsoft.com, lub w obrębie środowiska klienta firmy Microsoft.

Nie należy zaznaczać tej opcji w następujących okolicznościach:

- Dostawca zarządza wyznaczoną przez firmę Microsoft placówką zewnętrzną (offshore facility - OF).
- Dostawca zapewnia pracowników firmie Microsoft, którzy niekiedy pracują w sieci firmy Microsoft, a czasem poza nią. Miejscem przetwarzania w przypadku pracy poza siecią jest „u dostawcy".

U Dostawcy
Tę opcję należy wybrać, jeśli nie ma zastosowania warunek „W firmie Microsoft lub u Klienta" (zgodnie z powyższym opisem).

_____

Rola w procesie przetwarzania danych

Administrator danych (dotyczy niezależnych Administratorów danych i Współadministratorów)

To zatwierdzenie należy wybrać, jeśli **wszystkie** aspekty wykonywania zobowiązań przez dostawcę są zgodne z definicją roli Administratora w procesie przetwarzania danych (patrz wymagania DPR).

Wybranie tego zatwierdzenia uniemożliwi Ci uczestniczenie w przetwarzaniu Danych osobowych w roli „Podmiotu przetwarzającego". Jeśli dostawca jest jednocześnie Podmiotem przetwarzającym i Administratorem względem firmy Microsoft, zamiast opcji „Administrator", należy wybrać opcję „Podmiot przetwarzający".

Podmiot przetwarzający

To najbardziej typowa rola w przypadku, gdy dostawcy zajmują się Przetwarzaniem danych na rzecz firmy Microsoft. Zapoznaj się z definicjami Podmiotu przetwarzającego i Podrzędnego podmiotu przetwarzającego zawartymi w wymaganiach DPR.

Podrzędny podmiot przetwarzający

Podrzędny podmiot przetwarzający jest stroną trzecią, którą firma Microsoft zatrudnia do wykonywania zadań, a przedmiot zadań obejmuje Przetwarzanie Danych osobowych firmy Microsoft, w odniesieniu do których Microsoft jest Podmiotem przetwarzającym. Podwykonawcy nie mogą sami określić się w firmie Microsoft jako Podrzędne podmioty przetwarzające, ponieważ wymaga to wstępnego zatwierdzenia przez wewnętrzne zespoły ds. ochrony prywatności. Podrzędne podmioty

przetwarzające mogą posiadać ten status jedynie wówczas, gdy firma Microsoft jest Podmiotem przetwarzającym, a dostawcy przetwarzają kwalifikujące się rodzaje Danych osobowych przedsiębiorstwa. Podrzędne podmioty przetwarzające będą działać w ramach dodatkowego kontraktu i będą objęte dodatkowymi wymogami w zakresie zgodności, w tym Aneksem dotyczącym ochrony danych i wymogiem poddania się niezależnej ocenie (patrz poniżej).

Przetwarzanie kart płatniczych

Wybierz to zatwierdzenie, jeśli jakakolwiek część danych Przetwarzanych przez dostawcę obejmuje dane dotyczące obsługi kart kredytowych lub innych kart płatniczych na rzecz firmy Microsoft.

To zatwierdzenie umożliwia dostawcy uczestniczenie w przedsięwzięciach związanych z przetwarzaniem kart płatniczych.

Oprogramowanie

Microsoft Procurement wymaga od nabywców wszelkiego oprogramowania poddanie się procedurze przyjmowania wniosków, która obejmuje różne sprawdziany, w tym sprawdzian najistotniejszych czynników – „SSPA triage" – aby zdecydować, czy dostawca oprogramowania odpowiada wymogom SSPA. (Nabywcy firmy Microsoft mogą zapoznać się z krokami i bliższymi szczegółami określonymi na wewnętrznej stronie internetowej ProcureWeb Software and Cloud Service). Jeśli mają zastosowanie wymogi SSPA, od dostawców może także być wymagane określenie mającego zastosowanie profilu „Oprogramowanie jako usługa" (SaaS). W przypadku dostawców zarejestrowanych dla potrzeb SSPA może to być dokonane podczas wprowadzania informacji dotyczących profilu przetwarzania danych w portalu Microsoft Supplier Compliance Portal.

Termin SaaS należy dla potrzeb zgodności z SSPA interpretować szeroko i uwzględnić „Platformę jako usługa" (Platform as a service - PaaS), a także „Infrastrukturę jako usługa" (Infrastructure as a service - IaaS). (Aby dowiedzieć się więcej, proszę zapoznać się z tym wyjaśnieniem.)

