Microsoft Procurement

Leitfaden zum Supplier Security & Privacy Assurance Program (SSPA; Programm zur Sicherheit und für den Datenschutz von Lieferanten)

Version 8

Juni 2022

Einführung

Wir bei Microsoft glauben, dass der Schutz der Privatsphäre ein Grundrecht ist. In unserem Bestreben, jeden Einzelnen und jedes Unternehmen auf der Welt in die Lage zu versetzen, mehr zu erreichen, unternehmen wir Tag um Tag Anstrengungen, das Vertrauen unserer Kunden zu gewinnen und zu erhalten.

Starke Datenschutz- und Sicherheitspraktiken sind entscheidend für unsere Mission, unerlässlich für das Vertrauen unserer Kunden und in einigen Ländern sogar gesetzlich vorgeschrieben. Die in den Datenschutz- und Sicherheitsrichtlinien von Microsoft festgehaltenen Standards spiegeln unsere Werte als Unternehmen wider und gelten auch für unsere Zulieferer (wie Ihr Unternehmen), die in unserem Auftrag Daten von Microsoft verarbeiten.

Das Supplier Security and Privacy Assurance Program (Programm zur Sicherheit und für den Datenschutz von Lieferanten) („**SSPA**“) ist das Unternehmensprogramm von Microsoft, das dazu dient, die grundlegenden Datenverarbeitungsanweisungen von Microsoft an unsere Lieferanten weiterzugeben, und zwar in Form der Datenschutzanforderungen für Lieferanten von Microsoft („**DPR**“), die auf SSPA auf Microsoft.com/Procurement. verfügbar sind. Beachten Sie, dass Lieferanten möglicherweise zusätzliche Anforderungen auf organisatorischer Ebene erfüllen müssen, die außerhalb des SSPA von der Microsoft-Gruppe, die für die Zusammenarbeit mit dem Lieferanten verantwortlich ist, beschlossen und kommuniziert werden.

Die wichtigsten SSPA-Begriffe sind in der DPR definiert. Um mehr über das Programm zu erfahren, lesen Sie unsere Häufig gestellten Fragen (FAQs) oder wenden Sie sich an unser globales Team, indem Sie an SSPAHelp@microsoft.com schreiben.

Überblick über das SSPA-Programm

SSPA ist eine Partnerschaft zwischen Microsoft Procurement, Corporate External and Legal Affairs und Corporate Security, um sicherzustellen, dass die Prinzipien des Datenschutzes und der Sicherheit von unseren Zulieferern eingehalten werden.

Der Geltungsbereich von SSPA erstreckt sich auf alle Lieferanten weltweit, die personenbezogene Daten und/oder vertrauliche Daten von Microsoft im Zusammenhang mit der Leistung des Lieferanten (z.B. Bereitstellung von Diensten, Softwarelizenzen, Cloud-Diensten) gemäß den Bedingungen seines Vertrags mit Microsoft (z.B. Bestellbedingungen, Rahmenvertrag) verarbeiten („**durchführen**“, „**leisten / Leistung erbringen / erfüllen**“ oder „**Leistung**“).

SSPA ermöglicht dem Lieferanten die Auswahl von Datenverarbeitungsprofilen, die auf die Waren und/oder Dienstleistungen abgestimmt sind, für die Sie einen Vertrag abgeschlossen haben. Diese Auswahlen lösen entsprechende Anforderungen aus, um Microsoft die Einhaltung der Vorschriften zuzusichern.

Alle registrierten Lieferanten füllen jährlich eine Selbstauskunft zur Einhaltung der DPR aus. Ihr Datenverarbeitungsprofil bestimmt, ob die vollständige DPR ausgestellt wird oder ob eine Teilmenge der Anforderungen gilt. Lieferanten, die Daten verarbeiten, die von Microsoft als risikoreicher eingestuft werden, müssen möglicherweise zusätzliche Anforderungen erfüllen, wie eine unabhängige Überprüfung der Einhaltung der DPR. Lieferanten, die auf einer von Microsoft veröffentlichten Liste von Unterauftragsverarbeitern stehen, werden ebenfalls aufgefordert, eine unabhängige Überprüfung der Einhaltung der Anforderungen vorzulegen.

Wichtig: Die Konformitätsaktivitäten bestimmen einen SSPA-Status von Grün (konform) oder Rot (nicht konform). Die Tools von Microsoft für den Einkauf überprüfen, ob der SSPA-Status „Grün“ ist (für Lieferanten, die in den Geltungsbereich von SSPA fallen), bevor sie die Durchführung eines Auftrags erlauben.

