Microsoft Tedarikçisi Veri Koruma Gereksinimleri

Uygulanabilirlik

Microsoft Tedarikçisi Veri Koruma Gereksinimleri ("**DPR**"), Microsoft ile yaptığı sözleşmenin koşulları (ör. Satınalma Siparişi koşulları, ana sözleşme) altında yerine getirmesi gereken iş (ör. hizmetlerin, yazılım lisanslarının, bulut hizmetlerinin sağlanması) ile bağlantılı olarak Microsoft Kişisel Verileri veya Microsoft Gizli Verilerini İşleyen her bir Microsoft tedarikçisi için geçerlidir ("**İşin Yerine Getirilmesi**," "**Yerine Getirilmesi Gereken İş**" veya "**İş**").

- DPR ile tedarikçi ve Microsoft arasındaki sözleşmeye dayalı anlaşmalarda belirtilen gereksinimler arasında bir uyuşmazlık olması durumunda, ilgili veri koruma gereksinimini geçersiz kılan sözleşmedeki doğru hüküm tedarikçi tarafından tanımlanmadığı sürece DPR öncelikli olur (doğru hükmün tedarikçi tarafından tanımlanması durumunda sözleşmenin koşulları öncelikli olur).
- Burada yer alan gereksinimlerle herhangi bir hukuki veya yasal gereksinim arasında uyuşmazlık olması durumunda, hukuki veya yasal gereksinimler öncelikli olur.
- Microsoft tedarikçisinin Sorumlu olarak faaliyet göstermesi durumunda, tedarikçinin DPR'deki gereksinimleri daha düşük olabilir.
- Microsoft tedarikçisinin Microsoft Kişisel Verilerini değil, yalnızca Microsoft Gizli Verilerini işlemesi durumunda, tedarikçinin, bu DPR bakımından, gereksinimleri daha düşük olabilir.

Uluslararası Veri Aktarımı

Tedarikçi, diğer yükümlülükleri sınırlandırılmaksızın, Microsoft'un önceden yazılı onayı olmadan Microsoft Kişisel Verilerinin hiçbir şekilde uluslararası aktarımını yapmayacağı gibi, ne olursa olsun, Standart Sözleşme Maddeleri de dâhil olmak üzere Veri Koruma Gereksinimlerine, ya da Microsoft'un takdirine bağlı olarak, duruma göre, uygun bir veri koruma otoritesi veya Avrupa Komisyonu tarafından onaylı ve Microsoft tarafından benimsenmiş veya kabul edilmiş diğer uygun yurt dışı aktarım mekanizmalarına uyacaktır. (i) Avrupa Komisyonu tarafından benimsenmiş veya Avrupa Veri Koruma Denetçisi tarafından benimsenip, Avrupa Komisyonu, (ii) Birleşik Krallık Genel Federal Veri Koruma Yasası uyarınca Birleşik Krallık, (iii) İsviçre Federal Veri Koruma Yasası uyarınca İsviçre tarafından onaylanmış Halef Standart Sözleşme Maddeleri veya (iv) İsviçre ve Birleşik Krallık haricindeki bir yargı alanında ve Avrupa Birliği / Avrupa Ekonomik Alanı'nı içeren yargı alanlarında bulunan bir hükümet tarafından resmi olarak benimsenen ve kişisel verilerin uluslararası aktarımını düzenleyen maddeler birleştirilecek ve benimsendikleri tarihten itibaren Tedarikçi nezdinde bağlayıcı olacaktır. Tedarikçi, ayrıca, tüm alt işleyicilerin (Standart Sözleşme Maddelerinde tanımlandığı şekilde) de bunlara uymasını sağlayacaktır.

Önemli Tanımlar

Bu DPR'de kullanılan aşağıdaki terimler bitişiklerinde belirtilen anlamları taşırlar. "Dâhil" veya "gibi" ifadelerinden önce ve "ör." ya da "örneğin" ifadelerinden sonra gelen sıralı örnekler veya bu DPR genelinde kullanılan benzerleri, "yalnızca" veya "sadece" gibi sözcüklerle nitelenmedikleri sürece "sınırlama olmaksızın" veya "ancak bununla sınırlı olmamak üzere" anlamını içerecek şekilde yorumlanmalıdırlar. Daha fazla tanım için lütfen bu belgenin sonundaki Terimler Sözlüğü'ne bakın.

"**Sorumlu**" Kişisel Verilerin İşlenmesinin amaç ve yöntemlerini belirleyen tüzel kişi anlamına gelir. "Sorumlu", bağlamın gerektirdiği şekilde bir İşletmeyi, Sorumluyu (bu terimin GDPR'de taşıdığı anlamda) ve Veri Koruma Kanunlarındaki eş değer terimleri içerir.

"**Tanımlama Bilgileri**", web siteleri ve/veya uygulamalar tarafından cihazlarda depolanan ve Veri Sahibini veya cihazı tanımak için kullanılan bilgileri içeren küçük metin dosyalarıdır.

“**Veri Olayı**” (1) Tedarikçi veya Alt Yüklenicileri tarafından iletilen, depolanan veya başka bir şekilde İşlenen Microsoft Kişisel Verilerinin veya Microsoft Gizli Verilerinin kazara veya Yasa Dışı Olarak imha edilmelerine, kaybedilmelerine, değiştirilmelerine, yetkisiz olarak ifşa edilmelerine veya erişilebilmelerine yol açan bir güvenlik ihlali veya (2) Tedarikçinin Microsoft Kişisel Verilerini veya Microsoft Gizli Verilerini işlemesiyle ilgili güvenlik açığı anlamına gelir.

“**Veri Sahibi**” özellikle ad, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı gibi bir tanımlayıcı, ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla unsur aracılığıyla doğrudan ya da dolaylı olarak kimliği belirlenebilen bir gerçek kişi anlamına gelir.

“**Veri Sahibi Hakkı**”, söz konusu Veri Sahibinin kendi Microsoft Kişisel Verilerine erişme, bunları silme, düzenleme, dışa aktarma, kısıtlama veya Yasa gerektirdiğinde İşlenmesine itiraz etme hakkı anlamına gelir.

“**Yasa**” yargı yetkisine sahip herhangi bir kamu otoritesinin (federal, eyalet, yerel veya uluslararası) yürürlükteki tüm kanunlarını, kurallarını, tüzüklerini, yargılarını, kararlarını, emirlerini, düzenlemelerini, hükümlerini, yasalarını, kararnamelerini, önergelerini ve gereksinimlerini ifade eder. “**Yasa Dışı**” ifadesi Yasanın her türlü ihlali anlamına gelir.

“**Microsoft Gizli Verileri**” gizlilik veya bütünlük bakımından ifşalarının Microsoft’u ciddi itibar kaybına ve maddi zarara uğratabileceği bilgilerdir. Microsoft donanım ve yazılım ürünleri, kurum içi iş kolu uygulamaları, lansman öncesi pazarlama materyalleri, ürün lisans anahtarları, Microsoft ürünleri ve hizmetleriyle ilişkili teknik belgeler bu terimin kapsamı içerisinde yer alırlar.