Oprogramowanie jako usługa (Software as a Service, SaaS)

Oprogramowanie jako usługa (SaaS) pozwala użytkownikom łączyć się przez Internet i korzystać z aplikacji w chmurze.

Firma Microsoft definiuje **„SaaS"** jako dostarczanie funkcji oprogramowania za pośrednictwem mechanizmu internetowego, opartego na wspólnym kodzie, używanego w modelu jeden-do-wielu (one-to-many) na zasadzie płatności za użytkowanie lub jako subskrypcji opartej na metrykach użytkowania. Dostawca usług w chmurze tworzy i utrzymuje oprogramowanie zlokalizowane w chmurze, zapewnia automatyczną aktualizację oprogramowania, udostępnia je klientom przez Internet na bazie jeden-do-wielu (one-to-many) i pay-as-you-go. Ta metoda udostępniania oprogramowania i korzystania z licencji pozwala na korzystanie z oprogramowania w trybie online w ramach subskrypcji, a nie nabywania go i instalowania na indywidualnym komputerze.

Uwaga: Większość dostawców SaaS będzie wymagać dodania zatwierdzenia podwykonawcy w

portalu Microsoft Supplier Compliance Portal, jeśli Dane osobowe lub Dane poufne firmy Microsoft znajdują się na platformie strony trzeciej.

Korzystanie z Podwykonawców

Wybierz to zatwierdzenie, jeśli wykonywanie zobowiązań przez dostawcę obejmuje korzystanie z usług Podwykonawców (zapoznaj się z definicjami zawartymi w wymaganiach DPR).

Dotyczy to również Osób pracujących na własny rachunek (patrz DPR).

Wymagania dotyczące poświadczenia zgodności

Wymagania na podstawie zatwierdzeń związanych z profilami

Zatwierdzenia wybrane w twoim Profilu przetwarzania danych pomagają SSPA w ocenie poziomu ryzyka w zakresie twojego zadania lub zadań wykonywanych na rzecz firmy Microsoft. Wymagania dotyczące zgodności różnią się w zależności od Profilu przetwarzania danych i związanych z nimi zatwierdzeniami. Niniejsza sekcja wyjaśnia różne wymagania SSPA.

Są również kombinacje, które mogą zwiększać lub zmniejszać wymagania dotyczące zgodności. Przedstawiono je w Dodatku A i tego można się spodziewać po wypełnieniu profilu w portalu Supplier Compliance Portal. Można zawsze sprawdzić, czy dany scenariusz mieści się w tych ramach, zwracając się do zespołu SSPA o dokonanie przeglądu.

Działanie: Znajdź swój profil zatwierdzenia w Dodatku A i zapoznaj się z odpowiednimi wymaganiami poświadczania zgodności, a w stosownych przypadkach z opcjami niezależnego poświadczania zgodności.

Ważne: W przypadku wybrania w profilu opcji Oprogramowanie jako usługa (SaaS), Korzystanie z podwykonawców, Hostowanie witryn internetowych lub Karty płatnicze wymagane jest dodatkowe poświadczenie zgodności.

Samodzielna atestacja zgodności z wymaganiami DPR

Wszyscy dostawcy zarejestrowani w programie SSPA są zobowiązani do przeprowadzenia samodzielnej atestacji zgodności z wymaganiami DPR w terminie 90 dni od otrzymania prośby. Wezwanie to będzie kierowane do nich corocznie, ale może się pojawiać częściej, jeśli Profil przetwarzania danych będzie aktualizowany w trakcie trwania roku. Jeśli termin 90 dni zostanie przekroczony, status SSPA kont dostawcy zostanie zmieniony na Czerwony (brak zgodności). Nowe zamówienia zakupu podlegające zgodności z programem można przetwarzać dopiero po zmianie statusu SSPA na Zielony (zgodność).

Nowo zarejestrowani dostawcy muszą spełniać wymagania, zgodnie z wyborami zatwierdzeń, aby przed rozpoczęciem przedsięwzięć uzyskać Zielony status SSPA (zgodność).

Ważne: Zespół SSPA nie ma uprawnień do przedłużania terminu realizacji tego zadania.

Upoważnieni przedstawiciele, którzy przeprowadzą atestację samodzielną, powinni uzyskać odpowiednie informacje od specjalistów, aby zapewnić spełnienie wszystkich wymagań. Ponadto, wpisując swoje imię i nazwisko do formularza SSPA, dana osoba poświadcza, że zapoznała się z wymaganiami DPR i w pełni zrozumiała ich treść. Dostawcy zawsze mogą dodawać inne osoby kontaktowe w narzędziu online, które będą im pomagały w spełnianiu wymagań.

