Microsoft Tedarikçi Veri Koruma Gereksinimleri

Uygulanabilirlik

Microsoft Tedarikçi Veri Koruma Gereksinimleri ("**DPR**"), söz konusu tedarikçinin Microsoft ile yaptığı sözleşmenin (Satınalma Siparişi koşulları, ana sözleşme) koşulları altında yerine getirmesi gereken iş (örn. hizmetlerin, yazılım lisanslarının, bulut hizmetlerinin sağlanması) ile bağlantılı olarak Microsoft Kişisel Verilerini veya Microsoft Gizli Verilerini işleyen her bir Microsoft tedarikçisi için geçerlidir ("**İşin yerine getirilmesi,**" "**Yerine getirilmesi gereken iş**" veya "**İş**").

- Burada yer alan gereksinimler ile tedarikçi ve Microsoft arasındaki sözleşmeye dayalı anlaşmalarda belirtilen gereksinimler arasında uyuşmazlık olması durumunda, ilgili DPR bölümüyle uyuşmazlık oluşturan sözleşmedeki doğru hüküm ilgili tedarikçi tarafından DPR onayı formunda tanımlanmadığı sürece DPR öncelikli olur (söz konusu formda tanımlanması durumunda sözleşmenin koşulları öncelikli olur).
- Burada belirtilen gereksinimlerle herhangi bir yasal gereksinim arasında uyuşmazlık olması durumunda, yasal gereksinimler öncelikli olur.
- Bu DPR bakımından, Microsoft tedarikçisinin Denetleyici olarak çalıştığı durumda, söz konusu tedarikçinin İşleme faaliyetlerine ilişkin olarak yalnızca bölüm J Güvenlik ve bölüm A Yönetim içindeki gereksinimler geçerli olur.
- Bu DPR bakımından, Microsoft tedarikçisinin Microsoft Kişisel Verilerini işlememesi, ancak yalnızca Microsoft Gizli Verilerini işlemesi durumda, söz konusu tedarikçinin Microsoft Gizli Verilerini işlemesine ilişkin olarak yalnızca bölüm A Yönetim, bölüm E Saklama ve bölüm J Güvenlik içindeki gereksinimler geçerli olur.

Verilerin Uluslararası İletimi

Diğer yükümlülüklerini sınırlamaksızın, Microsoft önceden yazılı onay vermedikçe tedarikçi, Microsoft Kişisel Verilerinin uluslararası iletimini yapamaz ve tedarikçi, standart sözleşme şartlarının, bağlayıcı kurumsal kuralların ve herhangi bir veri koruma makamı, Avrupa Veri Koruma Kurulu veya Avrupa Komisyonu tarafından onaylanan ya da AB-ABD ve İsviçre-ABD dahil olmak üzere Microsoft tarafından benimsenen veya kabul edilen diğer şemaların veri koruma gereksinimlerine her halükarda uymalıdır. Gizlilik Kalkanı çerçeveleri ve AB Genel Veri Koruma Yönetmeliği dahil ama bunlarla sınırlı olmamak üzere herhangi bir veri koruma makamı, Avrupa Veri Koruma Kurulu veya Avrupa Komisyonu tarafından onaylanan ve Microsoft tarafından benimsenen veya kabul edilen diğer şemaların veri koruma gereksinimlerine uymalıdır. Tedarikçi, Gizlilik Kalkanı ilkelerinin gerektirdiği düzeyde koruma sağlama yükümlülüğünü artık yerine getiremeyeceğini belirlemesi durumunda Microsoft'a bildirimde bulunmayı kabul eder. Ayrıca tedarikçi, tüm alt işleyicilerin de bu gereksinimlere uymasını sağlar (Avrupa Komisyonu Kararı C(2010)593'e Ek olarak yayımlanan 2010 tarihli Standart Sözleşme Maddelerinin 1(d) Maddesinde tanımlandığı şekilde).

Önemli Tanımlar

Bu DPR'de kullanılan aşağıdaki terimler aşağıda belirtilen anlamlara gelmektedir. "Dahil" veya "gibi" ifadelerinden önce ve "örn." ya da "örneğin" ifadelerinden sonra gelen sıralı örnekler veya bu DPR genelinde kullanılan benzerleri, "yalnızca" veya "sadece" gibi sözcüklerle nitelenmediği sürece "sınırlama olmaksızın" veya "ancak bununla sınırlı olmamak üzere" anlamını içerecek şekilde yorumlanmalıdır.

"**Denetleyici**" tek başına veya başkalarıyla müşterek olarak Kişisel Verilerin İşlenme amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi, kamu yetkilisi, kurum veya diğer organ anlamına gelir; burada İşleme amaçları ve araçları Avrupa Birliği ("**AB**") veya Üye Devlet Yasalarınca belirlenirken, denetleyici (veya denetleyiciyi atamak için kullanılan ölçütler) bu Yasalarca tayin edilebilir.

“**İşlem**” toplama, kayıt, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, elde etme, başvurma, kullanma, iletmek 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 olan veya olmayan araçlarla gerçekleştirilen her türlü işlem veya işlem grubudur. “İşleme” ve “İşlenen” anlam olarak birbirinin yerini tutar.

“**İşleyici**” Denetleyici adına Kişisel Verileri işleyen gerçek veya tüzel kişi, kamu yetkilisi, kurum veya diğer organ anlamına gelir.

“**Kişisel Veriler**” kimliği belirlenmiş veya belirlenebilecek bir gerçek kişiyle (“**Veri Sahibi**”) ilgili her tür bilgi anlamına gelir; kimliği belirlenebilecek gerçek kişi, özellikle ad, kimlik numarası, konum verisi, çevrimiçi bir tanımlayıcı gibi bir tanımlayıcıyla ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, mental, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha çok faktöre göre doğrudan veya dolaylı olarak tanımlanabilen kişidir.