“**Microsoft Kişisel Verileri**” Microsoft tarafından veya Microsoft adına İşlenen her türlü Kişisel Veri anlamına gelir.

“**Kişisel Veriler**”, bir Veri Sahibine ilişkin tüm bilgileri ve Yasalar uyarınca “kişisel veri” veya "kişisel bilgi” teşkil eden diğer tüm bilgileri ifade eder.

“**İşlem**” toplama, kayıt, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, elde etme, başvurma, kullanma, iletim yoluyla açıklama, yayma veya başka şekilde kullanıma sunma, uyumlaştırma veya birleştirme, kısıtlama, silme veya imha etme gibi, herhangi bir Microsoft Kişisel Verisi veya Gizli Verisi üzerinde otomatik veya otomatik olmayan araçlarla gerçekleştirilen her türlü işlem veya işlem dizisi anlamına gelir. “İşleme” ve “İşlenmiş” ifadeleri bu bağlamda karşılık gelen anlamlara sahip olacaktır.

“**İşleyici**”, Kişisel Verileri başka bir tüzel kişilik adına işleyen bir tüzel kişi anlamına gelir ve bağlamın gerektirdiği şekilde Hizmet Sağlayıcı, İşleyici (bu terim GDPR’de taşıdığı anlamda) ve Veri Koruma Kanunlarındaki eş değer terimleri içerir.

“**Alt Yüklenici**”, Microsoft ile doğrudan sözleşmeli olmayan bir tedarikçi iştiraki dâhil olmak üzere, tedarikçinin, yükümlülüklerini bunların Yerine Getirilmesini kapsayan sözleşmeyle bağlantılı olarak devrettiği üçüncü taraf anlamına gelir.

“**Alt İşleyici**” Microsoft'un İşin Yerine Getirilmesi için etkileşimde bulunduğu bir üçüncü taraf anlamına gelir. Burada İş, Microsoft'un İşleyicisi olduğu Microsoft Kişisel Verilerinin İşlenmesini içerir.

Tedarikçi Yanıtı

Tedarikçi, Microsoft tarafından yönetilen bir çevrimiçi hizmeti kullanarak bu gereksinimlerle uyumluluğunu her yıl onaylar. Uyumluluğun nasıl yönetildiğini anlamak için lütfen SSPA Program Kılavuzu’na bakın.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm A: Yönetim	
1	Microsoft ile tedarikçi arasındaki her bir geçerli sözleşme (ör. ana sözleşme, iş bildirimi, satın alma siparişleri ve diğer siparişler), Microsoft Kişisel Verilerinin satışı ve Microsoft Kişisel Verilerinin Microsoft ve tedarikçi arasındaki doğrudan iş ilişkisi dışında İşlenmesine ilişkin yasaklar da dâhil olmak üzere, Microsoft Gizli ve Kişisel Verilerine ilişkin olarak gizlilik ve güvenlik veri koruma dili içerir. Microsoft Kişisel Verileri bakımından, İş ile bağlantılı olarak İşleyici veya Alt İşleyici olarak çalışan şirketler için, İşlemin ana konusu ve süresi, İşlemin niteliği ve amacı, Microsoft Kişisel Verilerinin türü ve Veri Sahiplerinin kategorileri ile Microsoft'un yükümlülükleri ve hakları sözleşmede yer almalıdır.	Tedarikçi, Microsoft ile Tedarikçi arasındaki geçerli sözleşmeyi sunmalıdır. İşleyiciler ve Alt İşleyiciler için, İşleme açıklamaları geçerli sözleşmede (ör. iş bildirimi, satınalma siparişleri) yer alır. Not: Süreç içi satınalma siparişleri olan şirketler, İşleme faaliyetleriyle ilgili gerekli açıklamanın satınalma işlemine sonradan eklenmesini sağlayabilir.
2	Etkileşimlerinizin bir Alt İşleyici rolünü yerine getirdiğinin Microsoft tarafından onaylanması durumunda, Tedarikçinin Microsoft ile arasında geçerli veri koruma anlaşmaları olmalıdır. Not: Bu geçerli olduğunda Microsoft bu unvanı profilinizde yayınlar.	Standart Sözleşme Maddeleri, Çevrimiçi Müşteri Verileri Eki ve/veya Tedarikçi ve İş Ortağı Profesyonel Hizmetleri Veri İşleme Eki.
3	Şirket içinde belirlenecek bir kişi veya gruba DPR'ye uyum noktasında sorumluluk ve hesap verebilirlik yükleyin.	Microsoft Tedarikçi DPR'sine uyumluluğu sağlama görevi verilmiş kişinin veya grubun rolü belirtilmelidir. Bu kişinin veya grubun yetkisini ve hesap verebilirliğini bir gizlilik ve/veya güvenlik rolünü kanıtlar nitelikte açıklayan bir belge.
4	Microsoft Gizli Verilerine veya İşin Yerine Getirilmesi ile bağlantılı olarak tedarikçi tarafından İşlenen Kişisel Verilere erişim sahibi olacak çalışanlar için yıllık gizlilik ve güvenlik eğitimi hazırlanmalı, devamlılığı sağlanmalı ve gerçekleştirilmelidir. Şirketinizin hazır bir içeriği yoksa bu görsel taslağı kullanabilir ve şirketinize uyarlayabilirsiniz. Not: Tedarikçi personelinden Microsoft bölümleri tarafından sağlanan ek eğitimleri tamamlaması istenebilir.	Yıllık katılım kayıtları mevcuttur ve talep edildiğinde Microsoft'a sağlanabilir. Eğitim içeriği gizlilik ve güvenlik ilkelerini kapsar. Eğitim gereksinimlerine uyumluluk belgeleri, gizlilik mevzuatı gereksinimleriyle, güvenlik yükümlülükleriyle ve ilgili sözleşmenin gereksinimlerine ve yükümlülüklerine uyumlulukla ilişkili eğitim kanıtını içerecektir.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm A: Yönetim (devam)	
5	Yasayla aksine gerek görülmedikçe, Microsoft Kişisel Verileri, üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılmalarına ilişkin senaryolar da dâhil olmak üzere, yalnızca Microsoft'un belgelenmiş talimatlarına uygun şekilde işlenmelidir; bir yasal gereklilikle karşılaşılması durumunda ise, kamu yararına ilişkin önemli gerekçelerle söz konusu bilgilendirmeye Yasa tarafından yasak getirilmedikçe, İşleyici veya Alt İşleyici (tedarikçi), İşleme geçmeden önce söz konusu yasal gereksinimi sorumluya (Microsoft) bildirecektir.	Tedarikçi, belgelenmiş tüm Microsoft talimatlarını (ör. sözleşme, iş bildirimi veya sipariş belgeleri) İşe katılan tedarikçi çalışanlarının ve yüklenicilerinin kolayca erişebilecekleri bir konumda elektronik olarak derler ve muhafaza eder.
	Bölüm B: Bildirim	
6	Tedarikçi, Microsoft adına Kişisel Verileri toplarken Microsoft Gizlilik Bildirimi'ni kullanmalıdır. Kişisel Verilerini tedarikçiye gönderip göndermeyeceklerine karar verme noktasında kendilerine yardımcı olacak şekilde, gizlilik bildirimi Veri Sahipleri tarafından açıkça görülebilir ve ulaşılabilir olmalıdır. Not: İşleme faaliyetinin Sorumlusu sizin şirketiniz olduğunda kendi gizlilik bildiriminizi yayınlarsınız.	Tedarikçi, geçerli ve yayımlanmış Microsoft Gizlilik Bildirimi için bir fwdlink kullanır. Bir kullanıcının Kişisel Verilerinin toplanacağı her bağlamda Gizlilik Bildirimi yayınlanır. Mümkünse çevrimdışı bir sürümü bulundurulur ve veri toplama işlemi öncesinde sağlanır. Kullanılan tüm çevrimdışı Gizlilik Bildirimleri en son yayımlanmış sürümdür ve tarihleri uygun şekilde atılmıştır. Microsoft çalışanı hizmetleri için Microsoft Veri Gizliliği Bildirimi kullanılır.
7	Tedarikçiler canlı veya kayıttan sesli arama aracılığıyla Microsoft Kişisel Verilerini toplarken; ilgili veri toplama, işleme, kullanma ve saklama uygulamaları hakkında Veri Sahipleriyle görüşmeye hazır olmalıdır.	Ses kayıtlarına ilişkin yazılı metin Microsoft Kişisel Verilerinin nasıl İşlendiğini anlatır ve şunlara yer verir: ▪ toplama ▪ kullanma ve ▪ saklama