Obowiązki Autoryzowanego przedstawiciela (patrz definicja w DPR):

1. Ustalenie obowiązujących wymagań.
2. Udzielenie odpowiedzi dotyczącej każdego obowiązującego wymagania.
3. Podpisanie i przesłanie atestacji w portalu Microsoft Supplier Compliance Portal.

Zakres zastosowania

Od dostawców oczekuje się udzielenia odpowiedzi dotyczących wszystkich obowiązujących wymagań DPR wydanych dla każdego Profilu przetwarzania danych. Można oczekiwać, że kilka z wydanych wymagań może nie dotyczyć towarów lub usług dostarczanych przez dostawcę firmie Microsoft. Mogą być one oznaczone jako „nie ma zastosowania" i opatrzone szczegółowym komentarzem dla audytorów SSPA w celu weryfikacji.

Zgłoszenia dotyczące wymagań DPR są przeglądane przez zespół SSPA pod kątem zaznaczonych opcji „nie ma zastosowania", „kolizja z prawem lokalnym" lub „kolizja dotycząca zobowiązań umownych". Zespół SSPA może poprosić o wyjaśnienie niektórych opcji. Kolizje z prawem lokalnym lub dotyczące zobowiązań umownych są dopuszczalne tylko wówczas, gdy zostaną dostarczone materiały referencyjne i charakter kolizji jest jasny.

Wymaganie dotyczące niezależnej oceny

W części Wymagania na podstawie zatwierdzeń związanych z profilami w Dodatku A znaleźć można zatwierdzenia dotyczące przetwarzania, które aktywują to wymaganie.

Dostawcy mają możliwość zmiany zatwierdzeń poprzez aktualizowanie swojego Profilu przetwarzania danych. Jeśli jednak rola dostawcy w procesie przetwarzania danych to „Podrzędny podmiot przetwarzający", dostawca nie może zmienić tego zatwierdzenia i będzie od niego wymagane coroczne poddawanie się niezależnej ocenie.

Aby uzyskać zatwierdzenie wymagające niezależnej weryfikacji zgodności, dostawcy muszą wybrać niezależnego rewidenta, który zweryfikuje zgodność z wymaganiami DPR. Rewident powinien przygotować pismo doradcze, aby przedstawić firmie Microsoft poświadczenia zgodności. Pismo to powinno być wolne od zastrzeżeń, a wszystkie kwestie niezgodności muszą zostać rozstrzygnięte i naprawione przed dostarczeniem pisma zespołowi SSPA do weryfikacji za pomocą portalu Microsoft Supplier Compliance Portal. Rewidenci mogą ściągnąć zatwierdzony szablon pisma doradczego, który załączony jest do „Listy preferowanych rewidentów". Plik PDF dostępny jest tutaj.

Dodatek A zawiera dopuszczalne alternatywne opcje certyfikacji w przypadku podjęcia decyzji o nieskorzystaniu z weryfikacji zgodności z wymaganiami DPR przez niezależnego rewidenta (w stosownych przypadkach, na przykład w przypadku dostawców usług SaaS, dostawców hostingu witryn internetowych lub dostawców korzystających z usług podwykonawców). Certyfikaty ISO 27701(prywatność) i ISO 27001 (bezpieczeństwo) są uznawane z uwagi na merytoryczne pokrewieństwo z Wymaganiami dotyczącymi ochrony danych (DPR).

W przypadkach, w których Dostawca jest usługodawcą w zakresie ochrony zdrowia w Stanach Zjednoczonych lub na kwalifikującym się obszarze, uznamy raport HITRUST w zakresie ochrony prywatności i bezpieczeństwa za dostateczny.

Zespół SSPA może doraźnie przeprowadzać niezależną ocenę, jeśli okoliczności niezależne od standardowych czynników uzasadniają konieczność zachowania dodatkowej staranności. Przykładowo może to być wniosek od osób zajmujących się ochroną prywatności lub bezpieczeństwem w oddziale, weryfikacja działań naprawczych po przypadkach naruszeń ochrony danych lub wymaganie zautomatyzowanego egzekwowania praw osób, których dane dotyczą.