Diagramm des SSPA-Verfahrens – Registrierung Neuer Lieferanten

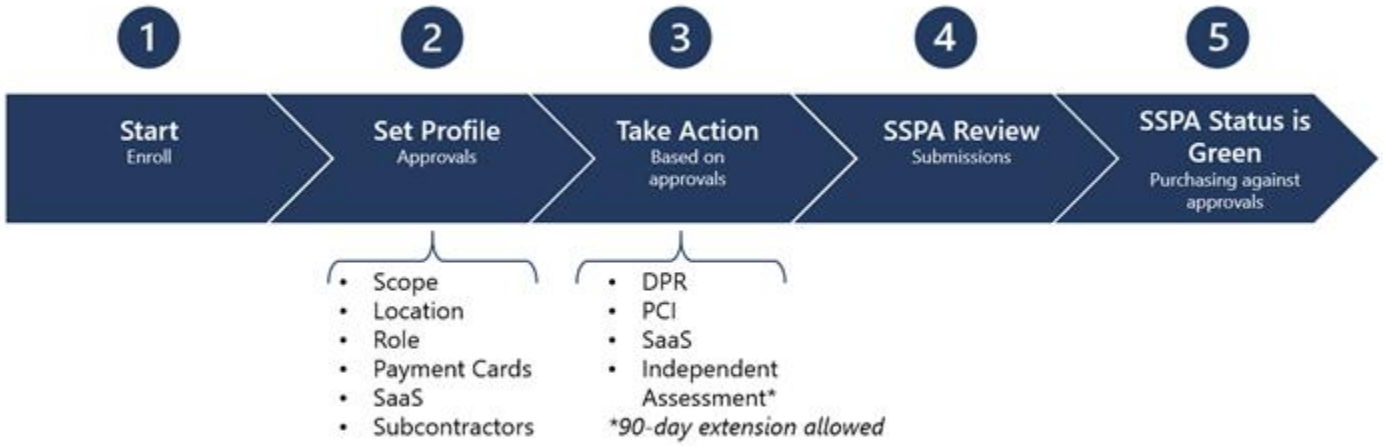
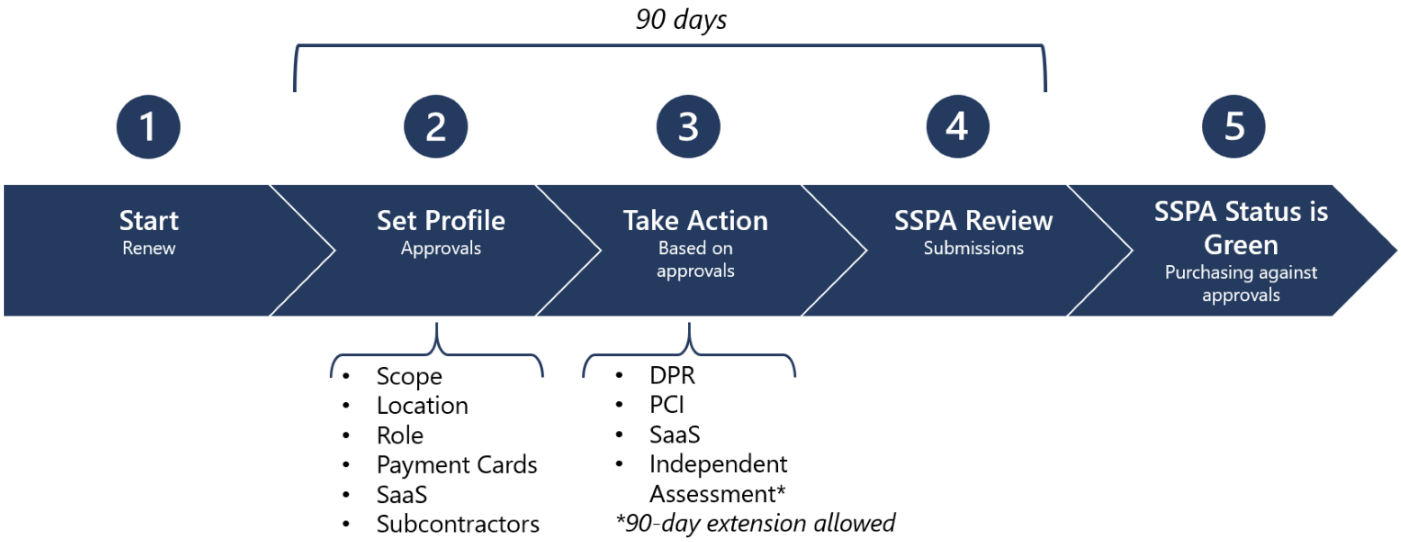


Diagramm des SSPA-Verfahrens – Jährliche Verlängerung des Lieferanten



SSPA-Umfang

Um festzustellen, ob Sie (der Lieferant) personenbezogene Daten und/oder vertrauliche Daten von Microsoft verarbeiten, sehen Sie sich die Liste der Beispiele in den folgenden Tabellen an. Bitte beachten Sie, dass es sich hierbei um Beispiele handelt und die Liste nicht erschöpfend ist.

Hinweis: Ein Microsoft-Geschäftseigentümer kann in Anbetracht des vertraulichen Charakters der verarbeiteten Daten um eine Registrierung außerhalb dieser Liste bitten.

Personenbezogene Daten nach Datentyp

Beispiele umfassen, sind aber nicht beschränkt auf:

Sensible Daten
Daten in Bezug auf Kinder
Genetische Daten, biometrische Daten oder Gesundheitsdaten
Rasse oder ethnische Herkunft
Politische, religiöse oder philosophische Überzeugungen, Meinungen und Zugehörigkeiten
Mitgliedschaft in einer Gewerkschaft
Das Sexualleben oder die sexuelle Orientierung einer natürlichen Person
Einwanderungsstatus (Visum; Arbeitsgenehmigung usw.)
Staatliche Identifikationsmerkmale (Reisepass; Führerschein; Visum; Sozialversicherungsnummern; staatliche Ausweisnummern)
Genaue Positionsdaten des Benutzers (innerhalb von 300 Metern)
Persönliche Bankkontonummern
Kreditkartennummer und Gültigkeitsdatum
Daten zum Kundeninhalt
Dokumente, Fotos, Videos, Musik, usw.
Für ein Produkt oder eine Dienstleistung abgegebene Bewertungen und/oder Beurteilungen
Antworten auf Umfragen
Browserverlauf, Interessen und Favoriten
Handschriftliche und maschinelle Eingaben und Sprachäußerungen (Stimme/Audio und/oder Chat/Bot)
Berechtigungsdaten (Kennwörter, Kennwort-Hinweise, Benutzername, biometrische Daten, die zur Identifizierung verwendet werden)
Kundendaten, die mit einem Supportfall verbunden sind