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm C: Seçenek ve İzin	
8	Uygulanabilir olduğunda, tedarikçi, Kişisel Verilerini toplamadan önce (her türlü yeni ve güncellenmiş İşleme faaliyeti dâhil) tüm İşleme faaliyetlerine yönelik Veri Sahibinin iznini almalı ve bunu kayda geçirmelidir. Tedarikçi, bir tercih değişikliğinin gerçekleştirileceği zaman diliminin geçerli olan en kısıtlayıcı yerel yasal gereksinim olduğundan emin olmak için tercih yönetiminin etkililiğini izler.	Tedarikçi, Veri Sahibinin bir İşleme faaliyeti için nasıl izin verdiğini ve bu iznin, tedarikçinin Veri Sahibine ait Kişisel Veriler ile ilgili İşleme faaliyetlerinin tümünü kapsadığını kanıtlayabilir. Tedarikçi, Veri Sahibinin bir İşleme faaliyeti için iznini nasıl geri çektiğini kanıtlayabilir. Tedarikçi, yeni bir İşleme faaliyetinin başlatılmasından önce tercihlerin nasıl kontrol edildiğini kanıtlayabilir. Not: Kullanıcı etkileşimi ekran görüntüleri, hizmetle ilgili deneyimler veya teknik belgeleri görüntüleme olanağı birer kanıt olabilir.
9	Microsoft web sitelerini ve/veya uygulamalarını ya da Microsoft markasını taşıyan siteleri oluşturan ve yöneten tedarikçiler, Microsoft Gizlilik Bildirimi'ndeki taahhütlerle ve yerel yasal gereksinimlerle uyumlu olarak Veri Sahiplerine tanımlama bilgilerinin kullanımıyla ilgili şeffaf bir bildirim ve tercih sağlamalıdır. Sözleşmeli işletme birimi tarafından özel olarak tersi talep edilmedikçe, tedarikçiler tercih denetimlerini yönetmek üzere 1ES tarafından oluşturulan Standart Başlığı kullanmalıdır. Bu gereksinim, sitelerin hedef kitlesi Avrupa Birliği/Avrupa Ekonomik Alanı içindeki ve geçerli gizlilik yasalarına sahip diğer bölgelerdeki kullanıcılardan oluştuğunda ve Microsoft Gizlilik Bildiriminin kullanıldığı her yerde geçerlidir. Not: Tanımlama bilgileri envanterinin kataloglanması ve yönetilmesi için, Microsoft iş sponsorlarının Microsoft web sitelerini dâhili Web Uyumluluğu portalına (http://aka.ms/wcp) kaydetmeleri gerekmektedir.	Her bir tanımlama bilgisinin amacı belgelenmeli ve uygulanan tanımlama bilgisinin türü hakkında bilgi verilmelidir. ▪ Oturum tanımlama bilgileri yeterli olduğunda kalıcı tanımlama bilgileri kullanılmamalıdır. ▪ Kalıcı tanımlama bilgileri kullanıldığında, bunların son kullanma tarihi kullanıcının siteyi ziyaret ettiği tarihten itibaren 13 ayı aşmamalıdır. Uygulanabilir olduğunda AB Yasaları ile uyumluluk doğrulanmalıdır. Örneğin: ▪ Gizlilik bildirimi için "Gizlilik ve Tanımlama Bilgileri" etiketleme kuralının kullanımı ▪ "Gerekli olmayan" tanımlama bilgilerinin reklam benzeri amaçlarla kullanımları öncesinde kullanıcıdan onaylayıcı izin alınması ve ▪ İznin 6 ayı aşmayacak bir süre içinde sona ermesi veya yenilenmesi.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm D: Toplama	
10	Tedarikçi, Microsoft Kişisel ve/veya Gizli Verilerinin toplanmasını yalnızca İşin Yerine Getirilmesi için gereken verilerin toplandığından emin olmak amacıyla izlemelidir.	Tedarikçi, toplanan Microsoft Kişisel ve/veya Gizli Verilerine İşin Yerine Getirilmesi için ihtiyaç duyulduğunu gösteren belgeleri sağlayabilir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
11	Tedarikçi, çocuklardan veri toplamadan önce (geçerli yargı alanı tarafından tanımlandığı şekilde), yerel gizlilik yasalarına göre izin almalıdır.	Tedarikçi, ebeveyn/veli onayını gösteren belgeler sağlayabilir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
	Bölüm E: Saklama	
12	Microsoft Kişisel ve/veya Gizli Verilerinin saklanmaya devam edilmesi Yasa ile mecbur tutulmadıkça, bu verilerin İşi Yerine Getirmek için gerekenden daha uzun bir süre saklanmaması sağlanmalıdır.	Tedarikçi, Microsoft tarafından sözleşmede (ör. iş bildirimi veya satınalma siparişi) belirtilen belgelenmiş saklama ilkelerine veya saklama gereksinimlerine uyar. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
13	Tamamen Microsoft'un takdirine bağlı olarak, İş tamamlandıktan sonra veya Microsoft'un talep etmesi üzerine, tedarikçinin elinde bulunan veya kontrolü altında olan Microsoft Kişisel ve Gizli Verilerinin Microsoft'a iade edilmesi veya yok edilmesi sağlanmalıdır. Verilerin açık bir şekilde kullanıcılar eliyle veya verilerin eskimesi gibi başka sebeplerden ötürü uygulamadan çıkartılmaları durumunda, uygulamaların içerisinde verilerin güvenli bir şekilde silinmesini sağlayacak işlemler mevcut olmalıdır. Microsoft Kişisel veya Gizli Verilerinin yok edilmesi gerektiğinde, tedarikçi, Microsoft Kişisel ve/veya Gizli Verilerini içeren fiziksel varlıkları yakarak, öğüterek veya parçalayarak bu bilgilerin okunamayacak veya yeniden oluşturulamayacak hale gelmesini sağlamalıdır.	Microsoft Kişisel ve Gizli Verilerinin (imha için Microsoft'a iadeleri de dâhil) elden çıkarılmalarının bir kaydı tutulmalıdır. Microsoft tarafından imhaya gerek görülmesi veya talep edilmesi halinde, tedarikçinin yetkililerinden birisinin imzasını taşıyan bir imha sertifikası sunulmalıdır.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm F: Veri Sahipleri	
	Veri Sahiplerinin, Kişisel Verilerine erişme, bu verileri silme, düzenleme, dışa aktarma, kısıtlama ve bu verilerin İşlenmesine itiraz etme gibi Yasa kapsamında belirli hakları ("**Veri Sahibi Hakları**") bulunmaktadır. Bir Veri Sahibinin, Microsoft Kişisel Verileri ile ilgili Yasa kapsamındaki haklarını kullanmak istemesi durumunda, tedarikçi, Microsoft'un aşağıdakileri yapmasına olanak sağlamalı veya kendisi bu eylemleri Microsoft adına gerçekleştirmelidir:	
14	Veri Sahibi Haklarını kullanmak isteyen Veri Sahiplerinin isteklerini yanıtlama yükümlülüklerini fazla gecikme olmadan yerine getirebilmesi için, mümkün oldukça, uygun teknik ve kurumsal önlemler aracılığıyla Microsoft'a yardımcı olmalıdır. Microsoft'un aksi yönde talimatı olmadıkça, Tedarikçi, kendisiyle iletişime geçen tüm Veri Sahiplerini, Veri Sahibi Haklarını kullanmaları için doğrudan Microsoft'a yönlendirecektir.	Tedarikçi, Veri Sahibi Haklarının uygulanmasını desteklemek için belgelenmiş süreç ve prosedürlere ilişkin kanıtları muhafaza edecektir. Tedarikçi, testlerin belgelenmiş kanıtlarını muhafaza edecektir. Kanıtlar Microsoft'un talebi üzerine sunulacaktır.
15	Veri Sahibine doğrudan yanıt verdiği veya self servis bir çevrimiçi mekanizma sağladığı durumlarda, Tedarikçi, talepte bulunan Veri Sahibini tanımlayabilmesini sağlayacak süreç ve prosedürlere sahiptir.	Tedarikçi, Microsoft Veri Sahiplerini tanımlamada kullanılan yöntemi belgelemiştir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
16	Microsoft'un kendisinden Veri Sahibi hakkında self servis çevrimiçi mekanizma aracılığıyla erişilemeyen Microsoft Kişisel Verilerini tespit etmesini istemesi durumunda, Tedarikçi, talep edilen verileri tespit etmek için makul bir çaba gösterecek ve makul bir arama gerçekleştirdiğini kanıtlamaya yetecek kadar da kayıt tutacaktır.	Tedarikçi, Microsoft Kişisel Verilerinin tutulup tutulmadığını belirleyen prosedürlerin belgelere dayalı kanıtını muhafaza edecek ve talep edildiğinde Microsoft'a belgeleri sunacaktır. Tedarikçi, Veri Sahibi Hak taleplerini karşılamak için atılan adımları kanıtlayan bir kayıt tutar. Belgede şu bilgiler yer alır: ▪ Talep tarihi ve saati ▪ Talebi yanıtlamak için atılan adımlar ve Microsoft'un ne zaman bilgilendirildiğine ilişkin kayıt. Tedarikçi, talep edildiğinde kayıt tutulduğuna ilişkin kanıtı Microsoft'a sağlayacaktır.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm F: Veri Sahipleri (devam)	
17	Tedarikçi, kendi Microsoft Kişisel Verilerine erişebilmeleri veya kullanabilmeleri noktasında atmaları gereken adımları Veri Sahiplerine bildirecektir.	Tedarikçi, Microsoft Kişisel Verilerine erişimle ilgili iletişimlerin ve prosedürlerin belgelere dayalı kanıtını muhafaza edecektir. Tedarikçi, belgelere dayalı kanıtı muhafaza edecek ve talep edildiğinde bu kanıtı Microsoft'a sunacaktır.
18	Veri Sahibi Haklarına ilişkin taleplerin tarih ve saatleri ile tedarikçinin bu taleplere yanıt olarak attığı adımlar kayıt altına alınmalıdır. Taleplerinin reddedilmesi durumunda, Microsoft'un talimatıyla, Veri Sahibine yazılı bir açıklama sağlanmalıdır. Talep edildiğinde, Veri Sahibi taleplerinin kayıtları Microsoft'a sağlanmalıdır.	Tedarikçi, erişim/silme taleplerinin kaydını tutar ve Microsoft Kişisel Verileri üzerinde yapılan değişiklikleri belgeler. Taleplerin reddedildiği durumlar belgelenmeli ve Microsoft değerlendirme ve onayının kanıtı saklanmalıdır. Tedarikçi, Microsoft Kişisel Verilerine erişimle ilgili taleplerin ve reddedilme durumlarının kaydının tutulduğuna dair kanıt sunacaktır.
19	Tedarikçi, Microsoft'un kimliği doğrulanmış Veri Sahibi için talep edilen Microsoft Kişisel Verilerinin kopyasını uygun bir basılı, elektronik veya sözlü formatta elde etmesini sağlamalıdır.	Tedarikçi, Microsoft Kişisel Verilerini Veri Sahibine anlaşılır bir formatta ve Veri Sahibi ve tedarikçi için uygun olan biçimde tedarik eder.
20	Tedarikçi, Microsoft'a veya kimliği doğrulanmış Veri Sahibine sağlanan Microsoft Kişisel Verilerinin başka bir kişinin kimliğini tespit maksadıyla kullanılmasını önleyecek makul tedbirleri almalıdır.	Tedarikçi, Veri Sahibinin kimliğinin Sözleşme koşullarına aykırı bir şekilde tespit edilmesini önleyici tedbirlerle ilgili prosedürlerin belgelere dayalı kanıtlarını muhafaza edecektir. Tedarikçi, talep edildiğinde Microsoft'a bu kanıtları temin edecektir.
21	Bir Veri Sahibi, Microsoft Kişisel Verilerinin tam ve doğru olmadığına inanıyorsa, tedarikçi bu sorunu Microsoft'a bildirmeli ve sorunu çözmek için Microsoft ile gerektiği gibi iş birliği yapmalıdır.	Tedarikçi, anlaşmazlık durumlarını belgeler ve sorunu Microsoft'a bildirir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm G: Alt yükleniciler	
	Tedarikçi, Microsoft Kişisel veya Gizli Verilerini İşlemek için bir alt yüklenici kullanmak niyetindeyse:	
22	Hizmetleri alt yükleniciye vermeden veya alt yüklenicilerin eklenmesi veya değiştirilmesiyle ilgili herhangi bir değişiklik yapmadan önce Microsoft'u bilgilendirmelidir. Not: Hâlihazırda alt yüklenici kullanmıyor olsanız da gelecekte kullanma ihtimalinize yönelik, bu yükümlülüğü kabul ettiğinizi belirtin.	Microsoft Kişisel Verilerinin yalnızca ilgili sözleşmede (ör. iş bildirimi, ek, satınalma siparişi) gerekli görüldüğü gibi Microsoft tarafından bilinen veya SSPA veritabanında yer alan şirketler tarafından İşlendiğini doğrulamalıdır. Tedarikçi, alt yüklenici listesini çevrimiçi yayınlayabilir ve SSPA veritabanındaki sayfaya bağlantı ekleyebilir.
23	İşin Yerine Getirilmesi için gerekli bilgilerin toplandığını temin etme noktasında, alt yükleniciler tarafından alt-İşlenen Microsoft Kişisel ve Gizli Verilerinin niteliğini ve kapsamını belgelemelidir.	Tedarikçi, alt yüklenicilere açıklanan veya aktarılan Microsoft Kişisel ve Gizli Verileri ile ilgili belgeleri muhafaza eder. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
24	Microsoft'un bir Microsoft Kişisel Verileri sorumlusu olması durumunda alt yüklenicinin, Microsoft Kişisel Verilerini Veri Sahibinin belirttiği iletişim tercihlerine göre kullandığından emin olun.	Bir Microsoft Veri Sahibi tercihinin alt yükleniciler tarafından nasıl kullanıldığını kanıtlamalıdır. Bir alt yüklenicinin tercih değişikliğini gerçekleştirmesi için gerekli zaman dilimini içeren destekleyici belgeleri (örneğin ekran görüntüsü, SLA, SOW vb.) sağlamalıdır.