“**Microsoft Gizli Verileri**” gizlilik veya bütünlük nedeniyle ifşa edildiğinde, Microsoft açısından önemli maddi ve manevi kayıplar doğurabilecek türden bilgilerdir. Microsoft donanım ve yazılım ürünleri, şirket içinde kullanılan iş kolu uygulamaları, pazarlama malzemelerinin ön sürümleri, ürün lisans anahtarları ve Microsoft ürün ve hizmetleriyle ilgili teknik belgeler buna dahildir.

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

“**Veri İhlali**” iletilen, saklanan veya başka şekilde işlenen Kişisel Verilerin veya Microsoft Gizli Verilerinin kazara veya yasa dışı bir şekilde yok edilmesine, kaybolmasına, değiştirilmesine, yetkisiz ifşasına veya bu bilgilere erişilmesine yol açan bir güvenlik ihlali anlamına gelir.

“**Veri Sahibi Hakları**” Yasa ile mecbur tutulması halinde bir Veri Sahibi ile ilgili Microsoft Kişisel Verilerine o Veri Sahibinin erişme, silme, düzenleme, aktarma, kısıtlama ve bu verilerin işlenmesine itiraz etme hakkını ifade eder.

“**Yasa**” ise tüm geçerli yasaları, kuralları, kanunları, resmi emirleri, kararları, mahkeme kararlarını, yönetmelik hükümlerini, kanunnameleri, kararnameleri, resmi kararları ve yargı yetkisine sahip herhangi bir devlet makamının (federal, devlet, yerel veya uluslararası) gereksinimlerini ifade eder. “**Yasa Dışı**” ifadesi Yasanın ihlali anlamına gelir.