Erfasste und generierte Daten
Unpräzise Positionsdaten
IP-Adresse
Gerätepräferenzen und Personalisierung
Servicenutzung für Websites, Verfolgung von Webseitenklicks
Daten aus sozialen Medien, Social Graph-Beziehungen
Aktivitätsdaten von angeschlossenen Geräten wie Fitnessmonitoren
Kontaktdaten wie Name, Adresse, Telefonnummer, E-Mail-Adresse, Geburtsdatum, abhängige und Notfallkontakte
Betrugs- und Risikobewertung, Hintergrundüberprüfung
Versicherung, Rente, positive Auswirkungen
Lebensläufe von Bewerbern, Gesprächsnotizen/Feedback
Metadata and telemetry
Kontodaten
Daten von Zahlungsinstrumenten
Kreditkartennummer und Gültigkeitsdatum
Bankleitzahl
Bankkontonummer
Kreditanträge und Kreditlinien
Steuerdokumente und Identifikatoren
Daten zu Investitionen und Ausgaben
Firmenkarten
Pseudonymisierte Endbenutzer-Informationen (EUPI) (Identifikatoren, die von Microsoft erstellt wurden, um Benutzer von Microsoft-Produkten und -Diensten zu identifizieren)
Globally Unique Identifier (GUID)
Passport User ID und Unique Identifier (PUID)
Hashed End-User Identifiable Information (EUII)
Sitzungs-ID
Geräte-ID
Diagnostische Daten
Protokolldaten

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

Microsoft Vertrauliche Daten nach Datenklasse

Beispiele umfassen, sind aber nicht beschränkt auf:

Streng vertraulich
Informationen, die die Entwicklung, das Testen oder die Herstellung von Microsoft-Produkten oder Komponenten von Microsoft-Produkten betreffen oder damit in Zusammenhang stehen *Software, Online-Dienste oder Hardware von Microsoft, die über einen beliebigen Vertriebskanal verkauft werden, gelten als „**Microsoft-Produkte**“*
Marketinginformationen vor der Veröffentlichung von Microsoft-Geräten
Unangekündigte Finanzdaten von Microsoft-Unternehmen, die den Regeln der SEC unterliegen
Vertraulich
Microsoft-Produktlizenzschlüssel im Namen von Microsoft zur Verteilung über jegliche Methode
Informationen, die die Entwicklung oder das Testen von Microsoft-internen Line of Business (LOB)-Anwendungen betreffen oder damit in Zusammenhang stehen
Marketingmaterial von Microsoft vor der Veröffentlichung von Microsoft-Software und -Diensten wie Office, SQL, Azure usw.
Schriftliche, gestalterische, elektronische oder gedruckte Dokumentation für Microsoft-Dienste oder -Produkte, wie z. B. Geräte (Prozess- oder Verfahrensanleitungen, Konfigurationsdaten usw.)

Wichtig: Ein Microsoft Geschäftsinhaber kann die Teilnahme an Daten verlangen, die nicht in dieser Liste enthalten sind.

Datenverarbeitungsprofil

Microsoft-Lieferanten haben die Kontrolle über ihr SSPA-Datenverarbeitungsprofil.

Dies erlaubt es den Lieferanten, zu entscheiden, welche Aufträge sie durchführen möchten. Achten Sie sorgfältig auf die Auswahl und berücksichtigen Sie die Compliance-Aktivitäten, die zur Erlangung der Genehmigung durchgeführt werden müssen. **Siehe den folgenden Abschnitt „Anforderungen an die Zusicherung“ und Anhang A.**

Microsoft Geschäftsgruppen können nur dann Aufträge mit Lieferanten erstellen, wenn die Datenverarbeitungsaktivität mit den Genehmigungen übereinstimmt, die der Lieferant erhalten hat.

Lieferanten können ihr Datenverarbeitungsprofil jederzeit im Laufe des Jahres aktualisieren, **wenn es keine unerledigten Aufgaben gibt**. Wenn eine Änderung vorgenommen wird, wird die entsprechende Aktivität ausgegeben und muss abgeschlossen werden, bevor die Genehmigungen gesichert sind. Die bestehenden, abgeschlossenen Genehmigungen gelten so lange, bis die neu ausgegebenen Anforderungen erfüllt sind.

Wenn die neu ausgeführten Aufgaben nicht innerhalb des erlaubten Zeitrahmens von 90 Tagen abgeschlossen werden, wechselt der SSPA-Status auf Rot (nicht konform), und das Konto läuft Gefahr, aus den Microsoft-Kreditorenbuchhaltungssystemen deaktiviert zu werden.