25	Alt yüklenicinin Microsoft Kişisel veya Gizli Verileri üzerinde yapabileceği İşlemleri, tedarikçinin Microsoft ile yaptığı sözleşmeyi yerine getirmek için gereken amaçlarla sınırlandırmalıdır.	Tedarikçi, bir alt yükleniciye sağlanan Microsoft Kişisel Verilerinin İşin Yerine Getirilmesi için gerekli olduğunu gösteren belgeleri sağlayabilir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
26	Microsoft Kişisel Verilerinin yetkisiz veya Yasa Dışı olarak İşlenmesi emarelerine dair şikayetleri incelemelidir.	Tedarikçi, Microsoft Kişisel Verilerinin bir alt yüklenici tarafından yetkisiz kullanıldığına veya ifşa edildiğine dair şikâyetleri ele almaya yönelik sistemlerin ve işlemlerin devrede olduğunu kanıtlayabilir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm G: Alt Yükleniciler (devam)	
27	Bir alt yüklenicinin, Microsoft Kişisel veya Gizli Verileri üzerinde İşle ilgili olanların dışında bir amaçla işlem yaptığını öğrenir öğrenmez bu durumu derhal Microsoft'a bildirmelidir.	Tedarikçi, bir alt yüklenicinin Microsoft verilerinin kötüye kullanımını bildirmesi için gerekli talimatı ve araçları sağlamıştır. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
28	Tedarikçi, Microsoft adına üçüncü taraflardan Kişisel Veri topluyorsa, üçüncü taraf veri koruma politikalarının ve uygulamalarının tedarikçinin Microsoft ile yaptığı sözleşmeye ve DPR'ye uygun olduğunu doğrulamalıdır.	Tedarikçi, üçüncü tarafın veri koruma politikaları ve uygulamaları konusunda gereken özenin gösterildiğine dair belgeleri sağlayabilir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
29	Bir alt yüklenicinin, Microsoft Kişisel ve Gizli Verilerini yetkisiz veya Yasadışı olarak İşlemesinin doğuracağı fiili veya potansiyel zararı azaltmak için derhal harekete geçmelidir.	Tedarikçi, planın ve prosedürün belgelere dayalı kanıtını muhafaza etmeli ve talep edildiğinde belge kanıtını Microsoft'a sağlamalıdır.
	Bölüm H: Nitelik	
30	Tedarikçi, Microsoft Kişisel Verilerinin tümünün hatasız, eksiksiz ve beyan edilen İşlenme amaçlarıyla ilgili olmasını sağlamak suretiyle, bu verilerin bütünlüğünü korumalıdır.	Tedarikçi, Microsoft Kişisel Verileri toplanırken, oluşturulurken ve güncellenirken bu verileri doğrulamaya yönelik prosedürlerin devrede olduğunu kanıtlayabilir. Tedarikçi, hatasızlığı devamlı olarak teyit edip, gerekli düzeltmeleri yapan izleme ve örnekleme prosedürlerinin devrede olduğunu kanıtlayabilir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm I: İzleme ve Uygulama	
31	Tedarikçi, bir Veri Olayının farkına varır varmaz, Tedarikçinin, hangisi daha erkense, sözleşme gerekliliklerine göre veya gereksiz bir gecikmeye yol açmayacak şekilde Microsoft'u durumdan haberdar etmesini gerektiren bir olay müdahale planına sahiptir. Tedarikçi, Microsoft'un talebi veya yönlendirmesi doğrultusunda, bir adli inceleme gerçekleştirmesi için Microsoft'a gereken verilerin ve bilgilerin yanı sıra, Tedarikçi personeline veya donanımına erişimin sağlanması dâhil, Olayın araştırılması, tesirinin hafifletilmesi veya giderilmesine yönelik Microsoft ile işbirliği yapmalıdır. Not: Bir olayı Microsoft'a nasıl bildireceğiniz konusunda lütfen SSPA Program Kılavuzu'na bakın.	Tedarikçi, bu bölümde açıklandığı şekilde müşterileri (Microsoft) bilgilendirme adımını içeren bir olay müdahale planına sahiptir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
32	Bir iyileştirme planı uygulamalı ve uygun düzeltici önlemin zamanında alındığından emin olmak için her bir Veri Olayının çözümünü takip etmelidir.	Tedarikçi, bir Veri Olayını kapatmaya yönelik müdahalesinde uygulayacağı prosedürleri belgelemiştir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.
33	Microsoft'un bir Microsoft Kişisel Verileri sorumlusu olması durumunda, Microsoft Kişisel Verileriyle ilgili tüm veri koruma şikâyetlerine yanıt verecek bir resmi şikâyet süreci oluşturulmalıdır.	Tedarikçi, Microsoft Kişisel Verileri ile ilgili şikâyetleri alma olanaklarının yanı sıra, şikâyetlerle ilgilenilmesine yönelik belgelenmiş bir şikâyet prosedürüne sahiptir. Tedarikçi, talep edildiğinde Microsoft'a belgelere dayalı kanıt sağlayacaktır.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm J: Güvenlik	
	Tedarikçi, iyi endüstri uygulamaları doğrultusunda ve Yasanın gerektirdiği şekilde Microsoft Kişisel ve Gizli Verilerinin korunması ve güvenliğinin sağlanmasına yönelik politikalar ve prosedürler içeren bir bilgi güvenliği programı hazırlamalı, uygulamalı ve sürdürmelidir. Tedarikçinin güvenlik programı, aşağıda 34-50 gereksinimlerinde belirtilen standartları karşılamalıdır.	Geçerli bir ISO 27001 Sertifikası, Bölüm J için kabul edilebilir ikamedir. Bu ikameyi uygulamak için SSPA ile iletişime geçin. Not: Sertifikayı sağlamanız gerekecektir.
34	Aşağıdakileri içeren yıllık ağ güvenliği değerlendirmeleri yapılmalıdır: ▪ Yeni sistem bileşeni, ağ topolojisi, güvenlik duvarı kuralları gibi ortamda yapılan önemli değişiklikleri gözden geçirme ▪ Güvenlik açığı taramaları yapma ve ▪ Değişim günlüklerini muhafaza etme.	Tedarikçi, ağ değerlendirmelerini, değişim günlüklerini ve tarama sonuçlarını belgelemiştir. Gerek görülen değişim günlükleri değişiklikleri izlemeli, değişikliğin gerekçesiyle ilgili bilgi sağlamalı ve tayin edilmiş onaylayanın adını ve unvanını içermelidir.
35	Tedarikçi, bir mobil cihaz üzerinden erişilen veya kullanılan Microsoft Kişisel veya Gizli Verilerini güvenceye alan ve kullanımlarını sınırlandıran bir mobil cihaz politikası tanımlamalı, bu politikayı iletmeli ve uygulamalıdır.	Tedarikçi, Microsoft Kişisel veya Gizli Verilerinin İşlenmesi için bir mobil cihazın kullanımının gerekli olduğu durumlarda uyumlu bir mobil cihaz politikasının kullanıldığını kanıtlar.
36	İşi desteklemek üzere kullanılan tüm varlıkların hesabı tutulmalı ve bu varlıkların tanımlanmış bir sahibi olmalıdır. Tedarikçi, bu bilgi varlıklarının envanterini tutmaktan, kabul edilebilir ve yetkili kullanımlarını sağlamaktan ve kullanım ömürleri boyunca bu varlıklara uygun düzeyde koruma sağlamaktan sorumludur.	İşi desteklemek için kullanılan cihaz varlıkları envanteri. Bu varlıkların envanteri şunları içermelidir: ▪ Cihazın konumu ▪ Varlık üzerinde bulunan verilerin veri sınıflandırması ▪ Hizmet akdi veya iş anlaşması sona erdiğinde varlıkların geri alındığına ilişkin kayıt ve ▪ Gerekliliği kalmayan veri depolama ortamının imha edildiğine ilişkin kayıt.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm J: Güvenlik (devam)	
37	Tedarikçinin denetimi altındaki Microsoft Kişisel veya Gizli Verilerine yetkisiz erişimi önlemek için erişim hakkı yönetimi prosedürleri oluşturulmalı ve bunların devamlılığı sağlanmalıdır.	Tedarikçi aşağıdakileri içeren bir erişim hakları yönetim planını uygulamaya koyduğunu kanıtlar: ▪ Erişim denetimi prosedürleri ▪ Kimlik saptama prosedürleri ▪ Başarısız denemelerden sonra kilitleme prosedürleri ▪ Kimlik doğrulama bilgilerini seçmek için sağlam parametrelerin yanı sıra ▪ Hizmet akdinin sona ermesiyle birlikte 48 saat içinde kullanıcı hesaplarının devre dışı bırakılması ▪ Parola uzunluğunu ve karmaşıklığını zorunlu kılan ve yeniden kullanımı önleyen güçlü parola denetimleri Tedarikçi, Microsoft Kişisel ve Gizli Verilerine kullanıcı erişimini gözden geçirme noktasında en düşük erişim hakkı ilkesini uygulayan yerleşik bir süreç oluşturduğunu kanıtlar. Süreç şunları içerir: ▪ Açıkça tanımlanmış kullanıcı rolleri ▪ Rollere erişim onayını gözden geçiren ve gerekçelendiren prosedürler ve ▪ Microsoft verilerine erişim hakkına sahip rollerde yer alan kullanıcıların ilgili grupta/rolde yer almak için belgeli bir gerekçeye sahip olup olmadıklarını tespite yönelik test.
38	Microsoft Kişisel veya Gizli Verilerinin İşlenmesinde kullanılan sistemlerin güvenlik yamalarını önceliklendiren yama yönetimi prosedürleri tanımlanmalı ve uygulanmalıdır. Bu prosedürler şunları içermelidir: ▪ Güvenlik yamalarını önceliklendirmeye yönelik tanımlı risk yaklaşımı ▪ Acil durum yamalarını işleme ve uygulama yetisi ▪ İşletim Sistemine ve uygulama sunucusu gibi sunucu yazılımları ile veritabanı yazılımlarına uygulanabilirlik, ▪ Yamanın azalttığı riskin belgelenmesi ve özel durumların izlenmesi ve ▪ Yazan şirket tarafından artık desteklenmeyen yazılımın kullanımdan kaldırılmasına yönelik gereksinimler	Tedarikçi bu gereksinimi karşılayan ve asgari olarak aşağıdakileri kapsayan bir yama yönetimi prosedürü uyguladığını kanıtlayabilir: ▪ Önceliklendirmeyi bildirmek için önem derecesi atanması (Önem derecesi tanımları belgelenir.) ▪ Acil durum yamalarını uygulamak için belgelenmiş prosedür ▪ Yazan şirket tarafından artık desteklenmeyen işletim sistemlerinin kullanılmadığının doğrulanması. ▪ Onayları ve özel durumları izleyen yama yönetim kayıtları.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm J: Güvenlik (devam)	
39	Zararlı olabilecek virüslere ve kötü amaçlı yazılım uygulamalarına karşı koruma sağlamak amacıyla, sunucular, üretim ve eğitim masaüstü bilgisayarları dâhil olmak üzere, Microsoft Kişisel ve Gizli Verilerinin İşlenmesinde kullanılan ağa bağlı ekipmanlara virüsten ve kötü amaçlı yazılımdan koruma yazılımı yüklenmelidir. Kötü amaçlı yazılımdan koruma tanımları günde bir defa veya virüsten koruma/kötü amaçlı yazılımdan koruma yazılımı tedarikçisinin talimatına göre güncellenmelidir. Not: Bu, Linux dâhil olmak üzere tüm işletim sistemleri için geçerlidir.	Virüsten ve kötü amaçlı yazılımdan koruma yazılımı kullanımının etkin olduğunu gösterecek kayıtlar mevcuttur. Not: Bu gereksinim tüm işletim sistemleri için geçerlidir.
40	Microsoft için yazılım geliştiren tedarikçiler, tasarıma göre güvenlik ilkelerini yapım sürecine dâhil etmelidir.	Tedarikçi teknik belirtim belgeleri, geliştirme döngülerinde güvenlik doğrulaması için denetim noktaları içerir.
41	İzinsiz girişleri, kayıpları ve diğer yetkisiz faaliyetleri önlemek amacıyla bir Veri Kaybı Önleme (“**DLP**”) programı kullanılmalıdır. Veriler uygun şekilde sınıflandırılmalı, etiketlenmeli ve korunmalı ve tedarikçi, Microsoft Kişisel veya Gizli Verilerinin İşlenmesinde kullanılan bilgi sistemlerini izinsiz girişler, kayıplar ve diğer yetkisiz faaliyetler açısından izlemelidir. DLP programı, asgari koşul olarak: ▪ Microsoft Kişisel veya Gizli Verilerini saklıyorsanız, endüstri standardında konak, ağ ve bulut tabanlı İzinsiz Giriş Algılama Sistemleri (“**IDS**”) kullanılmasını gerektirir. ▪ Veri kaybını izlemek ve etkin olarak engellemek üzere yapılandırılan gelişmiş İzinsiz Giriş Koruma Sistemlerinin (“**IPS**”) uygulamaya geçirilmesini gerektirir. ▪ Sistem güvenliğinin ihlal edilmesi durumunda, varsa kalan güvenlik açıklarının da giderilmesi için sistemin analiz edilmesini gerektirir. ▪ Sistem güvenliğinin tehlikeye girdiği durumları algılayan araçların izlenmesine yönelik gerekli prosedürleri açıklamalıdır. ▪ Veri Olayı algılandığında uygulanması gereken bir olay müdahale ve yönetimi işlemi tesis eder ve	İzinsiz giriş, kayıp ve diğer yetkisiz faaliyetleri (ve en azından bu bölümde belirtilen tüm öğeleri) önlemek için prosedürlerin uygulandığı belgelenmiş DLP programı.