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm A: Yönetim		
1	Microsoft ile tedarikçi arasındaki her bir geçerli sözleşme (örn. ana sözleşme, iş bildirimi, satınalma siparişi ve diğer siparişler), uygun olduğunda Microsoft Gizli ve Kişisel Verilerine ilişkin olarak gizlilik ve güvenlik veri koruması dili içerir. İşleyici olarak çalışan şirketler için, İşlemin ana konusu ve süresi, İşlemin niteliği ve amacı, Microsoft Kişisel Verilerinin türü ve Veri Sahiplerinin kategorileri ve de Microsoft'un yükümlülükleri ve hakları sözleşmede yer almalıdır.	Tedarikçi, Microsoft ile Tedarikçi arasındaki geçerli sözleşmeyi sunmalıdır. İşleyiciler için, İşleme açıklamaları geçerli sözleşmede yer alır (*örn.*, iş bildirimi, satınalma siparişleri). Not: Süreç içi satınalma siparişleri olan şirketler, işleme faaliyetleriyle ilgili gerekli açıklamanın satınalma işlemine sonradan ekletilmesini sağlayabilir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
2	Şirket içinde belirlenen bir kişiyi veya grubu Veri Koruma Gereksinimleri (DPR) ile uyumluluktan sorumlu tutmalıdır.	Microsoft Tedarikçi DPR'sine uyumluluğu sağlama görevi verilmiş kişinin veya grubun adı. Bu kişinin veya grubun yetkisini ve hesap verme sorumluluğunu açıklayan ve gizlilik ve/veya güvenlik rolünü kanıtlayan bir belge.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
3	Microsoft Kişisel veya Gizli Verilerine erişim sahibi olacak çalışanlar için yıllık gizlilik ve güvenlik eğitimi hazırlamalı, devamlılığını sağlamalı ve gerçekleştirmelidir. Şirketinizin hazır bir içeriği yoksa bu görsel taslağı kullanabilir ve şirketinize uyarlayabilirsiniz.	Yıllık katılım kayıtları mevcuttur. Eğitim içeriği gizlilik ve güvenlik ilkelerini kapsar.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
4	Yasaya göre aksini yapması gerekmedikçe Microsoft Kişisel Verilerini yalnızca Microsoft'un Kişisel Verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa iletilmesiyle ilgili belgelenmiş talimatlarına uygun şekilde işlemelidir. Yasayla zorunlu bırakılması durumunda İşleyici (tedarikçi), önemli kamu çıkarı gerekçeleriyle söz konusu bilgiler Yasa tarafından yasaklanmadıkça, yasal gereksinimi denetleyiciye (Microsoft) İşlem yapmadan önce bilgi verecektir.	Talimatların, bir sözleşme, iş bildirimi veya satın alma siparişinde belirtilen ya da yerine getirilmesi gereken işte kullanılan elektronik sistemin bir parçası olarak elde edilen belgelenmiş kanıtı.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm B: Bildirim		
5	Tedarikçi, Microsoft adına Kişisel Verileri toplarken Microsoft Gizlilik Bildirimi'ni kullanmalıdır. Kişisel Verilerini tedarikçiye gönderip göndermeyeceklerine karar vermelerine yardımcı olmak için gizlilik bildirimi Veri Sahipleri tarafından açıkça görülebilir ve ulaşılabilir olmalıdır. Not: İşleme faaliyetinin Denetleyicisi sizin şirketiniz olduğunda kendi gizlilik bildiriminizi gönderirsiniz. *Doğru Microsoft bildirimlerine erişim için SSPAHelp@microsoft.com ile iletişime geçin.*	Tedarikçi geçerli ve yayımlanmış Microsoft Gizlilik Bildirimi'nin fwdlink bağlantısını kullanır. Bir kullanıcının Kişisel Verilerinin toplanacağı her bağlamda Gizlilik Bildirimi'ne yer verilir. Uygulanabilirse, çevrimdışı bir sürümü bulundurulur ve veri toplama işlemi öncesinde sağlanır. Kullanılan çevrimdışı Gizlilik Bildirimleri en son yayımlanmış sürümdür ve uygun şekilde tarih atılmıştır. Microsoft çalışan hizmetleri için Microsoft Veri Koruma Bildirimi kullanılır.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
6	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 işlendiğini içerir ve şu konular yer alır: ▪ toplama, ▪ kullanım ve ▪ saklama.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm C: Seçenek ve İzin		
7	Tedarikçinin verileri İşlemek için yasal dayanağı izinse Veri Sahibinin Kişisel Verilerini toplamadan önce tüm İşleme faaliyetleri (varsa, yeni ve güncellenen İşleme faaliyetleri de dahil) için o Veri Sahibinin iznini almalı ve bunları kayda geçirmelidir.	Tedarikçi, Veri Sahibinin bir işleme faaliyeti için nasıl onay verdiğini ve bu onayın kapsamının, Veri Sahibine ait Kişisel Verilere ilişkin olarak tedarikçinin işleme faaliyetlerinin tümünü kapsadığını kanıtlayabilir. Tedarikçi, Veri Sahibinin bir işleme faaliyeti için onayı nasıl geri çektiğini kanıtlayabilir. Tedarikçi, yeni bir işleme faaliyetinin başlatılmasından önce tercihlerin nasıl kontrol edildiğini kanıtlayabilir. Tedarikçi, bir tercih değişikliğinin geçerli olan en kısıtlayıcı yerel yasal gereksinimlere uygun zaman diliminde gerçekleştirilmesini sağlamak için tercih yönetiminin etkililiğini izler. Not: Kullanıcı etkileşimi ekran görüntüleri, hizmetle ilgili denemeler veya teknik belgelere bakma fırsatı birer kanıt olabilir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm C: Seçenek ve İzin (devamı)		