Genehmigungen für die Datenverarbeitung	
1	Umfang der Datenverarbeitung ▪ Vertraulich ▪ Persönlich, vertraulich
2	Ort der Datenverarbeitung ▪ Bei Microsoft oder beim Kunden ▪ Bei einem Lieferanten
3	Rolle der Datenverarbeitung ▪ Steuergerät (Unabhängiger oder gemeinsamer Controller) ▪ Prozessor ▪ Unterauftragsverarbeiter (von Microsoft benannt)
4	Verarbeitung von Zahlungskarten ▪ Ja ▪ Nicht zutreffend
5	Software as a Service ▪ Ja ▪ Nicht zutreffend
6	Einsatz von Unterauftragnehmern ▪ Ja ▪ Nicht zutreffend

Überlegungen zur Genehmigung

Umfang der Datenverarbeitung

Vertraulich

Wählen Sie diese Genehmigung, wenn die Leistung des Lieferanten nur die Verarbeitung vertraulicher Daten von Microsoft umfasst.

Wenn Sie diese Genehmigung wählen, sind Sie nicht für die Verarbeitung personenbezogener Daten zugelassen.

Persönlich, vertraulich

Wählen Sie diese Genehmigung, wenn die Leistung des Lieferanten die Verarbeitung personenbezogener Daten und vertraulicher Daten von Microsoft umfasst.

Ort der Verarbeitung

Bei Microsoft oder beim Kunden

Wählen Sie diese Genehmigung, wenn die Leistung des Lieferanten die Verarbeitung von Daten innerhalb der Microsoft-Netzwerkumgebung umfasst, in der Mitarbeiter *@microsoft.com*-Zugangsdaten verwenden, oder innerhalb der Umgebung eines Microsoft-Kunden.

Wählen Sie diese Option unter diesen Umständen nicht:

- Der Lieferant verwaltet eine von Microsoft benannte Offshore-Einrichtung (OF).
- Der Lieferant stellt Microsoft Ressourcen zur Verfügung, die zeitweise innerhalb und außerhalb des Microsoft-Netzwerks arbeiten. Das Verfahren für die Arbeit außerhalb des Netzwerks wird als „beim Lieferanten" betrachtet.

Bei einem Lieferanten
Wenn die Bedingung „Bei Microsoft oder beim Kunden" (wie oben beschrieben) nicht zutrifft, wählen Sie diese Option.

_____

Rolle der Datenverarbeitung

Controller (umfasst unabhängige und gemeinsame Controller)

Wählen Sie diese Genehmigung, wenn **alle** Aspekte der Leistung durch den Lieferanten die Definition der Rolle des Controllers bei der Datenverarbeitung erfüllen (siehe DPR).

Wenn Sie diese Genehmigung wählen, sind Sie nicht für die Verarbeitung personenbezogener Daten mit der Rollenbezeichnung „Verarbeiter" zugelassen. Wenn der Lieferant sowohl ein Verarbeiter als auch ein Steuergerät für Microsoft ist, wählen Sie nicht „Controller", sondern „Verarbeiter".

Prozessor

Dies ist die häufigste Verarbeitungsrolle, wenn Lieferanten Daten im Auftrag von Microsoft verarbeiten. Bitte lesen Sie die Definition von Verarbeiter in den DPR.

Unterauftragsverarbeiter

Ein Unterauftragsverarbeiter ist eine Drittpartei, die Microsoft mit einer Leistung beauftragt, wobei die Leistung die Verarbeitung personenbezogener Daten von Microsoft umfasst, für die Microsoft ein Auftragsverarbeiter ist. Lieferanten können sich nicht selbst als Unterauftragsverarbeiter bei Microsoft ausweisen, da dies eine vorherige Genehmigung durch interne Datenschutzteams erfordert. Lieferanten können nur dann Unterauftragsverarbeiter sein, wenn Microsoft der Datenverarbeiter ist und der Lieferant qualifizierte personenbezogene Daten des Unternehmens verarbeitet. Für Unterauftragsverarbeiter gelten zusätzliche Vertrags- und Compliance-Anforderungen, einschließlich eines Datenschutzzusatzes und einer unabhängigen Bewertung (siehe unten).

Verarbeitung von Zahlungskarten

Wählen Sie diese Genehmigung, wenn ein Teil der vom Lieferanten verarbeiteten Daten Daten zur Unterstützung von Kreditkarten- oder anderen Zahlungskartenverfahren im Auftrag von Microsoft enthält.

Diese Genehmigung erlaubt es einem Lieferanten, sich an der Verarbeitung von Zahlungskarten zu beteiligen.

Software

Microsoft Procurement leitet Einkäufer bei allen Softwarekäufen durch ein Verfahren, das verschiedene Überprüfungen beinhaltet, darunter auch eine SSPA-Triage, um zu entscheiden, ob der Lieferant der Software für die SSPA-Verwaltung in Frage kommt. (Microsoft-Einkäufer können die Schritte auf der internen Seite ProcureWeb Software and Cloud Service nachlesen, um weitere Einzelheiten zu erfahren). Wenn SSPA erforderlich ist, müssen die Lieferanten möglicherweise auch angeben, dass das Profil „Software as a Service“ (SaaS) ausgewählt wurde. Für in SSPA registrierte Lieferanten kann dies beim Ausfüllen des Datenverarbeitungsprofils im Microsoft Supplier Compliance Portal geschehen.

Für die Zwecke der SSPA-Compliance sollten Sie SaaS im weitesten Sinne betrachten und auch Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) einbeziehen. (Um mehr über SaaS zu erfahren, lesen Sie bitte diese Erläuterung.)