	▪ Microsoft Kişisel veya Gizli Verilerinin yetkisiz olarak indirilmesi ve kullanılmasıyla ilgili iletişim sağlanmasını (tedarikçinin İşinden çıkarılan tüm tedarikçi çalışanlarına ve alt yüklenicilerine) gerektirir.	
42	Olay müdahalesinden elde edilen Araştırma sonuçları derhal üst yönetime ve Microsoft'a bildirilmelidir.	Olay müdahalesi araştırma sonuçlarını Microsoft'a bildiren sistemler ve işlemler devrede olmalıdır.
43	Sistem yöneticileri, operasyon personeli, yönetim ve üçüncü taraflara yıllık güvenlik eğitimi verilmelidir.	Aşağıdakileri içeren bir güvenlik eğitimi programı oluşturulmalıdır: ▪ Olay müdahalesi için yıllık eğitim ve ▪ Kriz durumlarına etkili bir şekilde müdahale etmeyi kolaylaştırıcı olay simülasyonları ve otomatik mekanizmalar ▪ Kötü amaçlı yazılımların indirilmesiyle ilişkili riskler gibi olay önleme farkındalığı.
44	Tedarikçi, yedekleme planlama işlemlerinin Microsoft Kişisel ve Gizli Verilerini yetkisiz kullanımdan, erişimden, ifşadan, değiştirmeden ve imhadan korunmasını sağlamalıdır.	Tedarikçi, kuruluşun aksatıcı bir olayı nasıl yöneteceğine ve bilgi güvenliğini yönetim onaylı bilgi güvenliği sürekliliği hedefleri temelinde önceden belirlenmiş bir düzeye nasıl getirebileceğine ilişkin ayrıntıları içeren belgelenmiş müdahale ve kurtarma prosedürlerini kanıt olarak sunabilir. Tedarikçi, kritik verilerin düzenli olarak yedeklenmesi, güvenli şekilde depolanması ve etkili bir şekilde kurtarılmasına yönelik prosedürler tanımlayıp uyguladığını kanıt olarak sunabilir.
45	İş sürekliliği ve felâket kurtarma planları oluşturulup test edilmelidir.	Bir felâket kurtarma planı aşağıdakileri içermelidir: ▪ Bir sistemin tedarikçinin işletmesinin çalışması açısından kritik olup olmadığını belirlemeye yönelik tanımlanmış ölçütler. ▪ Tanımlanmış kriterlere göre bir felâket durumunda kurtarma için hedeflenmesi gereken kritik sistemlerin listesi. ▪ Her kritik sistem için, sistemi bilmeyen bir mühendisin dahi uygulamayı 72 saatten kısa sürede kurtarabilmesini sağlayan tanımlanmış felâket kurtarma prosedürü. ▪ Kurtarma hedeflerine ulaşılabilmesini sağlamak için felâket kurtarma planlarının yılda bir (veya daha sık) test edilmesi ve gözden geçirilmesi.
46	Bir kişiye Microsoft Kişisel veya Gizli Bilgilerine bireysel erişim izni vermeden önce, ilgili kişinin kimliği doğrulanmalı ve erişiminin İşi destekleme noktasında müsaade edilen faaliyet kapsamıyla sınırlı olması sağlanmalıdır.	Tüm kullanıcı kimliklerinin benzersiz olması ve her birinin Azure Active Directory gibi endüstri standardı bir kimlik doğrulama yöntemine sahip olması sağlanmalıdır.