8	Tanımlama bilgileri, web siteleri ve/veya uygulamalar tarafından cihazlarda saklanan ve Veri Sahibini veya cihazı tanımlamak için kullanılan bilgiler içeren küçük metin dosyalarıdır. Microsoft web sitelerini ve/veya uygulamalarını oluşturan ve yöneten tedarikçiler Veri Sahiplerine tanımlama bilgilerinin kullanımıyla ilgili açık bir bildirim ve seçenek sağlamalıdır. Microsoft web sitelerini ve/veya uygulamalarını oluşturan ve yöneten tedarikçiler, tanımlama bilgilerinin kullanımının Microsoft Gizlilik Bildirimi'ndeki taahhütlerle ve Avrupa Birliği (AB) tarafından belirlenen kurallar gibi yerel yasal gereksinimlerle uyumlu olmasını sağlamalıdır.	Her 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 2 yılı aşmamalıdır. AB kullanıcıları için kalıcı bir tanımlama bilgisinin son kullanma tarihi 13 ayı aşmamalıdır. Uygulanabilir olduğunda AB Yasaları ile uyumluluk doğrulanmalıdır. Örneğin: ▪ Gizlilik bildirimi için "Gizlilik ve Tanımlama Bilgileri" etiketleme kuralının kullanımı; ve ▪ Reklam gibi "gerekli olmayan" amaçlara yönelik olarak tanımlama bilgilerinin kullanılmasından önce olumlu kullanıcıdan izin alınması.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm D: Toplama		
9	Tedarikçi, yalnızca İşin yerine getirilmesi için gereken bilgilerin toplandığından emin olmak üzere Microsoft Kişisel ve/veya Gizli Verilerinin toplanmasını izlemelidir.	Tedarikçi, toplanan Microsoft Kişisel ve/veya Gizli Verilerine İşin yerine getirilmesi için ihtiyaç duyulduğunu gösteren belgeleri sağlayabilir.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
10	Tedarikçi, Microsoft adına üçüncü taraflardan Kişisel Veri topluyorsa, tedarikçi, üçüncü taraf veri koruma ilkelerinin ve uygulamalarının tedarikçinin Microsoft ile yaptığı sözleşmeye ve DPR'ye uygun olduğunu doğrulamalıdır.	Tedarikçi, üçüncü tarafın veri koruma ilkeleri ve uygulamaları konusunda gereken özenin gösterildiğine dair belgeleri sağlayabilir.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
11	Bir Veri Sahibinin cihazına yürütülebilir yazılım yüklenmesi veya bilgisayarda yürütülebilir yazılımın kullanılması aracılığıyla Microsoft Kişisel Verilerini toplamadan önce, bu bilgilerin toplanmasının gerektiği, Microsoft ile yapılan tedarikçi sözleşmesinde belgelenmelidir.	Yürütülebilir yazılımın Veri Sahibinin cihazında kullanımına ilişkin Microsoft sözleşmesi, yapılan sözleşmede belirtilir.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
12	Hassas konulardaki Microsoft Kişisel Verilerini (ırk veya etnik kökeni, siyasi görüşleri, dini veya felsefi inançları ya da sendika üyeliğini ortaya çıkaran veriler, genetik veriler, biyometrik veriler, sağlık durumuyla ilgili veriler veya kişinin cinsel hayatı veya cinsel yönelimiyle ilgili bilgiler) toplamadan önce, bu Microsoft Kişisel Verilerinin toplanmasının gerektiği, Microsoft ile yapılan tedarikçi sözleşmesinde belgelenmelidir.	Hassas Microsoft Kişisel Verilerini toplama gereksinimi, Microsoft ile yapılan sözleşmede belirtilmelidir.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm E: Saklama		
13	Microsoft Kişisel ve/veya Gizli Verilerinin sürekli olarak saklanması Yasa ile mecbur tutulmadıkça, bu verilerin İşin yerine getirilmesi için gerekenden fazla bir süre saklanmamasını sağlamalıdır.	Tedarikçi, Microsoft tarafından sözleşmede (örn. iş bildirimi veya satınalma siparişi) belirtilen belgelenmiş saklama ilkelerine veya saklama gereksinimlerine uyar.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
14	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 edilmesini veya yok edilmesini sağlamalıdır. Uygulamaların içinde, açık bir şekilde kullanıcılar tarafından ya da verinin eskimesi gibi diğer nedenlerden dolayı uygulamadaki verilerin kaldırılması durumunda verilerin güvenli bir şekilde silinmesini sağlayacak işlemler yürürlükte olmalıdır. Microsoft Kişisel veya Gizli Verilerinin yok edilmesi gerektiğinde, tedarikçi, Microsoft Kişisel ve/veya Gizli Verilerini içeren fiziksel varlıkları yakarak, öğüterek veya yırtarak bu bilgilerin okunamayacak veya yeniden oluşturulamayacak hale gelmesini sağlamalıdır.	Microsoft Kişisel ve Gizli Verilerinin elden çıkarılmasının bir kaydının tutulması (yok edilmek üzere Microsoft'a iadesini de içerebilir). Microsoft verilerin yok edilmesini gerekli görüyor veya talep ediyorsa, tedarikçinin yetkililerinden biri tarafından imzalanmış bir yok etme sertifikası sunulması.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm F: Veri Sahipleri		
	Veri Sahipleri, Kişisel Verilerine erişme, bu verileri silme, düzenleme, aktarma, kısıtlama ve bu verilerin işlenmesine itiraz etme haklarına sahiptir ("**Veri Sahibinin Hakları**"). Veri Sahibi, Microsoft Kişisel Verileri ile ilgili olarak Yasa kapsamındaki haklarını kullanmak isterse tedarikçi:		
15	Veri Sahibi Haklarını kullanmak isteyen Veri Sahiplerinin isteklerini yanıtlama yükümlülüklerini yerine getirmesi için, mümkün olduğu ölçüde, uygun teknik ve kurumsal önlemler aracılığıyla Microsoft'a yardımcı olmalıdır.	Veri Sahibi Haklarının uygulanmasını destekleyecek işlemler ve yordamlar mevcuttur.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
16	Fazla gecikmeden Veri Sahiplerinin Haklarına tümüyle yanıt vermelidir.	Tedarikçi, Veri Sahibi Haklarını destekleyebildiğini düzenli olarak test etmelidir.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
17	Microsoft tarafından aksi bir yönerge sunulmadıkça Tedarikçi, kendisiyle iletişime geçen tüm Veri Sahiplerini, Veri Sahibi Haklarını kullanmaları için doğrudan Microsoft'a yönlendirir. Tedarikçi, Veri Sahiplerinin kendi Microsoft Kişisel Bilgilerine erişebilmeleri ya da bu bilgilerle ilgili haklarını başka şekilde kullanabilmeleri için yapmaları gereken şeyleri onlara bildirir. *Bu gereksinimle ilgili yardım almak için SSPAHelp@microsoft.com ile iletişime geçin.*	Tedarikçi, Kişisel Verilere erişim için uygulanması gereken adımları ve bu verilerin güncellenmesi için kullanılan yöntemleri bildirir.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