Wskazówki dotyczące spełnienia tego wymagania:

1. Aby adekwatnie ocenić zgodność, rewident musi ukończyć odpowiednie szkolenie techniczne i mieć dostateczną wiedzę specjalistyczną.
2. Rewidenci muszą być członkami Międzynarodowej Federacji Księgowych (IFAC, International Federation of Accountants) lub Amerykańskiego Instytutu Biegłych Rewidentów (AICPA, American Institute of Certified Public Accountants) lub muszą posiadać certyfikaty innych odpowiednich organizacji zajmujących się ochroną prywatności i bezpieczeństwem, takich jak Międzynarodowe Stowarzyszenie Specjalistów ds. Ochrony Prywatności (IAPP, International Association of Privacy Professionals) lub Stowarzyszenie Audytu i Kontroli Systemów Informacyjnych (ISACA, Information Systems Audit and Control Association).
3. Rewident musi korzystać z najbardziej aktualnego dokumentu DPR, który zawiera opis dowodu zgodności na poparcie każdego wymagania. **Dostawcy powinni dostarczyć rewidentowi najbardziej aktualne, zatwierdzone odpowiedzi atestu zgodności z wymaganiami DPR.**
4. W przypadku nowo zarejestrowanego dostawcy rewident musi sprawdzić projekt mechanizmów kontroli procesu. We wszystkich innych przypadkach rewident sprawdza skuteczność mechanizmów kontroli.
5. Zakres oceny jest ograniczony do Danych osobowych i Danych poufnych firmy Microsoft związanych z wykonywaniem zobowiązań przez danego dostawcę.
6. Zakres oceny jest ograniczony do wszystkich aktywności przetwarzania danych objętych programem wykonywanych w odniesieniu do numeru konta dostawcy, który otrzymał wniosek. Jeśli dostawca zdecyduje się na ocenę kilku kont jednocześnie, **atest musi zawierać listę kont dostawcy objętych oceną i powiązanych z nimi adresów.**
7. Pismo przedłożone zespołowi SSPA nie może zawierać żadnych zapisów stwierdzających, że dostawca nie może spełnić zapisanych Wymagań dotyczących ochrony danych. Takie kwestie muszą zostać rozwiązane przed przesłaniem pisma.

Zespół SSPA udostępnił listę preferowanych rewidentów. Firmy te są zorientowane w przeprowadzaniu ocen SSPA. Za ocenę powinni płacić dostawcy. Koszty różnią się w zależności od skali i zakresu przetwarzania danych.

Wymaganie dotyczące certyfikacji PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) to struktura mająca na celu zapewnienie skutecznych zabezpieczeń płatności kartami płatniczymi obejmująca także zapobieganie incydentom naruszenia zabezpieczeń, wykrywanie takich incydentów i reagowanie na nie. Została ona stworzona przez Radę Standardów Bezpieczeństwa PCI (PCI Security Standards Council) – branżową organizację samoregulacyjną. Wymagania PCI DSS mają na celu identyfikowanie luk w technologii i procesach, które stwarzają zagrożenie dla bezpieczeństwa przetwarzanych danych posiadaczy kart płatniczych.

Firma Microsoft jest zobowiązana do zachowania zgodności z tymi standardami. Jeśli dostawca przetwarza informacje dotyczące kart płatniczych na rzecz firmy Microsoft, wymagamy dowodów potwierdzających przestrzegania tych standardów. Na stronie Rady Standardów Bezpieczeństwa PCI można znaleźć informacje ułatwiające zrozumienie wymagań organizacji PCI.

W zależności od liczby przetwarzanych transakcji od dostawcy wymagane będzie zlecenie poświadczenia zgodności przez wykwalifikowanego rewidenta ds. bezpieczeństwa albo wypełnienie formularza samooceny.

Marki kart płatniczych wyznaczają wartości progowe typu oceny, zazwyczaj są one następujące:

- Poziom 1: Przedłożenie certyfikatu PCI AOC rewidenta będącego osobą trzecią
- Poziom 2 lub 3: Przedłożenie kwestionariusza samooceny (SAQ) PCI DSS podpisanego przez członka kierownictwa dostawcy.

Należy przedłożyć certyfikat, który dotyczy wymagań PCI i który je spełnia.

Wymaganie dotyczące Oprogramowania jako usługa

Od dostawców, którzy odpowiadają definicji SaaS znajdującej się w profilu przetwarzania danych może być wymagane przedłożenie ważnego certyfikatu ISO 27001, jeśli jest to wymagane w porozumieniu z firmą Microsoft w zakresie usług w chmurze (Cloud Services Agreement).

