Microsoft Tedarik

Tedarikçi Güvenlik ve Gizlilik Güvencesi (SSPA) Programı Kılavuzu

8. Sürüm

Haziran 2022

Giriş

Microsoft olarak gizliliğin temel bir hak olduğuna inanıyoruz. Dünyadaki her kişinin ve kuruluşun daha fazlasını başarmasını sağlama misyonumuz doğrultusunda, her gün müşterilerimizin güvenini kazanmayı ve muhafaza etmeyi amaçlıyoruz.

Güçlü güvenlik ve gizlilik uygulamaları, misyonumuz ve müşterilerin güveni açısından kritik önemde olup, bazı yargı alanlarında kanunen gereklidir. Microsoft gizlilik ve güvenlik politikalarında yer alan standartlar bir şirket olarak değerlerimizi yansıtmakta olup, Microsoft verilerini bizim adımıza işleyen (sizin şirketiniz gibi) tedarikçilerimiz için de geçerlidir.

Tedarikçi Güvenlik ve Gizlilik Güvencesi ("**SSPA**") Programı, Microsoft'un tedarikçilerine yönelik temel veri işleme talimatlarının yerine getirilmesi amacıyla SSPA on Microsoft.com/Procurement. adresinde Microsoft Tedarikçi Veri Koruma Gereksinimleri ("**DPR**") adı altında yürürlüğe konulmuş Microsoft'un kurumsal programıdır. Tedarikçilerin, Microsoft'un tedarikçilerle iletişimden sorumlu birimi tarafından kararlaştırılıp bildirilen ve SSPA kapsamının dışına çıkan kurumsal düzeyde birtakım başka gereksinimlerin de yerine getirmelerinin gerekli olabileceğini dikkate alın.

Önemli SSPA terimleri DPR'da tanımlanmıştır. Program hakkında daha fazla bilgi almak için Sıkça Sorulan Sorular (SSS) bölümüne bakın ve SSPAHelp@microsoft.com adresinden küresel ekibimizle iletişime geçin.

SSPA Programına Genel Bakış

SSPA, tedarikçilerimizin gizlilik ve güvenliğe ilişkin ilkelere uyduklarını temin etmek amacıyla Microsoft Tedarik, Kurumsal Dış ve Hukuki İşler ve Kurumsal Güvenlik birimleri arasında ortaklaşa yürütülen bir programdır.

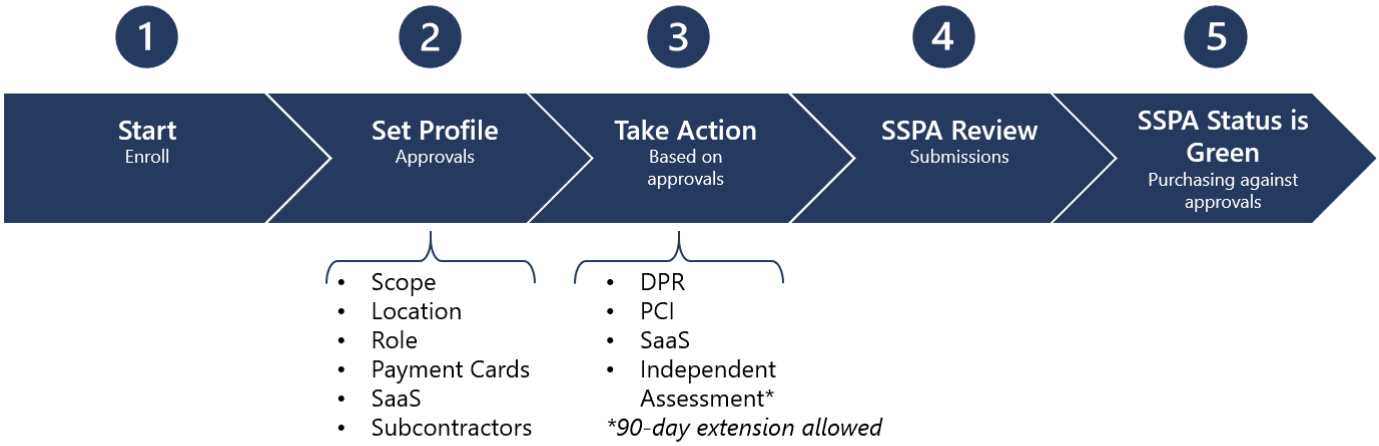
SSPA'nın kapsamına, tedarikçinin Microsoft ile olan sözleşmesinin (ör. Tedarik Sipariş şartları, ana sözleşme) şartları doğrultusunda yükümlülüklerini (ör. hizmetlerin, yazılım lisanslarının, bulut bilişim hizmetlerinin sağlanması) yerine getirmesiyle ("**Yükümlülüğü Yerine Getirme**", "**Yerine Getirme**" veya "**Yükümlülük**") ilgili olarak Kişisel Veriler ve/veya Microsoft Gizli Verilerini işleyen dünya genelindeki tüm tedarikçiler girer.

SSPA tedarikçinin sözleşme gereği Yerine Getirmekle yükümlü olduğu mal ve/veya hizmetlerle uyumlu Veri İşleme Profili seçimleri yapmasına olanak sağlar. Bu seçimler Microsoft'a uyumluluk güvenceleri sağlamaya yönelik ilgili gereksinimlerin devreye girmesini sağlar.