18	Veri Sahibine doğrudan yanıt verirken, istekte bulunan Veri Sahibinin kimliğini doğrulamalıdır.	Tedarikçi, Microsoft Veri Sahiplerini tanımlamak için kullanılan yöntemi belgelemiştir.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm F: Veri Sahipleri (devamı)		
	Bir Veri Sahibinin kimliği doğrulandıktan sonra tedarikçi:		
19	O Veri Sahibine ait Microsoft Kişisel Verilerini elinde tutup tutmadığını veya kontrol edip etmediğini belirlemelidir.	Tedarikçi, Kişisel Verilerin tutulup tutulmadığını belirleyen yordamlara sahiptir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
20	İstenen Microsoft Kişisel Verilerini bulmak için makul bir çaba göstermeli ve makul bir aramanın yapıldığını göstermeye yetecek kadar kayıt tutmalıdır.	Tedarikçi, Veri Sahibi Hak taleplerini karşılamak için atılan adımları kanıtlayan bir kayıt tutar. Belgede şu bilgiler yer alır: ▪ Talep tarihi ve saati ▪ Talebe yanıt vermek için gerçekleştirilen eylemler ve ▪ Microsoft'a ne zaman bilgi verildiğinin kaydı	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
21	Veri Sahibi Haklarına ilişkin isteklerin tarihini ve saatini ve tedarikçinin bu isteklere yanıt olarak gerçekleştirdiği eylemleri kaydetmelidir. İstendiğinde, Veri Sahibi taleplerinin kayıtlarını Microsoft'a sağlamalıdır.	Tedarikçi, erişim taleplerinin kaydını tutar ve Kişisel Veriler üzerinde yapılan değişiklikleri belgeler.	
	Veri Sahibinin kimliği doğrulanıp tedarikçi, talep edilen Microsoft Kişisel Verilerine sahip olduğunu doğruladıktan sonra, tedarikçi:		
22	Kişisel Verilerin kopyasının istenmesi durumunda, Microsoft Kişisel Verilerini uygun bir basılı, elektronik veya sözlü biçimde Veri Sahiplerine vermelidir.	Tedarikçi, Veri Sahibine Kişisel Verileri anlaşılabilir bir biçimde ve Veri Sahibi ve tedarikçi için uygun olan bir formda sağlar.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
23	İstekleri reddedilirse, Microsoft'un talimatıyla Veri Sahibine, daha önceden Microsoft tarafından sağlanan ilgili yönergelerle tutarlılık gösteren yazılı bir açıklama yapmalıdır. *Bu gereksinimle ilgili yardım almak için SSPAHelp@microsoft.com ile iletişime geçin.*	İsteklerin reddedildiği durumlar belgelenmeli ve Microsoft değerlendirme ve onayının kanıtı saklanmalıdır.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm F: Veri Sahipleri (devamı)		
24	Tedarikçi, Veri Sahibine verilen Microsoft Kişisel Verilerinin başka bir kişinin kimliğini tespit etmek için kullanılamamasını sağlamak üzere makul ölçüde tedbir almalıdır.	Tedarikçi, verilen bilgilerden başka bir şahsın kimliğinin belirlenememesini sağlayacak makul önlemlerin alındığını kanıtlamalıdır (örneğin, talep edilen Veri Sahibi Kişisel Verilerinin yalnızca tek bir satırda yer aldığı bir sayfanın tamamı çoğaltılamaz).	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
25	Veri Sahibi ve tedarikçi arasında Microsoft Kişisel Verilerinin eksiksiz ve doğru olup olmadığı konusunda anlaşmazlık olursa tedarikçi bu sorunu Microsoft'a bildirmeli ve sorunu çözmek için Microsoft ile gerektiği gibi iş birliği yapmalıdır. *Bu gereksinimle ilgili yardım almak için SSPAHelp@microsoft.com ile iletişime geçin.*	Tedarikçi, anlaşmazlık durumlarını belgeler ve sorunu Microsoft'a iletir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm G: Üçüncü Taraflara İfşa Etme		
	Tedarikçi, Microsoft Kişisel veya Gizli Verilerinin İşlenmesi için bir alt yüklenici kullanmak niyetindeyse:		
26	Hizmetler için alt yüklenici kullanmadan ya da alt yüklenici ekleme veya değiştirmeyle ilgili değişiklikler yapmadan önce Microsoft'un açık yazılı iznini almalıdır. *Bu gereksinimle ilgili yardım almak için SSPAHelp@microsoft.com ile iletişime geçin.*	Microsoft Kişisel Verilerinin yalnızca, ilgili sözleşmede (örn. iş bildirimi, ek, satınalma siparişi) gerekli görülen veya SSPA veritabanında kaydedilmiş, Microsoft'un bildiği şirketler tarafından işlendiğinin doğrulanması.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
27	İşin yerine getirilmesi için gereken bilgilerin toplandığından emin olmak üzere alt yükleniciler tarafından işlenen Microsoft Kişisel ve Gizli Verilerinin mahiyetini ve kapsamını belgelemelidir.	Tedarikçi, alt yüklenicilere ifşa edilen veya aktarılan Microsoft Kişisel ve Gizli Verileri konusunda sürekli olarak belgelendirme yapar.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
28	Alt yüklenicinin, Microsoft Kişisel Verilerini, Veri Sahibinin beyan edilmiş iletişim tercihlerine uygun olarak kullanmasını sağlamalıdır.	Bir Microsoft Veri Sahibi Tercihinin alt yükleniciler tarafından nasıl kullanıldığının kanıt olarak sunulması. Bir alt yüklenicinin tercih değişikliğini gerçekleştirmesi için gerekli zaman dilimini içeren destekleyici belgelerin sağlanması.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