Software as a Service (SaaS)

Software as a Service (SaaS) erlaubt es Benutzern, sich über das Internet mit Cloud-basierten Anwendungen zu verbinden und diese zu nutzen.

Microsoft definiert **Software as a Service** (SaaS) als Software, die auf einem gemeinsamen Code basiert und in einem One-to-Many-Modell auf Grundlage von Pay-for-Use oder als Abonnement auf der Grundlage von Nutzungskennzahlen verwendet wird. Der Cloud-Service-Anbieter entwickelt und pflegt Cloud-basierte Software, bietet automatische Software-Updates an und stellt seinen Kunden die Software über das Internet auf Grundlage von One-to-Many zur Verfügung, die nach Bedarf abgerechnet wird. Diese Methode der Softwarebereitstellung und -lizenzierung erlaubt den Online-Zugriff auf die Software über ein Abonnement, anstatt sie zu kaufen und auf jedem einzelnen Computer zu installieren.

Hinweis: Die meisten SaaS-Lieferanten müssen im Microsoft Supplier Compliance Portal die Genehmigung für Unterauftragnehmer hinzufügen, wenn die personenbezogenen Daten oder vertraulichen Daten von Microsoft auf einer Plattform eines Drittanbieters gehostet werden.

Einsatz von Unterauftragnehmern

Wählen Sie diese Genehmigung, wenn der Lieferant Unterauftragnehmer einsetzt (siehe DPR für Definitionen).

Dies schließt auch Freiberufler ein (siehe DPR).

Zusicherungsanforderungen

Anforderungen basierend auf Profilgenehmigungen

Die in Ihrem Datenverarbeitungsprofil ausgewählten Genehmigungen helfen SSPA bei der Bewertung des Risikoniveaus für den/die Auftrag/Aufträge von Microsoft. Die SSPA-Compliance-Anforderungen unterscheiden sich je nach Datenverarbeitungsprofil und den damit verbundenen Genehmigungen. In diesem Abschnitt werden die verschiedenen SSPA-Anforderungen erläutert.

Es gibt auch Kombinationen, die die Compliance-Anforderungen erhöhen oder verringern können. Die Kombinationen sind in Anhang A aufgeführt, und dies ist das, was Sie erwarten können, wenn Sie Ihr Profil im Microsoft Supplier Compliance Portal ausfüllen. Sie können jederzeit überprüfen, wie Ihr Szenario in diesen Rahmen passt, indem Sie eine Überprüfung durch ein SSPA-Team beantragen.

Aktion: Suchen Sie Ihr Genehmigungsprofil in Anhang A und prüfen Sie die entsprechenden Anforderungen und Optionen für die unabhängige Überprüfung, falls zutreffend.

Wichtig: Wenn Ihr Profil Software as a Service (SaaS), Unterauftragnehmer, Website-Hosting oder Zahlungskarten umfasst, sind zusätzliche Zusicherungen erforderlich.

Selbstbescheinigung für die DPR

Alle beim SSPA angemeldeten Lieferanten müssen innerhalb von 90 Tagen nach Erhalt der Aufforderung eine Selbstauskunft an die DPR über die Einhaltung der Anforderungen abgeben. Diese Aufforderung erfolgt jährlich, kann aber auch häufiger erfolgen, wenn das Datenverarbeitungsprofil zur Jahresmitte aktualisiert wird. Lieferantenkonten wechseln in den SSPA-Status Rot (nicht konform), wenn die 90-Tage-Frist überschritten wird. Neue Bestellungen, die in den Geltungsbereich fallen, können erst dann verfahren werden, wenn der SSPA-Status auf Grün (konform) wechselt.

Neu registrierte Lieferanten müssen die gestellten Anforderungen erfüllen, um den SSPA-Status Grün (konform) zu erhalten, bevor sie mit der Auftragsvergabe beginnen können.

Wichtig: Das SSPA-Team ist nicht berechtigt, diese Aufgabe zu verlängern.

Autorisierte Vertreter, die die Selbstauskunft ausfüllen werden, sollten sicherstellen, dass sie über ausreichende Informationen von Fachexperten verfügen, um jede Anforderung zuverlässig beantworten zu können. Mit der Unterzeichnung eines SSPA-Formulars bestätigen sie zudem, dass sie die Datenschutzbestimmungen gelesen und verstanden haben. Lieferanten können dem Online Werkzeug weitere Kontakte hinzufügen, die sie beim Ausfüllen der Anforderungen unterstützen.

Der autorisierte Vertreter (Definition siehe DPR) hat folgende Aufgaben:

1. Bestimmen, welche Anforderungen zutreffen.
2. Eine Antwort auf jede zutreffende Anforderung einstellen.
3. Die Bescheinigung im Microsoft Supplier Compliance Portal unterschreiben und übermitteln.

Geltungsbereich

Von den Lieferanten wird erwartet, dass sie alle anwendbaren DPR-Anforderungen erfüllen, die im Rahmen des Datenverarbeitungsprofils gestellt werden. Es ist zu erwarten, dass einige der Anforderungen nicht auf die Waren oder Dienstleistungen zutreffen, die der Lieferant für Microsoft bereitstellt. Diese können mit dem Vermerk „trifft nicht zu“ und einem detaillierten Kommentar versehen werden, den die SSPA-Prüfer dann validieren können.