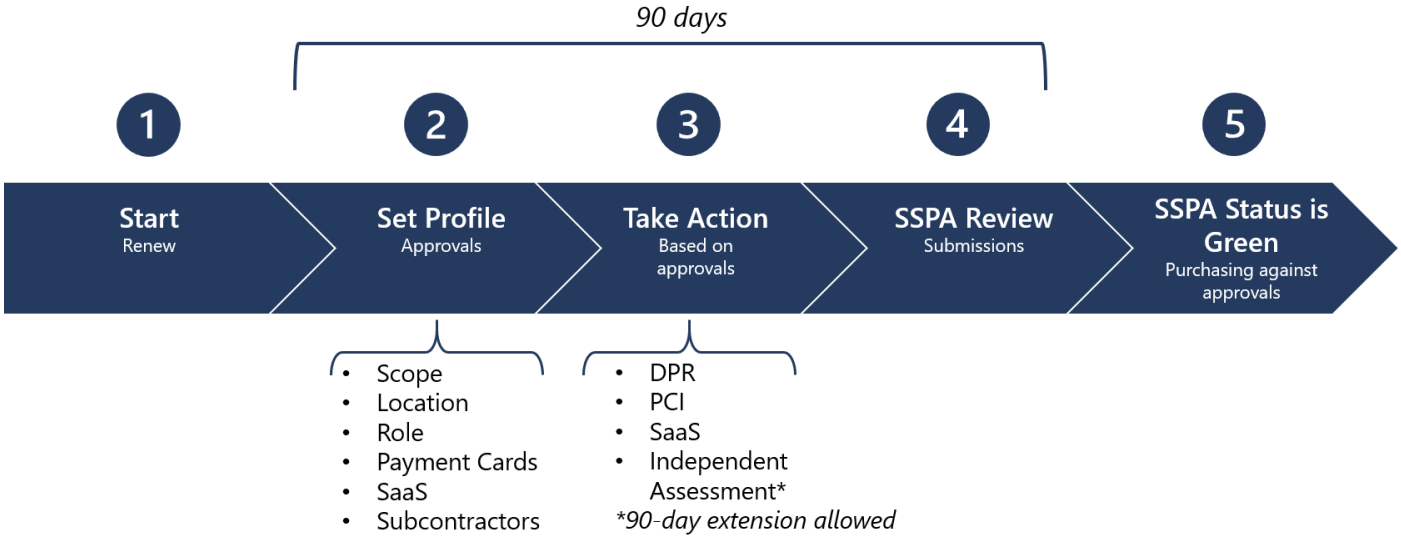
Tüm kayıtlı tedarikçilerin her sene DPR gereksinimlerine uyduklarına dair bir öz tasdik tamamlamaları gerekir. Veri işleme profiliniz, DPR'nin tamamen yayınlanıp yayınlanmadığını veya bazı alt gereksinimlerin geçerli olup olmadığını belirler. Microsoft'un yüksek riskli olduğunu düşündüğü verileri işleyen tedarikçilerin, örneğin bağımsız bir uyumluluk doğrulaması gibi birtakım ekstra gereksinimler yerine getirmesi gerekebilir. Yayımlanmış bir Microsoft Alt İşleyicisi listesinde yer alan tedarikçilerden ayrıca bağımsız bir uyumluluk doğrulaması temin etmeleri istenir.

Önemli: Uyumluluk faaliyetleri sonucunda SSPA durumu Yeşil (uyumlu) veya Kırmızı (uyumsuz) şeklinde belirlenir. Microsoft tedarik araçları, bir işlemin başlatılmasına izin vermeden önce (SSPA kapsamındaki her bir tedarikçinin) SSPA durumunun Yeşil olduğunu doğrular.

SSPA Süreci Şeması – Yeni Tedarikçi Kaydı



SSPA Süreci Şeması – Yıllık Tedarikçi Yenilemesi



SSPA Kapsamı

Tedarikçi olarak Kişisel Veriler ve/veya Microsoft Gizli Verilerini İşleyip İşlemediğinizi belirlemek için aşağıdaki tablolardaki örnekler listesine bakın. Lütfen bunların sadece örnek mahiyetinde olduğunu ve teferruatlı bir liste teşkil etmediğini dikkate alın.

Not: Bir Microsoft işletmesi sahibi, işlenen verilerin gizlilik türünü dikkate alarak bu listenin haricinde birtakım kayıt şartları talep edebilir.

Veri Türüne Göre Kişisel Veriler

Örnekler sınırlama olmaksızın şunları içerir:

Hassas Veriler
Çocuklarla ilgili veriler
Genetik veriler, Biyometrik veriler veya Sağlıkla ilgili veriler
Irksal ve etnik köken
Siyasi, Dini veya felsefi inançlar, düşünceler ve mensubiyetler
Sendika üyeliği
Kişinin cinsel hayatı veya cinsel yönelimi
Göçmenlik durumu (vize, çalışma izni vs.)
Resmi Kimlik Belgeleri (pasaport, ehliyet, vize, sosyal güvenlik numaraları, vatandaşlık numaraları)
Kesin kullanıcı konumu verileri (300 metre dahilinde)
Kişisel banka hesabı numaraları
Kredi kartı numarası ve bitiş tarihi
Müşteri İçeriği Verileri
Belgeler, fotoğraflar, videolar, müzik vs.
Bir ürün veya hizmetle ilgili yapılan değerlendirmeler ve/veya yorumlar
Anket yanıtları
Göz atma geçmişi, ilgi alanları ve favoriler
Mürekkeple oluşturulan içerikler, yazılan yazılar ve sözlü dile getirilen ifadeler (ses ve/veya sohbet/bot)
Kullanıcı kimlik bilgileri (şifreler, şifre ipuçları, kullanıcı adı, kimlik tespiti için kullanılan biyometrik veriler)
Bir destek talebiyle ilişkili müşteri verileri