29	Alt yüklenicinin Microsoft Kişisel Verileri üzerinde yapabileceği işlemleri, tedarikçinin Microsoft ile yaptığı sözleşme koşullarını yerine getirmesi için gereken şeylerle sınırlamalıdır.	Tedarikçi, bir alt yükleniciye sağlanan Microsoft Kişisel Verilerine İşin yerine getirilmesi için ihtiyaç duyulduğunu gösteren belgeleri sağlayabilir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
30	Microsoft Kişisel Verilerinin yetkisiz veya Yasa Dışı olarak İşlenmesi emarelerine dair şikayetleri incelemelidir.	Tedarikçi, Microsoft Kişisel Verilerinin alt yüklenici tarafından yetkisiz kullanımına veya ifşa edilmesine ilişkin şikayetler için sistemlerin ve işlemlerin mevcut olduğunu kanıtlayabilir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm G: Üçüncü Taraflara İfşa Etme (devamı)		
31	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 verileriyle ilgili kötüye kullanımı rapor etmesi için talimatı ve araçları sağlamıştır.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
32	Bir alt yüklenicinin, Microsoft Kişisel ve Gizli Verilerinin yetkisiz veya Yasa Dışı olarak İşlenmesi sonucunda ortaya çıkan zararı veya olası zararı azaltmak için derhal harekete geçmelidir.	Tedarikçi, Microsoft Kişisel ve Gizli Verilerinin bir alt yüklenici tarafından kötüye kullanılması ihtimaline karşı mevcut bir planı ve yordamları bulunduğunu kanıtlayabilir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
	Bölüm H: Kalite		
33	Tedarikçi, Microsoft Kişisel Verilerinin tümünün doğru, eksiksiz ve beyan edilen İşlenme amaçlarıyla ilgili olmasını sağlayarak bu bilgilerin bütünlüğünü korumalıdır.	Tedarikçi, Microsoft Kişisel Verileri toplanırken, oluşturulurken ve güncellenirken bu verileri doğrulamaya yönelik yordamların mevcut olduğunu kanıtlayabilir. Tedarikçi, sürekli olarak doğruluğu kontrol eden ve gerekli düzeltmeleri yapan izleme ve örnekleme yordamlarının mevcut olduğunu kanıtlayabilir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm I: İzleme ve Uygulama		
34	Tedarikçinin elinde, Microsoft Kişisel veya Gizli Verileri üzerinde kendi yaptığı işlemlerle ilgili bir Veri İhlali veya güvenlik açığının farkına varır varmaz, fazla gecikmeden bu durumu Microsoft'a bildirmesini gerektiren olay yanıtı planı olmalıdır. *Olay bildirmek için SSPAHelp@microsoft.com ile iletişime geçin.*	Tedarikçinin, bu bölümde açıklandığı üzere müşterileri (Microsoft) bilgilendirme adımını içeren bir olay yanıtı planı vardır.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
35	Yasalar gerektirmedikçe, Microsoft Kişisel veya Gizli Verilerini içeren bir Kişisel Veri İhlaliyle ilgili olarak, Microsoft'un onayını almadan herhangi bir basın açıklaması ya da genel duyuru yayınlamamalıdır.	Tedarikçi, olayın meydana gelmesi halinde bu gereksinimi karşılamayı kabul eder.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
36	Zamanında uygun bir düzeltme eyleminin gerçekleştirilmesini sağlamak için bir düzeltme planı uygulamalı ve Microsoft Kişisel veya Gizli Verileri ile ilgili Veri İhlallerinin ve güvenlik açıklarının çözümlenmesini izlemelidir.	Tedarikçi, bir Veri İhlaline yanıt vererek ihlali kapatmak için uygulayacağı yordamları belgelemiştir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
37	Microsoft Kişisel Verileriyle ilgili veri koruma şikayetlerinin tümüne yanıt vermek için resmi bir şikayet süreci oluşturmalıdır.	Tedarikçi, Microsoft Kişisel Verileriyle ilgili şikayetleri alma olanaklarına sahiptir ve şikayetleri ele almak üzere belgelenmiş bir şikayet yordamı vardır.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik		
	Tedarikçi, iyi endüstri uygulamaları doğrultusunda ve Yasanın gerektirdiği şekilde Microsoft Kişisel ve Gizli Verilerini korumak ve güvenliğini sağlamak için ilkeler ve yordamlar içeren bir bilgi güvenliği programı hazırlamalı, uygulamalı ve bu programı sürdürmelidir. Tedarikçinin güvenlik programı, aşağıda listelenen 38 -56 gereksinimlerindeki standartları karşılamalıdır.	Korumalar, mevzuat planlarını (örneğin, HIPPA, GLBA) veya sözleşme gereksinimlerini karşılamak için gerektiğinde listelenenlerden fazla olabilir. Güvenliği içeren geçerli bir ISO 27001 veya SOC 2 raporu, Bölüm J için kabul edilebilir ikamedir. Bu ikameyi uygulamak için SSPAHelp@microsoft.com ile iletişime geçin. Not: Bu sertifikaların/raporların kapsamını açıklayan belgeleri sağlamanız gerekecektir.	
38	Şunları içeren yıllık ağ güvenliği değerlendirmeleri yapmalıdır: ▪ 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. Gerekli değişim günlükleri değişiklikleri izlemeli, değişikliğin gerekçesiyle ilgili bilgi sağlamalı ve tayin edilmiş onaylayanın adını ve unvanını içermelidir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
39	Tedarikçi, bir mobil cihazda erişilen veya kullanılan Microsoft Kişisel veya Gizli Verilerini güvenceye alan ve bu bilgilerin kullanımını sınırlandıran bir mobil cihaz ilkesi tanımlamalı, bu ilkeyi iletmeli ve uygulamalıdır.	Tedarikçi, Microsoft Kişisel veya Gizli Verilerinin işlenmesi için bir mobil cihazın gerekli olduğu durumlarda uyumlu bir mobil cihaz ilkesinin kullanıldığını kanıtlar.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik (devamı)		