Audytorzy SSPA dokonają walidacji, oceniając czy twoje zgłoszenia odpowiadają zobowiązaniom kontraktowym.

Nie wymagamy zewnętrznej certyfikacji centrum danych. Oczekujemy certyfikatu ISO 27001 w odniesieniu do usług oprogramowania świadczonych na rzecz firmy Microsoft i zawartych w umowie z firmą Microsoft.

Korzystanie z podwykonawców

Firma Microsoft uważa korzystanie z podwykonawców za czynnik wysokiego ryzyka. Dostawcy korzystający z pomocy podwykonawców, którzy mają Przetwarzać Dane osobowe i Dane poufne firmy Microsoft muszą ujawnić tożsamość tych podwykonawców. Ponadto dostawca winien ujawnić, w

odniesieniu do każdego z podwykonawców, w których państwach te dane osobowe będą przetwarzane.

Przypadki naruszeń ochrony danych

Jeśli dostawca otrzyma informacje o wystąpieniu naruszenia związanego z ochroną prywatności lub bezpieczeństwem danych, musi powiadomić firmę Microsoft zgodnie z opisem w wymaganiach DPR.

Należy zgłosić naruszenie poprzez SupplierWeb lub wysłać wiadomość e-mail na adres SupplR@microsoft.com.

Należy uwzględnić następujące informacje:

- Data wystąpienia naruszenia ochrony danych:
- Nazwa dostawcy:
- Numer dostawcy:
- Powiadomiona osoba kontaktowa z firmy Microsoft:
- Powiązane zlecenie zakupu (jeśli dotyczy / jest dostępne):
- Krótki opis naruszenia ochrony danych:

Dodatek A

Wymagania na podstawie zatwierdzeń związanych z profilami

Lp.	Profil	Wymagania dotyczące poświadczenia zgodności	Opcje niezależnego poświadczenia zgodności
1	**Zakres:** Osobowe, Poufne **Miejsce przetwarzania:** W firmie Microsoft lub u Klienta **Rola w procesie przetwarzania:** Podmiot przetwarzający lub Administrator danych **Klasa danych:** Poufne lub Ściśle poufne **Karty płatnicze:** Nie dotyczy **SaaS:** Nie dotyczy **Korzystanie z podwykonawców:** Nie dotyczy **Hostowanie witryn internetowych:** Nie dotyczy	Samodzielna atestacja zgodności z wymogami DPR	
2	**Zakres:** Poufne **Miejsce przetwarzania:** U Dostawcy **Rola w procesie przetwarzania:** N/A **Klasa danych:** Poufne **Karty płatnicze:** Nie dotyczy **SaaS:** Nie dotyczy **Korzystanie z podwykonawców:** Nie dotyczy **Hostowanie witryn internetowych:** Nie dotyczy	Samodzielna atestacja zgodności z wymogami DPR	

3	**Zakres:** Poufne **Miejsce przetwarzania:** U Dostawcy **Rola w procesie przetwarzania:** Podmiot przetwarzający **Klasa danych:** Ściśle poufne **Karty płatnicze:** Nie dotyczy **SaaS:** Nie dotyczy **Korzystanie z podwykonawców:** Nie dotyczy **Hostowanie witryn internetowych:** Nie dotyczy	Samodzielna atestacja zgodności z wymogami DPR **i** Niezależne poświadczenie zgodności	Opcje niezależnego poświadczenia zgodności: 1. Przeprowadzenie niezależnej oceny zgodności z wymogami DPR, **lub** 2. Przedłożenie certyfikatu ISO 27001

Lp.	Profil	Wymagania dotyczące poświadczenia zgodności	Opcje niezależnego poświadczenia zgodności
4	**Zakres:** Osobowe, Poufne **Miejsce przetwarzania:** U Dostawcy **Rola w procesie przetwarzania:** Podmiot przetwarzający **Klasa danych:** Ściśle poufne **Karty płatnicze:** Nie dotyczy **SaaS:** Nie dotyczy **Korzystanie z podwykonawców:** Nie dotyczy **Hostowanie witryn internetowych:** Nie dotyczy	Samodzielna atestacja zgodności z wymogami DPR **i** Niezależne poświadczenie zgodności	Opcje niezależnego poświadczenia zgodności: 1. Przeprowadzenie niezależnej oceny zgodności z wymogami DPR, 2. Przeprowadzenie niezależnej oceny zgodności z wymogami sekcji A-I DPR i ISO 27001, **lub** 3. Przedłożenie certyfikatów ISO 27701 **i** ISO 27001
5	**Zakres:** Osobowe, Poufne **Miejsce przetwarzania:** U Dostawcy **Rola w procesie przetwarzania:** Podmiot przetwarzający **Klasa danych:** Poufne **Karty płatnicze:** Nie dotyczy **SaaS:** Nie dotyczy **Korzystanie z podwykonawców:** Nie dotyczy **Hostowanie witryn internetowych:** Nie dotyczy	Samodzielna atestacja zgodności z wymogami DPR	