Yakalanan ve Oluşturulan Veriler
Kesin olmayan konum verileri
IP adresi
Cihaz tercihleri ve kişiselleştirme
Web sitelere yönelik hizmet kullanımı, sayfa tıklama izlemesi
Sosyal medya verileri, sosyal grafik ilişkileri
Fitness monitörleri gibi bağlı cihazlardan gelen aktivite verileri
İsim, adres, telefon numarası, e-posta adresi, doğum tarihi, bağlı kişiler ve acil durumda iletişime geçilecek kişiler gibi irtibat verileri
Dolandırıcılık ve risk değerlendirmesi, geçmiş sorgulaması
Sigorta, emeklilik, haklara ilişkin bilgiler
Adaylara ait özgeçmiş, mülakat notları/geribildirimler
Metadata and telemetry
Hesap Verileri
Ödeme aracı verileri
Kredi kartı numarası ve bitiş tarihi
Banka şube bilgileri
Banka hesabı numarası
Kredi talepleri veya kredi limiti
Vergi belgeleri ve tanımlayıcılar
Yatırım veya masraflarla ilgili bilgiler
Kurumsal kartlar
Nihai Kullanıcıya Ait Anonimleştirilmiş Bilgiler (EUPI) (Microsoft ürün ve hizmetlerinin kullanıcılarını belirlemek amacıyla Microsoft tarafından oluşturulan kimlik tanımlayıcıları)
Genel Benzersiz Tanımlayıcı (GUID)
Pasaport Kullanıcı Kimliği veya Benzersiz Tanımlayıcısı (PUID)
Karma Son Kullanıcı Tanımlanabilir Bilgileri (EUII)
Oturum Kimlikleri
Cihaz Kimlikleri
Tanılama verileri
Günlük verileri

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

Veri Sınıfına göre Microsoft Gizli Verileri

Örnekler sınırlama olmaksızın şunları içerir:

Çok Gizli
Microsoft Ürünlerinin veya Microsoft Ürünlerinin bileşenlerinin geliştirilmesi, test edilmesi veya üretilmesine ilişkin veya bunlarla ilgili bilgiler *Herhangi bir kanalda ticari olarak satılan Microsoft yazılımı, çevrimiçi hizmetleri veya donanımları "**Microsoft Ürünü**" olarak kabul edilir*
Microsoft cihazlarına ilişkin piyasaya sürüm öncesi pazarlama bilgileri
Microsoft'un SEC kurallarına tabi olan kamuoyuna duyurulmamış kurumsal finans verileri
Gizli
Herhangi bir yöntemle dağıtılmak üzere Microsoft adına Microsoft ürün lisans anahtarları
Microsoft dahili İş Kolu (LOB) uygulamalarının geliştirilmesi veya test edilmesine ilişkin veya bunlarla ilgili bilgiler
Office, SQL, Azure vs. gibi Microsoft yazılım ve hizmetlerine ilişkin piyasaya sürüm öncesi Microsoft pazarlama malzemeleri.
Cihazlar gibi Microsoft hizmetleri veya ürünlerine ilişkin yazılı, tasarlanmış, elektronik veya basılı belgeler (süreç veya prosedür kılavuzları, yapılandırma verileri vs.)

Önemli: Bir Microsoft işletmesi sahibi, bu listede bulunmayan başka verilerin de dahil edilmesini talep edebilir.

Veri İşleme Profili

Microsoft tedarikçileri kendi SSPA Veri İşleme Profilleri üzerinde kontrole sahiptir.

Bu, tedarikçilerin hangi işlemleri Yerine Getirmeye uygun olduklarına karar vermelerine olanak sağlar. Yaptığınız seçimlere çok dikkat etmeniz ve onay almak için tamamlanması gereken uyumluluk etkinliğini dikkate almanız gerekir. **Aşağıdaki "Güvence Gereksinimleri" Bölümüne ve Ek A'ya bakın**.

Microsoft işletme grupları, yalnızca veri işleme etkinliğinin tedarikçinin aldığı onayla eşleştiği tedarikçilere yönelik işlemler oluşturabilir.

Tedarikçiler, **açık bir görev olmadığı takdirde** yıl boyunca istedikleri zaman Veri İşleme Profillerini güncelleyebilirler. Bir değişiklik yapıldığında, ilgili etkinlik yayınlanır ve onaylar sağlanmadan önce etkinliğin tamamlanması gerekir. Tamamlanmış mevcut onaylar, yeni yayınlanan gereksinimler tamamlanıncaya kadar geçerli olur.

Yeni gerçekleştirilen görevler izin verilen 90 günlük süre içinde tamamlanmazsa, SSPA durumu Kırmızı (uyumsuz) olur ve hesabın Microsoft Borç Hesapları sistemlerinden devre dışı bırakılma riski söz konusu olur.