40	İşi desteklemek üzere kullanılan tüm varlıklar açıklanmalı ve bu varlıkların tanımlanmış bir sahibi olmalıdır. Tedarikçi, bu bilgi varlıklarının envanterini tutmaktan, varlıkların kabul edilebilir ve yetkili kullanımını sağlamaktan ve varlıkların kullanım ömrü boyunca uygun düzeyde koruma sağlamaktan sorumludur.	İşi desteklemesi için kullanılan cihaz varlıkları envanteri. Bu varlıkların envanteri şunları içermelidir: ▪ Cihazın konumu ▪ Varlıktaki verilerin veri sınıflandırması ▪ İş akdinin veya iş anlaşmasının sona ermesi durumunda varlıkların geri alındığına ilişkin kayıt ve ▪ Artık gerekli olmaması durumunda veri depolama ortamının imha edildiğine ilişkin kayıt	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik (devamı)		
41	Tedarikçinin denetimi altındaki Microsoft Kişisel veya Gizli Verilerine yetkisiz erişimi engellemek için erişim hakkı yönetimi yordamları oluşturmalı ve bunların devamlılığını sağlamalıdır.	Tedarikçi aşağıdakileri içeren bir erişim hakları yönetim planını uygulamaya koyduğunu kanıtlar: ▪ Erişim denetimi yordamları ▪ Kimlik saptama yordamları ▪ Başarısız denemelerden sonra kilitleme yordamları ▪ 90 günde birden daha uzun olmamak üzere gereken sıklıkta parola sıfırlaması ▪ Kimlik doğrulama bilgilerini seçmek için sağlam parametreler ve ▪ İş akdinin sona ermesiyle birlikte 48 saat içinde kullanıcı hesaplarının devre dışı bırakılması Tedarikçi, Microsoft Kişisel ve Gizli Verilerine kullanıcı erişimini inceleyerek en düşük öncelik ilkesini uygulayan bir süreç oluşturduğunu kanıtlar. Süreç şunları içerir: ▪ Açıkça tanımlanmış kullanıcı rolleri ▪ Rollere erişim onayını gözden geçiren ve gerekçelendiren yordamlar ve ▪ Microsoft rollerine erişim hakkı olan rollere sahip kullanıcıların ilgili grupta/rolde olmasının belgeli bir gerekçesine sahip olduğuna dair test	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik (devamı)		
42	Microsoft Kişisel veya Gizli Verilerinin İşlenmesinde kullanılan sistemlerin güvenlik yamalarını önceliklendiren yama yönetimi yordamları tanımlamalı ve uygulamalıdır. Bu yordamlar şunları içermelidir: ▪ Güvenlik yamalarını önceliklendirmeye yönelik tanımlı risk yaklaşımı ▪ Acil durum yamalarının işlenmesi ve uygulanması yeteneği ▪ 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 çıkarılmasına ilişkin gereksinimler	Tedarikçi bu gereksinimi karşılayacak şekilde uygulamaya konmuş bir yama yönetim yordamını kanıtlayabilir. Bu yordam asgari koşul olarak şunları kapsar: ▪ Önceliklendirmeyi bildirmek için önem derecesi atanması (Önem derecesi tanımları belgelenir.) ▪ Acil durum yamalarını uygulamak için belgelenmiş yordam ▪ Yazan şirket tarafından artık desteklenmeyen işletim sistemlerinin bir işe yaramadığını doğrulanması ▪ Onayları ve özel durumları izleyen yama yönetim kayıtları	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
43	Zararlı olabilecek virüslere ve kötü amaçlı yazılım uygulamalarına karşı koruma sağlamak amacıyla, sunucular, üretim ve eğitim masaüstü bilgisayarları dahil olmak üzere, Microsoft Kişisel ve Gizli Verilerinin İşlenmesinde kullanılan ağa bağlı ekipmanlara virüsten ve kötü amaçlı yazılımdan koruma yazılımı yüklemelidir. Kötü amaçlı yazılımdan koruma tanımları günde bir defa veya virüsten koruma/kötü amaçlı yazılımdan koruma yazılımı tedarikçisinin talimatına göre güncellenmelidir. Not: Bu, Linux dahil 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.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
44	Microsoft için yazılım geliştiren tedarikçiler, tasarım tabanlı güvenlik ilkelerini yapım sürecine dahil etmelidir.	Tedarikçi teknik belirtim belgeleri, geliştirme döngülerinde güvenlik doğrulaması için denetim noktaları içerir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik (devamı)		
45	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 giriş, kayıp ve diğer yetkisiz faaliyetler açısından izlemelidir. DLP programı asgari koşul olarak: ▪ Microsoft Kişisel veya Gizli Verilerini saklıyorsanız, endüstri standardında ana bilgisayar, 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 yordamları açıklamalıdır; ve ▪ Veri İhlali olayları algılandığında uygulanması gereken bir olay yanıtı ve yönetim işlemi tesis eder.	Bir güvenlik açığı veya Veri İhlali algılandığında verilecek tepkiyi yönlendirmek üzere, yordamlar ile dağıtılan belgelenmiş IDS/IPS mevcut olmalıdır.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
46	Olay yanıtından elde edilen Araştırma sonuçlarını üst yönetime ve Microsoft'a derhal bildirmelidir. *Microsoft'a bildirimde bulunmak için SSPAHelp@microsoft.com ile iletişime geçin.*	Olay yanıtı araştırma sonuçlarını Microsoft'a bildiren sistemler ve işlemler mevcut olmalıdır.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
47	Sistem yöneticileri, operasyon personeli, yönetim ve üçüncü taraflara yıllık güvenlik eğitimi verilmelidir.	Şunları içeren bir güvenlik eğitimi programı oluşturulmalıdır: ▪ Olay yanıtı için yıllık eğitim ve ▪ Kriz durumlarına etkili bir şekilde müdahale etmeyi kolaylaştırmak için olay simülasyonları ve otomatik mekanizmalar Kötü amaçlı yazılımların indirilmesiyle ilişkili riskler gibi olay önleme farkındalığı.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik (devamı)		