6	**Zakres:** Osobowe, Poufne **Miejsce przetwarzania:** U Dostawcy **Rola w procesie przetwarzania:** Administrator danych **Klasa danych:** Ściśle poufne lub Poufne **Karty płatnicze:** Nie dotyczy **SaaS:** Nie dotyczy **Korzystanie z podwykonawców:** Nie dotyczy **Hostowanie witryn internetowych:** Nie dotyczy	Samodzielna atestacja zgodności z wymogami DPR	

Lp.	Profil	Wymagania dotyczące poświadczenia zgodności	Opcje niezależnego poświadczenia zgodności
7	**Zakres:** Osobowe, Poufne **Miejsce przetwarzania:** Dowolne **Rola w procesie przetwarzania:** Podrzędny podmiot przetwarzający (Rola określona przez firmę Microsoft – profil będzie zawierał tekst „Zatwierdzenie podrzędnego podmiotu przetwarzającego: Tak") **Klasa danych:** Ściśle poufne lub Poufne **Karty płatnicze:** Nie dotyczy **SaaS:** Nie dotyczy **Korzystanie z podwykonawców:** Nie dotyczy **Hostowanie witryn internetowych:** Nie dotyczy	Samodzielna atestacja zgodności z wymogami DPR **i** Niezależne poświadczenie zgodności	Opcje niezależnego poświadczenia zgodności: 1. Przeprowadzenie niezależnej oceny zgodności z wymogami DPR, 2. Przeprowadzenie niezależnej oceny zgodności z wymogami sekcji A-I DPR i ISO 27001, **lub** 3. Przedłożenie certyfikatów ISO 27701 **i** ISO 27001

Lp.	Profil	Wymagania dotyczące poświadczenia zgodności	Opcje niezależnego poświadczenia zgodności
Wpływ dodania opcji SaaS, Podwykonawcy, Hostowanie witryn internetowych			
8	**Zakres:** Osobowe, Poufne **Miejsce przetwarzania:** U Dostawcy **Rola w procesie przetwarzania:** Podmiot przetwarzający **Klasa danych:** Ściśle poufne lub Poufne **Karty płatnicze:** Nie dotyczy **Podwykonawcy:** TAK lub **SaaS:** TAK lub **Hostowanie witryn internetowych:** TAK	Samodzielna atestacja zgodności z wymogami DPR **i** Niezależne poświadczenie zgodności	Opcje niezależnego poświadczenia zgodności: 1. Przeprowadzenie niezależnej oceny zgodności z wymogami DPR, 2. Przeprowadzenie niezależnej oceny zgodności z wymogami sekcji A-I DPR i ISO 27001, **lub** 3. Przedłożenie certyfikatów ISO 27701 **i** ISO 27001
9	**Zakres:** Osobowe, Poufne **Miejsce przetwarzania:** U Dostawcy **Rola w procesie przetwarzania:** Administrator danych **Klasa danych:** Ściśle poufne lub Poufne **Karty płatnicze:** Nie dotyczy **Podwykonawcy:** TAK lub **SaaS:** TAK lub **Hostowanie witryn internetowych:** TAK	Samodzielna atestacja zgodności z wymogami DPR	

Lp.	Profil	Wymagania dotyczące poświadczenia zgodności	Opcje niezależnego poświadczenia zgodności
Dodatkowe poświadczenia w przypadku opcji Karty płatnicze i SaaS			
10	Dowolny z powyższych profili i **Karty płatnicze**	Stosowne powyższe wymagania **oraz** poświadczenie z branży kart płatniczych	Przedłożenie certyfikatu PCI DSS
11	Dowolny z powyższych profili i **Oprogramowanie jako usługa (SaaS)**	Stosowne powyższe wymagania **oraz** przedłożenie wymaganego na podstawie umowy certyfikatu ISO 27001 obejmującego usługi funkcjonalne.	Przedłożenie certyfikatu ISO 27001, którego zakres funkcjonalny obejmuje świadczone usługi.