Veri İşleme Onayları	
1	Veri İşleme Kapsamı ▪ Gizli ▪ Kişisel, Gizli
2	Veri İşleme Konumu ▪ Microsoft'ta veya Müşteride ▪ Tedarikçide
3	Veri İşleme Görevi ▪ Denetleyici (Bağımsız veya Ortak Denetleyici) ▪ İşleyen ▪ Alt İşleyen (Microsoft tarafından belirlenmiş)
4	Ödeme Kartı İşlemesi ▪ Evet ▪ İlgili Değil
5	Hizmet olarak Yazılım ▪ Evet ▪ İlgili Değil
6	Alt Yüklenici Kullanımı ▪ Evet ▪ İlgili Değil

Onayla İlgili Önemli Noktalar

Veri İşleme Kapsamı

Gizli

Tedarikçinin Yükümlülüğü sadece Microsoft Gizli Verilerinin İşlenmesini içerecekse bu onayı seçin.

Bu onayı seçtiğiniz takdirde Kişisel Veri işleme işlemlerine uygun bulunmazsınız.

Kişisel, Gizli

Tedarikçinin Yükümlülüğü Kişisel Verilerin ve Microsoft Gizli Verilerinin İşlenmesini içerecekse bu onayı seçin.

İşleme Konumu

Microsoft'ta veya Müşteride

Tedarikçinin Yükümlülüğü, personelin *@microsoft.com* erişim bilgilerini kullandığı Microsoft ağı ortamında veya bir Microsoft müşterisinin ortamında verilerin İşlenmesini içeriyorsa bu onayı seçin.

Bu seçeneği şu durumlarda seçmeyin:

- Tedarikçinin Microsoft tarafından belirlenmiş ABD dışında bir tesisi (OF) yönetiyor olması.
- Tedarikçinin Microsoft'a kaynaklar sağlaması ve zaman zaman birlikte Microsoft ağı içinde ve dışında çalışıyor olmaları. Ağ dışında çalışma söz konusu olduğunda işleme konumu "tedarikçide" olarak kabul edilir.

Tedarikçide
Eğer (yukarıda tanımlanan) "Microsoft'ta veya Müşteride" koşulu geçerli değilse bu seçeneği seçin.

_____

Veri İşleme Görevi

Denetleyici (bağımsız ve ortak denetleyicileri içerir)

Tedarikçinin Yükümlülüğünün **tüm** yönleri Denetleyici veri işleme görev tanımına (bkz. DPR) uyuyorsa bu onayı seçin.

Bu onayı seçtiğiniz takdirde 'İşleyen' görev tanımı ile Kişisel Veri işlemesine uygun bulunmazsınız. Tedarikçi, Microsoft adına hem İşleyen hem de Denetleyici konumundaysa 'Denetleyici' yerine İşleyen seçeneğini seçin.

İşleyen

Microsoft adına veri İşleyen tedarikçilere ilişkin en yaygın işleme görevi budur. Lütfen DPR'daki İşleyen tanımını inceleyin.

Alt İşleyen

Alt İşleyen, Microsoft'un İşleyen konumunda olduğu ve Yükümlülüğün Microsoft Kişisel Verilerinin İşlenmesini içerdiği durumlarda Microsoft'un Yükümlülüğü yerine getirmek üzere görevlendirdiği üçüncü taraftır. Tedarikçiler, dahili Gizlilik ekiplerinden ön onay gerektirdiği için kendilerini Microsoft'ta Alt İşleyen olarak tanımlayamazlar. Tedarikçiler ancak Microsoft'un Veri İşleyen konumunda olması ve tedarikçinin Yükümlülüklerinin Kurumsal Kişisel Veri türlerini işlemeye uygun olması halinde Alt İşleyen olabilirler. Alt İşleyenler, bir Veri Koruması Eki ve bir Bağımsız Değerlendirme (aşağıya bakın) de dahil ilave birtakım sözleşme ve uyumluluk gereksinimlerine tabi olurlar.

Ödeme Kartı İşlemesi

Tedarikçi tarafından İşlenen verilerin herhangi bir kısmı Microsoft adına kredi kartı veya başka ödeme kartı işlemesini destekleyecek veriler içeriyorsa bu onayı seçin.

Bu onay, tedarikçinin ödeme kartına ilişkin veri işleme işlemleri yapmasına izin verir.

_____

Yazılım

Microsoft Tedarik, tüm yazılım satın alımlarıyla ilgili olarak Satın Alıcıları bir alım sürecine yönlendirir; bu yazılımı sağlayan tedarikçinin SSPA yönetimi kapsamı dahilinde olup olmadığının belirlenmesine yönelik SSPA öncelik sıralaması da dahil olmak üzere çeşitli denetimleri içerir. (Microsoft Satın Alıcıları daha fazla bilgi için dahili ProcureWeb Yazılım ve Bulut Bilişim Hizmetleri sayfasında belirtilen adımları inceleyebilirler). SSPA'nın gerekli olması halinde tedarikçilerin aynı zamanda 'Hizmet olarak Yazılım' (SaaS) profili seçeneğinin de geçerli olduğunu belirlemeleri gerekebilir. SSPA'ya kayıtlı tedarikçilerle ilgili olarak bu, Microsoft Tedarikçi Uyumluluk Portalındaki Veri İşleme Profili tamamlandığında yapılabilir.

SSPA'ya uyumluluk amacıyla SaaS'ı aynı zamanda daha geniş olarak hizmet olarak platform (PaaS) ve hizmet olarak altyapıyı (IaaS) da içerecek şekilde kabul edin. (SaaS hakkında daha fazla bilgi edinmek için lütfen bu açıklamaya bakın.)