		Yükseltilmiş erişim (idari veya diğer türden gelişmiş ayrıcalıklar), akıllı kart veya telefon tabanlı kimlik doğrulayıcı gibi ikinci bir faktörün kullanılmasını gerektirmelidir. Tüm tedarikçi çalışanlarının ve alt yüklenicilerinin Microsoft Kişisel veya Gizli Verilerine erişiminin, İşi desteklemek için gerekenden daha geniş veya daha uzun süreli olmamasını sağlamaya yönelik süreci kapsayan belgelenmiş bilgi güvenliği programı.
47	Tedarikçi, İşi ile bağlantılı olarak İşlenen tüm verileri, ağlar arasında aktarımları sürecinde, Aktarım Katmanı Güvenliği ("**TLS**") veya İnternet Protokolü Güvenliği ("**IPsec**") kullanan bir şifreleme ile korumalıdır. Bu yöntemler, NIST 800-52 ve NIST 800-57'de açıklanmıştır; eşdeğer bir endüstri standardı da kullanılabilir. Tedarikçi, şifrelenmemiş yöntemlerle iletilen Microsoft Kişisel veya Gizli Verilerinin teslimini reddetmelidir.	TLS veya diğer sertifikaların oluşturulması, dağıtılması ve değiştirilmesi işlemleri tanımlanmalı ve mecbur tutulmalıdır.
48	Microsoft Kişisel veya Gizli Verilerine erişen veya bu verileri işleyen tüm tedarikçi cihazlarında (dizüstü bilgisayarlar, iş istasyonları vb.) disk tabanlı şifreleme kullanılmalıdır.	Microsoft Kişisel veya Gizli Verilerini işlemek için kullanılan tüm istemci cihazları, Bitlocker ya da başka bir endüstri eşdeğeri disk şifreleme çözümünü karşılayacak şekilde şifrelenmelidir.