Die DPR-Anträge werden vom SSPA-Team daraufhin überprüft, ob die Markierungen „trifft nicht zu“, „lokaler rechtlicher Konflikt“ oder „vertraglicher Konflikt“ auf die gestellten Anforderungen zutreffen. Das SSPA-Team kann um eine Klärung einer oder mehrerer Markierungen bitten. Lokale rechtliche und vertragliche Konflikte werden nur dann akzeptiert, wenn entsprechende Referenzen vorgelegt werden und der Konflikt eindeutig ist.

Unabhängige Bewertungsanforderung

Bitte sehen Sie sich die Anforderungen nach Genehmigungen in Anhang A an, um die Genehmigungen für die Datenverarbeitung einzusehen, die diese Anforderung auslösen.

Lieferanten haben die Möglichkeit, Genehmigungen zu ändern, indem sie ihr Datenverarbeitungsprofil aktualisieren. Wenn der Lieferant jedoch die Datenverarbeitungsrolle „Unterauftragsverarbeiter“ hat, kann er diese Genehmigung nicht ändern und ist verpflichtet, jährlich eine unabhängige Bewertung durchführen zu lassen.

Um die Genehmigungen zu erhalten, die eine unabhängige Überprüfung der Einhaltung der Vorschriften erfordern, müssen die Lieferanten einen unabhängigen Prüfer auswählen, der die Einhaltung der DPR überprüft. Der Prüfer erstellt ein Beratungsschreiben, in dem er Microsoft die Einhaltung der Bestimmungen zusichert. Dieses Schreiben muss uneingeschränkt sein, und alle nicht konformen Probleme müssen gelöst und behoben werden, bevor das Bestätigungsschreiben zur Überprüfung durch das SSPA-Team an das Microsoft Supplier Compliance Portal übermittelt wird. Prüfer können eine Vorlage für ein genehmigtes Beratungsschreiben herunterladen, die der PDF-Datei „Bevorzugte Prüfer“ beigefügt ist, die Sie hier finden.

Anhang A enthält akzeptable Zertifizierungsalternativen für den Fall, dass Sie sich nicht für einen unabhängigen Prüfer entscheiden, um die Einhaltung der DPR zu überprüfen (falls zutreffend, z.B. für SaaS-Lieferanten, Website-Hosting-Lieferanten oder Lieferanten mit Unterauftragnehmern). Die ISO 27701 (Datenschutz) und die ISO 27001 (Sicherheit) werden als eng mit den DPR übereinstimmend angesehen.

Handelt es sich bei dem Lieferanten um einen Gesundheitsdienstleister in den Vereinigten Staaten oder um eine betroffene Einrichtung, akzeptieren wir hinsichtlich Datenschutz und Sicherheit einen HITRUST-Bericht.

SSPA kann eine unabhängige Bewertung manuell durchführen, wenn Umstände, die über die Standardauslöser hinausgehen, eine zusätzliche Überprüfung gemäß Sorgfaltspflicht erfordern. Beispiele hierfür sind eine Anfrage der Datenschutz- oder Sicherheitsabteilung, die Validierung der

Behebung von Datenvorfällen oder die Forderung nach einer automatisierten Umsetzung der Rechte der betroffenen Personen.

Anleitung, wie diese Anforderung zu erfüllen ist:

1. Der Auftrag ist von einem Prüfer durchzuführen, der über eine ausreichende technische Ausbildung und Fachkenntnisse verfügt, um die Einhaltung der Vorschriften angemessen beurteilen zu können.
2. Die Prüfer müssen der International Federation of Accountants (IFAC) oder dem American Institute of Certified Public Accountants (AICPA) angeschlossen sein oder über Zertifizierungen anderer einschlägiger Datenschutz- und Sicherheitsorganisationen verfügen, wie der International Association of Privacy Professionals (IAPP) oder der Information Systems Audit and Control Association (ISACA).
3. Der Prüfer muss die aktuellste DPR verwenden, die die erforderlichen Nachweise für jede Anforderung enthält. **Die Lieferanten müssen dem Prüfer die Antworten ihrer zuletzt genehmigten DPR-Bescheinigung vorlegen.**
4. Im Fall eines neu registrierten Lieferanten wird der Prüfer die Gestaltung der Verfahrenskontrollen testen. In allen anderen Fällen überprüft der Prüfer die Wirksamkeit der Kontrollen.
5. Der Umfang des Prüfauftrags ist auf personenbezogene Daten und/oder vertrauliche Daten von Microsoft im Zusammenhang mit der Leistung des Lieferanten beschränkt.
6. Der Umfang der Prüfung beschränkt sich auf alle Datenverarbeitungsaktivitäten, die unter der Kontonummer des Lieferanten durchgeführt werden, der die Anfrage erhalten hat. Wenn sich der Lieferant für mehr als ein Lieferantenkonto gleichzeitig entscheidet, **muss das Bescheinigungsschreiben die Liste der Lieferantenkonten, die in die Bewertung einbezogen sind, und die zugehörigen Adressen enthalten.**
7. Das bei SSPA eingereichte Schreiben darf keine Angaben enthalten, bei denen der Lieferant die Datenschutzanforderungen in der vorliegenden Form nicht erfüllen kann. Diese Probleme müssen gestimmt werden, bevor das Schreiben eingereicht wird.