Hizmet olarak Yazılım (SaaS)

Hizmet olarak Yazılım (SaaS) kullanıcıların internette bulut tabanlı uygulamalara bağlanmasını ve bu uygulamaları kullanmasını sağlar.

Microsoft, **Hizmet olarak Yazılımı (SaaS)** kullanım başına ödeme temelinde ve kullanım metriklerine dayalı bir abonelik olarak birden çoğa modelinde kullanılan ortak bir koda dayalı bir yazılım şeklinde tanımlar. Bulut bilişim hizmet sağlayıcısı bulut tabanlı bir yazılım geliştirip sürdürür, otomatik yazılım güncellemeleri sağlar ve yazılımı müşterilerine internet üzerinden birden çoğa, kullandıkça ödeme temelinde sunar. Yazılımın bu yöntemle sunulması ve lisanslanması yazılımın satın alınıp her bir bilgisayara kurulmasından ziyade yazılıma abonelik yoluyla çevrimiçi olarak erişilmesini sağlar.

Not: Çoğu SaaS tedarikçisi, Kişisel Verilerin veya Microsoft Gizli Verilerinin bir 3. taraf platformunda barındırılıyor olması durumunda Microsoft Tedarikçi Uyumluluk Portalında Alt Yüklenicinin onayı eklemek zorundadır.

Alt Yüklenici Kullanımı

Tedarikçi veri İşlemek için Alt Yüklenici kullanıyorsa bu onayı seçin (tanımlar için DPR'a bakın).

Serbest Meslek Mensupları da bu kapsama dahildir (bkz. DPR).

Güvence Gereksinimleri

Profil Onaylarına dayalı gereksinimler

Veri İşleme Profilinizde seçtiğiniz onaylar, Microsoft'a ilişkin gerçekleştireceğiniz veri işleme işlemlerinin risk düzeyinin değerlendirilmesinde SSPA'ya yardımcı olur. SSPA uyumluluk gereksinimleri

Veri İşleme Profiline ve ilgili onaylara bağlı olarak farklılık gösterir. Bu bölümde farklı SSPA gereksinimleri açıklanmaktadır.

Uyumluluk gereksinimlerini artırabilecek veya azaltabilecek kombinasyonlar da söz konusudur. Bu kombinasyonlar Ek A'da ele alınmıştır ve profilinizi tamamladığınızda Tedarikçi Uyumluluk Portalında gerçekleştirmeyi bekleyebileceğiniz şey budur. SSPA ekibi tarafından bir inceleme yapılmasını talep ederek, senaryonuzun bu çerçeve içindeki yerini dilediğiniz zaman doğrulayabilirsiniz.

Eylem: Ek A'daki onay profilinizi bulun ve eğer mevcutsa ilgili güvence gereksinimlerini ve Bağımsız Güvence seçeneklerini inceleyin.

Önemli: Profilinizde Hizmet olarak Yazılım (SaaS), Alt yükleniciler, web sitesi barındırma ya da ödeme kartları seçenekleri yer alıyorsa ilave güvence sağlanması gerekir.

DPR'a İlişkin Öz Tasdik

SSPA'ya kayıtlı tüm tedarikçilerin, ilgili talebi aldıktan 90 gün içinde DPR ile uyumluluğa ilişkin bir öz tasdik gerçekleştirmesi gerekir. Bu talep yılda bir kez yapılır, ancak Veri İşleme Profili yıl ortasında güncellenirse daha da sık yapılabilir. 90 günlük süre aşılırsa tedarikçi hesaplarının SSPA durumu Kırmızı (uyumsuz) hale gelir. SSPA durumunuz Yeşil (uyumlu) olarak değişinceye kadar yeni kapsam içi satın alma siparişleri işlenemez.

Veri işleme işlemlerinin başlayabilmesi için yeni kaydolan tedarikçilerin Yeşil (uyumlu) SSPA durumu sağlamak üzere yayımlanan gereksinimleri yerine getirmeleri gerekir.

Önemli: SSPA ekibinin bu görev için tanınan süreyi uzatma yetkisi yoktur.

Öz tasdik işlemini tamamlayacak yetkili temsilcilerin her bir gereksinimi güvenle yanıtlayabilmek için konu uzmanlarından yeterli bilgi edinmeleri gerekir. Ayrıca bir SSPA formuna adlarını eklediklerinde DPR'ı okuduklarını ve anladıklarını onaylamış olurlar. Tedarikçiler gereksinimleri yerine getirmeye yardımcı olmaları için çevrimiçi araca başka kişiler ekleyebilirler.

Yetkili Temsilci (tanım için DPR'a bakın):

1. Hangi gereksinimlerin geçerli olduğunu belirler.
2. İlgili gereksinimlerin her biri için bir yanıt verir.
3. Tasdik belgesini Microsoft Tedarikçi Uyumluluk Portalında imzalayıp ibraz eder.

Uygulanabilirlik

Tedarikçilerden Veri İşleme Profili için yayımlanan tüm ilgili DPR gereksinimlerine yanıt vermeleri beklenir. Yayımlanan gereksinimlerden birkaçının, tedarikçinin Microsoft'a sağladığı mal veya hizmetler için geçerli olmayacağı beklenir. Bunlar, SSPA hakemlerinin onaylaması için ayrıntılı bir yorum ile 'geçerli değil' şeklinde işaretlenebilir.