48	Tedarikçi, yedekleme planlama işlemlerinin Microsoft Kişisel ve Gizli Verilerini yetkisiz kullanımdan, erişimden, ifşadan, değiştirmeden ve yok edilmeden korumasını sağlamalıdır.	Tedarikçi, kuruluşun işleri kesintiye uğratan bir olayı nasıl yöneteceği ve yönetim tarafından onaylanmış bilgi güvenliği sürekliliği hedefleri temelinde bilgi güvenliğinin önceden belirlenmiş bir düzeyde olmasını nasıl sağlayacağına ilişkin ayrıntıları içeren belgelenmiş yanıt ve kurtarma yordamlarını kanıt olarak sunabilir. Tedarikçi, kritik verilerin düzenli olarak yedeklenmesi, güvenli şekilde saklanması ve etkili bir şekilde kurtarılmasına yönelik yordamlar tanımlayıp uyguladığına dair kanıt sunabilir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
49	İş sürekliliği ve olağanüstü durum kurtarma planları oluşturup bu planları test etmelidir.	Olağanüstü durum kurtarma planı aşağıdakilerin tümünü içermelidir: ▪ Bir sistemin tedarikçinin işletmesinin çalışması açısından kritik olup olmadığını belirlemeye yönelik tanımlanmış ölçütler. ▪ Bir olağanüstü durumda kurtarma amacıyla hedeflenmesi gereken kritik sistemler tanımlanmış ölçütler temelinde listelenmelidir. ▪ Her kritik sistem için, sistemi bilmeyen bir mühendisin uygulamayı 72 saat içinde kurtarabilmesini sağlayan tanımlanmış olağanüstü durum kurtarma yordamı. ▪ Kurtarma hedeflerine ulaşılabilmesini sağlamak için olağanüstü kurtarma planları yılda bir (veya daha sık) test edilmeli ve gözden geçirilmelidir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik (devamı)		
50	Bir kişiye Microsoft Kişisel veya Gizli Verilerine erişim imkanı vermeden önce o kişinin kimliğini doğrulamalıdır.	Tüm kimliklerin benzersiz olmasını ve her birinin Azure Active Directory gibi bir endüstri standardı kimlik doğrulama yöntemine sahip olmasını sağlamalıdır. Yükseltilmiş erişim (idari veya diğer türden gelişmiş ayrıcalıklar), akıllı kart veya telefon tabanlı kimlik doğrulayıcı gibi ikinci bir faktörün kullanılmasını gerektirmelidir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
51	Tedarikçi, ağlarda iletilen Microsoft Kişisel ve Gizli Verilerini, Aktarım Katmanı Güvenliği (“**TLS**”) veya İnternet Protokolü Güvenliği (“**IPsec**”) kullanan 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 uygulanmalıdır.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
52	Microsoft Kişisel veya Gizli Verilerine erişen veya bu bilgileri işleyen tüm tedarikçi cihazlarında (dizüstü bilgisayarlar, iş istasyonları vb.) disk tabanlı şifreleme kullanılmalıdır.	Microsoft Kişisel veya Gizli Verilerini işlemek için kullanılan tüm cihazları, Bitlocker ya da başka bir endüstri eşdeğeri disk şifrelemesi çözümünü karşılayacak şekilde şifrelenmelidir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik (devamı)		
53	Bekleme halindeyken (saklanırken) tüm Microsoft Kişisel ve/veya Gizli Verilerini şifreleyecek sistemler ve yordamlar (NIST 800-111 standardında açıklananlar gibi geçerli endüstri standartlarının kullanıldığı) mevcut olmalı ve şunların tümünü içermelidir: ▪ Kimlik bilgileri (örn. kullanıcı adı/parolalar) ▪ Ödeme aracı verileri (örn. kredi kartı ve banka hesabı numaraları) ▪ Göçmenlikle ilgili kişisel veriler ▪ Tıbbi profil verileri (örn. 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 bilgiler (örn. sosyal güvenlik veya sürücü ehliyeti numaraları) ▪ Microsoft müşterilerine ait veriler (örn. Sharepoint, O365 belgeleri, One Drive müşterileri) ▪ Duyurulmamış Microsoft ürünleriyle ilgili malzeme ▪ Doğum Tarihi ▪ Çocukların profil bilgileri ▪ Gerçek zamanlı coğrafi veriler ▪ Fiziksel kişisel (iş dışı) adres ▪ Kişisel (iş dışı) telefon numaraları ▪ Din ▪ Siyasi görüşler ▪ Cinsel yönelim/tercih ▪ Güvenlik sorusu yanıtları (örn. 2fa, parola sıfırlama) o Annenin kızlık soyadı	Bu satırda listelenen Microsoft Kişisel ve Gizli Verilerinin bekleme durumundayken şifrelendiği kontrol edilir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
54	Kredi kartlarında Microsoft adına işlem yapılırken kartı veren kuruluşun geçerli kredi kartı işleme standartlarına bağlı kalınmalıdır.	Her yıl bir Ödeme Kartı Endüstrisi Veri Hizmetleri Standardı ("**PCI-DSS**") sertifikası sunarak uyumluluğu kanıtlamalıdır. *PCI DSS sertifikaları SSPA'e sunulmalıdır. Lütfen her tür sorunuz için SSPAHelp@microsoft.com ile iletişime geçin.*	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Tedarikçi Veri Koruma Gereksinimleri	Uyumluluk Kanıtı	Yanıt
	Bölüm J: Güvenlik (devamı)		
55	Tedarikçi Microsoft'un fiziksel varlıklarını erişimin denetlendiği bir ortamda saklamalıdır.	Microsoft verilerinin dijital, yazdırılmış kopya, arşiv ve yedek kopyalarına fiziksel erişimi düzenleyen sistemler ve işlemler mevcut olmalıdır. Microsoft verilerini içeren fiziksel ortamların taşınması ve imhasına yönelik olarak delil zinciri izlenmelidir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
56	Geliştirme veya test ortamında kullanılan Microsoft Kişisel Verilerinin tümünü isimsizleştirmelidir.	Microsoft Kişisel Verileri geliştirme ve test ortamlarında kullanılmamalıdır; başka bir seçenek yoksa Veri Sahiplerinin tanınmasını veya Kişisel Verilerin kötüye kullanılmasını önlemek için isimsiz kullanım tercih edilmelidir. Not: İsimsizleştirilmiş veriler Takma Ad haline getirilmiş verilerden farklıdır. İsimsizleştirilmiş veriler kimliği belirlenmiş veya belirlenebilir bir gerçek kişiyle ilgili olmayan verilerdir; burada kişisel verilerin ait olduğu veri sahibinin kimliği belirlenemez veya artık belirlemek mümkün değildir.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*