No.	Microsoft Tedarikçisi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı
	Bölüm J: Güvenlik (devam)	
49	Örnekleri aşağıda sıralanmış, fakat bunlarla sınırlı olmayan, her çeşit Microsoft Kişisel ve/veya Gizli Verilerini durağan (depolanmış) halde şifreleyecek (**NIST 800-111** standardında açıklananlar gibi geçerli endüstri standartlarını kullanan) sistem ve prosedürler devrede olmalıdır: ▪ Kimlik verileri (ör. kullanıcı adı/parolalar) ▪ Ödeme aracı verileri (ör. kredi kartı ve banka hesap numaraları) ▪ Göçmenlikle ilgili kişisel veriler ▪ Tıbbi profil verileri (ör. tıbbi kayıt numaraları veya kimlik doğrulama amacıyla kullanılan DNA, parmak izleri, göz retinaları ve irisler, ses modelleri, yüz modelleri ve el ölçümleri gibi biyometrik işaretleyiciler veya tanımlayıcılar) ▪ Devlet tarafından verilen tanımlayıcı veriler (ör. sosyal güvenlik veya sürücü ehliyeti numaraları) ▪ Microsoft müşterilerine ait veriler (ör. SharePoint, O365 belgeleri, OneDrive müşterileri) ▪ Duyurulmamış Microsoft ürünleriyle ilgili materyal ▪ Doğum Tarihi ▪ Çocukların profil bilgileri ▪ Gerçek zamanlı coğrafi veriler ▪ Fiziki kişisel (iş dışı) adres ▪ Kişisel (iş dışı) telefon numaraları ▪ Din ▪ Siyasi görüşler ▪ Cinsel yönelim/tercih ▪ Güvenlik sorusu yanıtları (ör. 2fa, parola sıfırlama) ▪ Anne kızlık soyadı	Microsoft Kişisel ve Gizli Verilerinin durağan halde şifrelenip şifrelenmediği kontrol edilir.
50	Geliştirme veya test ortamlarında kullanılan Microsoft Kişisel Verilerinin tümü anonimleştirilmelidir.	Microsoft Kişisel Verileri geliştirme ve test ortamlarında kullanılmamalıdır; başka bir seçenek yoksa Veri Sahiplerinin kimliğinin tespit edilmesini veya Kişisel Verilerin kötüye kullanılmasını önlemek için anonimleştirilmelidir.