DPR gönderimleri, yayımlanan gereksinimler doğrultusunda "geçerli değil", "yerel yasalarla ihtilaf" veya "sözleşme ihtilafı" seçimlerinin yapılıp yapılmadığının anlaşılması için SSPA ekibi tarafından incelenir. SSPA ekibi bir veya daha fazla seçimle ilgili açıklama isteyebilir. Yerel

yasalarla ve sözleşmeyle olan ihtilaflar ancak destekleyici referanslar sağlanmışsa ve ihtilaf belirli ise kabul edilir.

Bağımsız Değerlendirme Gereksinimi

Bu gereksinimi tetikleyen veri işleme onaylarını görmek için lütfen Ek A'daki Onaylara Göre Gereksinimler bölümüne bakın.

Tedarikçiler, Veri İşleme Profillerini güncelleyerek onayları değiştirme seçeneğine sahiptir. Bununla birlikte tedarikçi Veri İşleme Görevini "Alt İşleyen" sıfatıyla gerçekleştiriyorsa bu onayı değiştiremez ve kendisinden her sene bir Bağımsız Değerlendirme yaptırması istenir.

Bağımsız bir uyumluluk doğrulaması gerektiren onayları almak için tedarikçilerin DPR ile uyumluluğu doğrulamak üzere bağımsız bir değerlendirici seçmeleri gerekecektir. Değerlendirici, Microsoft'a uyumluluk güvencesi sağlamak için bir tavsiye mektubu hazırlar. Bu mektubun koşulsuz olması ve onay mektubu SSPA ekibinin incelemesi için Microsoft Tedarikçi Uyumluluk Portalına gönderilmeden önce uyumsuzlukla ilgili tüm konuların çözülüp düzeltilmesi gerekir. Değerlendiriciler, "Tercih Edilen Değerlendiriciler" PDF belgesine eklenmiş onaylı tavsiye mektubu şablonunu buradan indirebilirler.

DPR ile uyumluluğu doğrulamak için bağımsız bir değerlendirici kullanmamayı tercih ettiğiniz takdirde kabul edilebilir sertifika alternatiflerini **Ek A'**da görebilirsiniz (ilgili olması halinde örneğin SaaS tedarikçileri, web sitesi barındırma tedarikçileri veya Alt Yüklenicili tedarikçiler için). ISO 27701 (gizlilik) ve ISO 27001 (güvenlik) sertifikaları kapsam olarak DPR'a yakın olduğu için bu standartlar dikkate alınır.

Tedarikçinin Amerika Birleşik Devletleri'nde bir sağlık hizmetleri sağlayıcısı veya kapsam dahilinde bir kuruluş olması halinde gizlilik ve güvenlik kapsamı açısından HITRUST raporunu kabul ederiz.

Standart tetikleyicilerin ötesine geçen şartların ekstra kapsamlı bir inceleme yapılmasını gerektirmesi halinde SSPA manuel olarak bağımsız bir değerlendirme yürütebilir. Bu şartlara örnek olarak gizlilik veya güvenlik biriminden gelen bir talep, veri olayı düzeltmesinin doğrulanması veya otomatik veri sahibi haklarının kullanılması verilebilir.

Bu gereksinimin yerine getirilmesine ilişkin yol gösterici ilkeler:

1. İşlemin uyumluluğu uygun şekilde değerlendirmek için yeterli teknik eğitim ve bilgiye sahip bir değerlendirici tarafından gerçekleştirilmesi gerekir.
2. Değerlendiricilerin Uluslararası Muhasebeciler Federasyonu (IFAC) veya Amerikan Yeminli Mali Müşavirler Enstitüsü (AICPA) üyesi olmaları veya Uluslararası Gizlilik Uzmanları Derneği (IAPP) veya Bilgi Sistemleri Denetim ve Kontrol Derneği (ISACA) gibi gizlilik ve güvenlikle ilgili diğer kuruluşlardan sertifika almış olmaları gerekmektedir.
3. Değerlendiricinin, her bir gereksinimi desteklemek için gerekli kanıtı içeren en güncel DPR'ı kullanması gerekir. **Tedarikçilerin en son onaylı DPR tasdik yanıtlarını değerlendiriciye sunmaları gerekir.**
4. Eğer tedarikçi yeni kaydolmuşsa değerlendirici süreç kontrollerinin tasarımını test edecektir. Diğer tüm durumlarda, değerlendirici kontrollerin etkinliğini test edecektir.

5. Değerlendirme işleminin kapsamı, söz konusu tedarikçinin Yükümlülüğü ile bağlantılı olarak Kişisel Veriler ve/veya Microsoft Gizli Verileri ile sınırlıdır.
6. İşlemin kapsamı, talebi alan tedarikçi hesap numarasıyla yürütülen tüm kapsam içi veri işleme etkinlikleri ile sınırlıdır. Tedarikçinin tek seferde birden fazla tedarikçi hesabı seçmesi halinde **tasdik mektubunun değerlendirmeye dahil olan tedarikçi hesaplarının ve ilişkili adreslerin listesini içermesi gerekir**.
7. SSPA'ya gönderilen mektupta yazılı olarak tedarikçinin Veri Koruma Şartlarını yerine getiremediğine ilişkin beyanlar bulunmamalıdır. Mektup gönderilmeden önce bu sorunların düzeltilmesi gerekir.

SSPA'nın hazırlamış olduğu tercih edilen değerlendiricilerin listesine buradan ulaşabilirsiniz. Bu şirketler SSPA değerlendirmeleri konusunda deneyimlidir. Tedarikçilerin bu değerlendirme için ödeme yapması gerekir; maliyet, veri işlemenin boyut ve kapsamına bağlı olarak değişiklik gösterir.