Der SSPA hat eine Liste der bevorzugten Prüfer verfügbar gemacht. Diese Unternehmen sind mit der Durchführung von SSPA-Bewertungen vertraut. Von den Lieferanten wird erwartet, dass sie für diese Bewertung bezahlen; die Kosten hängen von der Größe und dem Umfang der Datenverarbeitung ab.

PCI DSS Zertifizierungsanforderung

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein Rahmenwerk für die Entwicklung einer robusten Sicherheit von Zahlungskartendaten, das die Vorbeugung, Erkennung und angemessene Reaktion auf Sicherheitsvorfälle umfasst. Das Rahmenwerk wurde vom PCI Security Standards Council, einem selbstregulierenden Unternehmen der Branche, entwickelt. Der Zweck der PCI DSS-Anforderungen besteht darin, Schwachstellen in Technologien und Verfahren zu identifizieren, die Risiken für die Sicherheit der verarbeiteten Karteninhaberdaten darstellen.

Microsoft ist verpflichtet, diese Standards einzuhalten. Wenn ein Lieferant im Auftrag von Microsoft Zahlungskartendaten verarbeitet, benötigen wir einen Nachweis über die Einhaltung dieser Standards.

Informieren Sie sich im PCI Security Standards Council über die Anforderungen des PCI-Unternehmens.

Je nach Umfang der verarbeiteten Transaktionen muss ein Lieferant entweder die Einhaltung der Anforderungen durch einen qualifizierten Sicherheitsgutachter bescheinigen lassen oder er kann das Formular des Selbsteinschätzung-Fragebogens ausfüllen.

Die Zahlungskartenhersteller legen die Schwellenwerte für die Art der Bewertung fest:

- Stufe 1: Vorlage eines PCI AOC-Zertifikats eines unabhängigen Prüfers
- Stufe 2 oder 3: Vorlage eines PCI DSS Fragebogen zur Selbsteinschätzung (SAQ), der vom Verantwortlichen des Lieferanten unterzeichnet ist.

Einsenden der Zertifizierung, die den PCI-Anforderungen entspricht.

Anforderung Software as a Service

Lieferanten, die die SaaS-Definition im Datenverarbeitungsprofil erfüllen, müssen möglicherweise eine gültige ISO 27001-Zertifizierung vorlegen, wenn dies im Microsoft Cloud Services Agreement gefordert wird.

Die SSPA-Prüfer überprüfen, ob die eingesandten Unterlagen die Vertragsverpflichtung erfüllt.

Bitte reichen Sie keine Rechenzentrum-Zertifizierung ein. Wir erwarten die ISO 27001-Zertifizierung, die für den/die Softwaredienst(e) gilt, die in Ihrem Vertrag mit Microsoft aufgeführt sind.

Einsatz von Unterauftragnehmern

Microsoft betrachtet den Einsatz von Unterauftragnehmern als einen hohen Risikofaktor. Lieferanten, die Unterauftragnehmer einsetzen, die personenbezogene Daten oder vertrauliche Daten von Microsoft verarbeiten, müssen diese Unterauftragnehmer offenlegen. Darüber hinaus sollte der Lieferant auch die Länder angeben, in denen die personenbezogenen Daten von den einzelnen Unterauftragnehmern verarbeitet werden.

Datenvorfälle

Wenn ein Lieferant von einem Datenschutz- oder Sicherheitsvorfall Kenntnis erlangt, muss er Microsoft wie in den DPR beschrieben informieren.

Melden Sie einen Datenvorfall über SupplierWeb oder per E-Mail an SuppIR@microsoft.com.

Geben Sie unbedingt an:

- Datum des Datenvorfalls:
- Lieferantenname:
- Lieferantennummer:
- Benachrichtigte Microsoft Kontaktperson(en):
- Zugehörige PO, falls zutreffend/verfügbar:
- Zusammenfassung des Datenvorfalls:

Anhang A

Anforderungen basierend auf Profilgenehmigungen

Nr.	Profil	Zusicherungsanforderungen	Optionen zur unabhängigen Überprüfung
1	**Umfang**: Persönlich, vertraulich **Ort der Verarbeitung:** Bei Microsoft oder beim Kunden **Verarbeitungsrolle:** Verarbeiter oder Controller **Datenklasse:** Vertraulich **oder** Streng Vertraulich **Zahlungskarten:** Nicht zutreffend **SaaS:** Nicht zutreffend **Einsatz von Unterauftragnehmern:** Nicht zutreffend **Website-Hosting:** Nicht zutreffend	Selbstbescheinigung der Konformität mit DPR	
2	**Umfang:** Vertraulich **Ort der Verarbeitung:** Bei einem Lieferanten **Verarbeitungsrolle:** n. z. **Datenklasse:** Vertraulich **Zahlungskarten:** Nicht zutreffend **SaaS:** Nicht zutreffend **Einsatz von Unterauftragnehmern:** Nicht zutreffend **Website-Hosting:** Nicht zutreffend	Selbstbescheinigung der Konformität mit DPR	

3	**Umfang**: Vertraulich **Ort der Verarbeitung:** Bei einem Lieferanten **Verarbeitungsrolle:** Prozessor **Datenklasse:** Streng vertraulich **Zahlungskarten:** Nicht zutreffend **SaaS:** Nicht zutreffend **Einsatz von Unterauftragnehmern:** Nicht zutreffend **Website-Hosting:** Nicht zutreffend	Selbstbescheinigung der Konformität mit DPR **und** Unabhängige Zusicherung der Einhaltung	Optionen für unabhängige Zusicherungen: 1. Durchführung einer unabhängigen Bewertung anhand der DPR, **oder** 2. ISO 27001-Zertifizierung einreichen