		Not: Anonimleştirilmiş veriler, Bulanıklaştırılmış verilerden farklıdır. Anonimleştirilmiş veriler kimliği belirlenmiş veya belirlenebilir bir gerçek kişiyle ilgili olmayan verilerdir; veri sahiplerinin kimlikleri belirsizdir, ya da artık belirlenmesi imkânsızdır.

Terimler Sözlüğü

“Yetkili Temsilci”, şirket adına uygun düzeyde imza yetkisine sahip kişidir. Bu kişi, bir SSPA Programı eylemine yanıtını iletmeden önce gerekli gizlilik ve güvenlik bilgisine sahip olacak veya konusunda uzman bir kişiye danışmış olacaktır. Ayrıca, adını bir SSPA formuna eklemekle DPR'yi okuyup anladığını onaylamış olur.

“EUDPR”, 45/2001 sayılı Yönetmelik (AT) ile 1247/2002/EC sayılı Kararı yürürlükten kaldıran, kişisel verilerin AB kurumları, organları, ofisleri ve ajansları tarafından işlenmesi noktasında gerçek kişilerin korunması ve bu türden verilerin serbest dolaşımı hakkında 23 Ekim 2018 tarihli ve 2018/1725 sayılı Avrupa Parlamentosu ve Konseyi Yönetmeliği (AB) demektir.

"Serbest Çalışan", dijital platformlar aracılığıyla veya diğer yollarla aldığı taleplere bağlı görevleri veya hizmetleri gerçekleştiren kişiler demektir.

“GDPR”, 95/46/EC sayılı Yönergeyi yürürlükten kaldıran, kişisel verilerin işlenmesi noktasında gerçek kişilerin korunması ve bu türden verilerin serbest dolaşımı hakkında 27 Nisan 2016 tarihli ve 2016/679 sayılı Avrupa Parlamentosu ve Konseyi Yönetmeliği (AB) (Genel Veri Koruma Yönetmeliği) demektir.

“Gizlilik Verilerini Koruma Gereksinimleri”; GDPR, EUDPR, Yerel AB/AEA Veri Koruma Yasaları, California Tüketici Gizliliği Yasası, California Medeni Kanunu 1798.100 ve takip eden Maddeleri (“*CCPA*”), 2018 Birleşik Krallık Veri Koruma Yasası ve Birleşik Krallıkta geçerli olan diğer tüm ilgili ya da takip eden yasalar, yönetmelikler ve diğer yasal gereksinimler ile (a) gizlilik ve veri güvenliği; ya da (b) Kişisel Verilerin kullanımı, toplanması, saklanması, depolanması, güvenliği, ifşası, aktarımı, elden çıkarılması ve başka şekillerde işlenmesiyle ilgili yürürlükte olan her türlü yasa, yönetmelik ve diğer yasal gereksinimler demektir.

“AB Model Maddeleri” ve “Standart Sözleşme Maddeleri” (i) GDPR Madde 46’da açıklandığı ve 4 Haziran 2021 tarihli ve 2021/914 sayılı Avrupa Komisyonu kararı (AB) ile onaylandığı şekliyle, yeterli düzeyde veri koruması sağlamayan üçüncü ülkelerde yerleşik işleyicilere kişisel verilerin aktarımı için standart veri koruma maddeleri, (ii) (a) Avrupa Komisyonu, (b) Avrupa Veri Koruma Denetçisi tarafından benimsenmiş ve Avrupa Komisyonu, (c) Birleşik Krallık Genel Federal Veri Koruma Yasası uyarınca Birleşik Krallık, (d) İsviçre Federal Veri Koruma Yasası uyarınca İsviçre veya (e) İsviçre ve Birleşik Krallık haricindeki bir yargı alanında ve kişisel verilerin uluslararası aktarımının bu maddelere tabi olduğu Avrupa Birliği / Avrupa Ekonomik Alanı'nı içeren yargı alanlarında bulunan bir hükümet tarafından onaylanan bu maddeler birleştirilecek ve benimsendikleri tarihten itibaren Tedarikçi nezdinde bağlayıcı olacaktır.

“Web Sitesi Barındırma”; Web sitesi barındırma hizmeti, Microsoft alan adı altında Microsoft adına web siteleri oluşturan ve/veya sürdüren çevrimiçi bir hizmettir, yani tedarikçi, bir site oluşturulup, sürdürülmesi için gerekli tüm materyalleri ve hizmetleri sağlar ve siteyi internet üzerinden erişilebilir hale getirir. “Web barındırma hizmeti sağlayıcısı” veya “web barındırıcısı”, web sitesinin veya web sayfasının İnternette görüntülenmesi için gerekli olan, Tanımlama Bilgileri veya reklam amaçlı web işaretçileri gibi araçları ve hizmetleri sağlayan tedarikçidir.