PCI DSS Sertifikası Gereksinimi

Ödeme Kartı Sektör Veri Güvenliği Standardı (PCI DSS), güvenlik ihlallerini önlemeyi, tespit etmeyi ve bunlara gerekli müdahalelerde bulunmayı amaçlayan sağlam bir ödeme kartı veri güvenliği tedbirleri geliştirmeye yönelik bir çerçevedir. Çerçeve, sektöre ilişkin bir özdenetim kuruluşu olan PCI Güvenlik Standartları Konseyi tarafından hazırlanmıştır. PCI DSS gereksinimlerinin amacı, işlenen kart sahibi verilerinin güvenliğini riske atabilecek teknolojileri ve işleme aşamasındaki güvenlik açıklarını belirlemektir.

Microsoft'un bu standartlara uyması gerekir. Bir tedarikçinin Microsoft adına ödeme kartı bilgilerini işlemesi halinde bu standartlara uyulduğuna dair kanıt isteriz. PCI kuruluşunun belirlediği gereksinimleri anlamak için PCI Güvenlik standartları konseyine danışın.

Yapılan işlemlerin hacmine bağlı olarak tedarikçiden ya Kalifiye bir Güvenlik Değerlendiricisine uyumluluk denetimi yaptırması ya da bir öz değerlendirme anket formu doldurması istenir.

Ödeme kartı markaları, değerlendirme türü eşiklerini genellikle şu şekilde belirler:

- 1. Seviye: Bir 3. Taraf Değerlendirici PCI AOC sertifikası temin edilmelidir
- 2. veya 3. Seviye: Tedarikçinin görevlisi tarafından imzalanmış bir PCI DSS Öz Değerlendirme Anketi (SAQ) temin edilmelidir.

PCI gereksinimlerine uyan ve bu gereksinimleri karşılayan sertifikayı sunun.

Hizmet olarak Yazılım Gereksinimi

Veri İşleme Profilinde SaaS tanımına uyan tedarikçilerin, Microsoft Bulut Bilişim Hizmetleri Sözleşmesinde istendiği takdirde geçerli bir ISO 27001 sertifikası sunması gerekli olabilir.

SSPA değerlendiricileri, gönderinizin sözleşme yükümlülüğünü yerine getirdiğini doğrulayacaktır.

Lütfen bir veri merkezi sertifikası sunmayın. ISO 27001 sertifikasının Microsoft ile olan sözleşmenizde belirtilen yazılım hizmet(ler)i için geçerli olmasını bekleriz.

Alt Yüklenici Kullanımı

Microsoft alt yüklenici kullanımını yüksek bir risk faktörü olarak kabul eder. Kişisel ve/veya Microsoft Gizli Verilerini işleyecek alt yükleniciler kullanan tedarikçilerin söz konusu verileri alt yüklenicilere açıklaması gerekir. Tedarikçinin ayrıca her bir alt yüklenicinin söz konusu kişisel verileri hangi ülkelerde işleyeceğini de açıklaması gerekir.

Veri İhlalleri

Tedarikçinin verilerin gizliliği veya güvenliğine ilişkin bir ihlalin farkına varması halinde bunu DPR'da belirtildiği ve tanımlandığı şekilde Microsoft'a bildirmesi gerekir.

SupplierWeb adresinden veya SuppIR@microsoft.com adresine e-posta göndererek veri ihlali bildiriminde bulunun

Bildiriminizde şu bilgileri eklediğinizden emin olun:

- Veri İhlalinin Tarihi:
- Tedarikçinin Adı:
- Tedarikçi Numarası:
- Haber Verilen Microsoft İrtibat Kişisi/Kişileri:
- İlgiliyse/mevcutsa ilişkili PO:
- Veri İhlalinin Özeti:

Ek A

Profil Onaylarına dayalı gereksinimler

#	Profil	Güvence Gereksinimleri	Bağımsız Güvence Seçenekleri
1	**Kapsam:** Kişisel, Gizli **İşleme Konumu:** Microsoft'ta veya Müşteride **İşleme Görevi:** İşleyen veya Denetleyici **Veri Sınıfı:** Gizli veya Çok Gizli **Ödeme Kartları:** İlgili Değil **SaaS:** İlgili Değil **Alt Yüklenici Kullanımı:** İlgili Değil **Web Sitesi Barındırma:** İlgili Değil	DPR ile uyumluluğa ilişkin öz tasdik	
2	**Kapsam:** Gizli **İşleme Konumu:** Tedarikçide **İşleme Görevi:** Yok **Veri Sınıfı:** Gizli **Ödeme Kartları:** İlgili Değil **SaaS:** İlgili Değil **Alt Yüklenici Kullanımı:** İlgili Değil **Web Sitesi Barındırma:** İlgili Değil	DPR ile uyumluluğa ilişkin öz tasdik	
3	**Kapsam:** Gizli **İşleme Konumu:** Tedarikçide **İşleme Görevi:** İşleyen **Veri Sınıfı:** Çok Gizli **Ödeme Kartları:** İlgili Değil **SaaS:** İlgili Değil **Alt Yüklenici Kullanımı:** İlgili Değil **Web Sitesi Barındırma:** İlgili Değil	DPR ile uyumluluğa ilişkin öz tasdik **ve** Bağımsız Uyumluluk Güvencesi	Bağımsız Güvence seçenekleri: 1. DPR'a uyumla ilgili Bağımsız bir Değerlendirme gerçekleştirin **veya** 2. ISO 27001 sertifikası sunun