Nr.	Profil	Zusicherungsanforderungen	Optionen zur unabhängigen Überprüfung
4	**Umfang:** Persönlich, vertraulich **Ort der Verarbeitung:** Bei einem Lieferanten **Verarbeitungsrolle:** Prozessor **Datenklasse:** Streng vertraulich **Zahlungskarten:** Nicht zutreffend **SaaS:** Nicht zutreffend **Einsatz von Unterauftragnehmern:** Nicht zutreffend **Website-Hosting:** Nicht zutreffend	Selbstbescheinigung der Konformität mit DPR **und** Unabhängige Zusicherung der Einhaltung	Optionen für unabhängige Zusicherungen: 1. Durchführung einer unabhängigen Bewertung anhand der DPR, 2. Unabhängige Bewertung anhand der Abschnitte A-I der DPR und ISO 27001, **oder** 3. Zertifizierungen nach ISO 27701 **und** ISO 27001 einreichen
5	**Umfang:** Persönlich, vertraulich **Ort der Verarbeitung:** Bei einem Lieferanten **Verarbeitungsrolle:** Prozessor **Datenklasse:** Vertraulich **Zahlungskarten:** Nicht zutreffend **SaaS:** Nicht zutreffend **Einsatz von Unterauftragnehmern:** Nicht zutreffend **Website-Hosting:** Nicht zutreffend	Selbstbescheinigung der Konformität mit DPR	

6	**Umfang:** Persönlich, vertraulich **Ort der Verarbeitung:** Bei einem Lieferanten **Verarbeitungsrolle:** Controller **Datenklasse:** Streng vertraulich oder Vertraulich **Zahlungskarten:** Nicht zutreffend **SaaS:** Nicht zutreffend **Einsatz von Unterauftragnehmern:** Nicht zutreffend **Website-Hosting:** Nicht zutreffend	Selbstbescheinigung der Konformität mit DPR	

Nr.	Profil	Zusicherungsanforderungen	Optionen zur unabhängigen Überprüfung
7	**Umfang:** Persönlich, vertraulich **Ort der Verarbeitung:** Beliebig **Verarbeitungsrolle:** Unterauftragsverarbeiter (Diese Rolle wird von Microsoft festgelegt – das Profil lautet „Unterauftragsverarbeiter-Genehmigung: Ja“) **Datenklasse:** Streng vertraulich oder Vertraulich **Zahlungskarten:** Nicht zutreffend **SaaS:** Nicht zutreffend **Einsatz von Unterauftragnehmern:** Nicht zutreffend **Website-Hosting:** Nicht zutreffend	Selbstbescheinigung der Konformität mit DPR **und** Unabhängige Zusicherung der Einhaltung	Optionen für unabhängige Zusicherungen: 1. Durchführung einer unabhängigen Bewertung anhand der DPR, 2. Unabhängige Bewertung anhand der Abschnitte A-I der DPR und ISO 27001, **oder** 3. Zertifizierungen nach ISO 27701 **und** ISO 27001 einreichen

Nr.	Profil	Zusicherungsanforderungen	Optionen zur unabhängigen Überprüfung
Auswirkungen des Hinzufügens von SaaS, Unterauftragnehmern, Website-Hosting			
8	**Umfang:** Persönlich, vertraulich **Ort der Verarbeitung:** Bei einem Lieferanten **Verarbeitungsrolle:** Prozessor **Datenklasse:** Streng vertraulich oder Vertraulich **Zahlungskarten:** Nicht zutreffend **Unterauftragnehmer:** JA oder **SaaS:** JA oder **Website-Hosting:** JA	Selbstbescheinigung der Konformität mit DPR **und** Unabhängige Zusicherung der Einhaltung	Optionen für unabhängige Zusicherungen: 1. Durchführung einer unabhängigen Bewertung anhand der DPR, 2. Unabhängige Bewertung anhand der Abschnitte A-I der DPR und ISO 27001, **oder** 3. Zertifizierungen nach ISO 27701 **und** ISO 27001 einreichen
9	**Umfang:** Persönlich, vertraulich **Ort der Verarbeitung:** Bei einem Lieferanten **Verarbeitungsrolle:** Controller **Datenklasse:** Streng vertraulich oder Vertraulich **Zahlungskarten:** Nicht zutreffend **Unterauftragnehmer:** JA oder **SaaS:** JA oder **Website-Hosting:** JA	Selbstbescheinigung der Konformität mit DPR	

Nr.	Profil	Zusicherungsanforderungen	Optionen zur unabhängigen Überprüfung
Zusätzliche Zusicherung für Zahlungskarten und SaaS			
10	**Jedes der oben genannten Profile und Zahlungskarten**	Die oben genannten Anforderungen **und** die Zusicherung der Payment Card Industry	PCI DSS-Zertifizierung einreichen
11	Eines der oben genannten Profile und **Software as a Service (SaaS)**	Die oben genannten Anforderungen **und** reichen Sie Ihre vertraglich geforderte ISO 27001-Zertifizierung ein, die die funktionalen Dienste umfasst.	Reichen Sie eine ISO 27001-Zertifizierung mit funktionalem Umfang des/der angebotenen Dienste(s) ein.