#	Profil	Güvence Gereksinimleri	Bağımsız Güvence Seçenekleri
4	**Kapsam:** Kişisel, Gizli **İşleme Konumu:** Tedarikçide **İşleme Görevi:** İşleyen **Veri Sınıfı:** Çok Gizli **Ödeme Kartları:** İlgili Değil **SaaS:** İlgili Değil **Alt Yüklenici Kullanımı:** İlgili Değil **Web Sitesi Barındırma:** İlgili Değil	DPR ile uyumluluğa ilişkin öz tasdik **ve** Bağımsız Uyumluluk Güvencesi	Bağımsız Güvence seçenekleri: 1. DPR'a uyumla ilgili Bağımsız bir Değerlendirme, 2. DPR'ın A-I bölümleri ve ISO 27001 standardına uyumla ilgili Bağımsız bir Değerlendirme gerçekleştirin **veya** 3. ISO 27701 **ve** ISO 27001 sertifikası sunun
5	**Kapsam:** Kişisel, Gizli **İşleme Konumu:** Tedarikçide **İşleme Görevi:** İşleyen **Veri Sınıfı:** Gizli **Ödeme Kartları:** İlgili Değil **SaaS:** İlgili Değil **Alt Yüklenici Kullanımı:** İlgili Değil **Web Sitesi Barındırma:** İlgili Değil	DPR ile uyumluluğa ilişkin öz tasdik	
6	**Kapsam:** Kişisel, Gizli **İşleme Konumu:** Tedarikçide **İşleme Görevi:** Denetleyici **Veri Sınıfı:** Çok Gizli veya Gizli **Ödeme Kartları:** İlgili Değil **SaaS:** İlgili Değil **Alt Yüklenici Kullanımı:** İlgili Değil **Web Sitesi Barındırma:** İlgili Değil	DPR ile uyumluluğa ilişkin öz tasdik	

#	Profil	Güvence Gereksinimleri	Bağımsız Güvence Seçenekleri
7	**Kapsam:** Kişisel, Gizli **İşleme Konumu:** Tüm konumlar **İşleme Görevi:** Alt yüklenici (Bu görev Microsoft tarafından belirlenecektir – profilde şu ibare yer alacaktır "Alt Yüklenici Onayı: Evet") **Veri Sınıfı:** Çok Gizli veya Gizli **Ödeme Kartları:** İlgili Değil **SaaS:** İlgili Değil **Alt Yüklenici Kullanımı:** İlgili Değil **Web Sitesi Barındırma:** İlgili Değil	DPR ile uyumluluğa ilişkin öz tasdik **ve** Bağımsız Uyumluluk Güvencesi	Bağımsız Güvence seçenekleri: 1. DPR'a uyumla ilgili Bağımsız bir Değerlendirme, 2. DPR'ın A-I bölümleri ve ISO 27001 standardına uyumla ilgili Bağımsız bir Değerlendirme gerçekleştirin **veya** 3. ISO 27701 **ve** ISO 27001 sertifikası sunun

#	Profil	Güvence Gereksinimleri	Bağımsız Güvence Seçenekleri
SaaS, Alt yüklenici, Web Sitesi Barındırma eklemenin etkisi			
8	**Kapsam:** Kişisel, Gizli **İşleme Konumu:** Tedarikçide **İşleme Görevi:** İşleyen **Veri Sınıfı:** Çok Gizli veya Gizli **Ödeme Kartları:** İlgili Değil **Alt Yükleniciler:** EVET veya **SaaS:** EVET veya **Web Sitesi Barındırma:** EVET	DPR ile uyumluluğa ilişkin öz tasdik **ve** Bağımsız Uyumluluk Güvencesi	Bağımsız Güvence seçenekleri: 1. DPR'a uyumla ilgili Bağımsız bir Değerlendirme, 2. DPR'ın A-I bölümleri ve ISO 27001 standardına uyumla ilgili Bağımsız bir Değerlendirme gerçekleştirin **veya** 3. ISO 27701 **ve** ISO 27001 sertifikası sunun
9	**Kapsam:** Kişisel, Gizli **İşleme Konumu:** Tedarikçide **İşleme Görevi:** Denetleyici **Veri Sınıfı:** Çok Gizli veya Gizli **Ödeme Kartları:** İlgili Değil **Alt Yükleniciler:** EVET veya **SaaS:** EVET veya **Web Sitesi Barındırma:** EVET	DPR ile uyumluluğa ilişkin öz tasdik	

#	Profil	Güvence Gereksinimleri	Bağımsız Güvence Seçenekleri
Ödeme Kartları ve SaaS ile ilgili ilave güvence			
10	Yukarıdaki profillerden herhangi biri ve **Ödeme Kartları**	İlgili olan yukarıdaki gereksinimler **ve** Ödeme Kartı Sektör güvencesi	PCI DSS Sertifikası sunun
11	Yukarıdaki profillerden herhangi biri ve **Hizmet olarak Yazılım (SaaS)**	İlgili olan yukarıdaki gereksinimler **ile** sözleşme gereği istenen ve işlevsel hizmetleri kapsayan ISO 27001 sertifikası sunun.	Sağlanan hizmet(ler)in işlevsel kapsamını içeren bir ISO 27001 sertifikası sunun.