



BAU

BAHÇEŞEHİR
UNIVERSITY

MICROSOFT 365 COPILOT KURUMSAL GÜVENLİK VE ETKİN KULLANIM KILAVUZU

*Akademik ve idari süreçlerde üretkenliği artıran; kurumsal veriyi,
insan sorumluluğunu ve güveni koruyan kullanım yönlendirmeleri*

Sürüm	01
Yayın Tarihi	29 Haziran 2026
Görüş ve İletişim	Yapay Zekâ Yetkinlik Birimi
Belge Koordinasyonu	Bilgi İşlem Daire Başkanlığı ve Yapay Zekâ Yetkinlik Birimi
Eğitim ve Kullanıcı Desteği	BAUPRO, Bilgi İşlem Daire Başkanlığı ve Yapay Zekâ Yetkinlik Birimi

Kılavuzu Nasıl Kullanmalısınız?

Bu Kılavuz, Microsoft 365 Copilot, Copilot Chat ve ilgili Copilot özelliklerini Bahçeşehir Üniversitesi ile bağlantılı eğitim, araştırma, çalışma, proje ve kurumsal görevlerde kullanırken dikkat edilmesi gereken hesap, veri, güvenlik, doğrulama ve insan sorumluluğu ilkelerini açıklar.

Copilot'u kullanmadan önce beş temel soru

1. Kurumsal BAU hesabımla mı, yoksa kişisel hesabımla mı oturum açtım?
2. Kullanacağım bilgi kamuya açık mı, kurum içi mi, kişisel veya gizli mi?
3. Bu bilgiyi işlemek ve Copilot ile kullanmak için gerekli görev yetkisine ve hukuki dayanağa sahip miyim?
4. Üretilen çıktıyı doğrulayabilecek ve sorumluluğunu üstlenebilecek miyim?
5. Kullanım; toplantı kaydı, kurumsal veri kaynağı, Copilot ajanı, eklenti, bağlayıcı veya başka kullanıcılarla paylaşım içeriyor mu?

Ek değerlendirme gerekebilir

Son sorunun yanıtı "evet" ise özelliği doğrudan kullanıma almadan önce teknik, veri koruma veya kurumsal değerlendirme gerekebilir.

Hızlı Bakış

Kullanım alanı	Genel yaklaşım
BAU kurumsal Microsoft 365 ortamı	BAU, çalışanları ve öğrencileri için kurumsal Microsoft 365 hesapları ve hizmetleri sağlar. Bu hesap, bütün gelişmiş Copilot özelliklerine otomatik erişim anlamına gelmez.
Copilot Chat- kurumsal hesap	Üniversitenin lisans ve teknik yapılandırması kapsamında erişilebilen konuşma tabanlı YZ hizmetidir. İşlevler kullanıcı lisansına ve etkinleştirilen özelliklere göre değişebilir.
Kişisel hesap veya bireysel abonelik	Çalışanlar ve öğrenciler kişisel Microsoft hesaplarıyla Microsoft Copilot'a erişebilir veya bireysel abonelik satın alabilir. BAU işi için kullanımda bu Kılavuz geçerlidir; kurum içi ve gizli bilgi kişisel hesaba aktarılmaz.
Gelişmiş Microsoft 365 Copilot	Word, Excel, PowerPoint, Outlook ve Teams gibi uygulamalarla bütünleşik gelişmiş kullanım ek lisans tahsisi ve gerekli kurumsal değerlendirmeyi gerektirebilir.
Kamuya açık veya düşük riskli içerik	Taslak, özet, fikir, dil iyileştirme ve genel analiz için kullanılabilir. Çıktı doğrulanmalıdır.
Kurum içi veya kontrollü içerik	Sadece kurumsal hesapta, görevle bağlantılı amaçla ve mevcut erişim yetkileri çerçevesinde kullanılmalıdır.
Kişisel, gizli veya sınırlı erişimli içerik	Kurumsal hesabın kullanılması tek başına yeterli değildir. Hukuki dayanak, görev yetkisi, veri asgarileştirme ve gerekli kurumsal kontroller sağlanmalıdır.
Resmî veya kişileri etkileyen kullanım	İnsan incelemesi ve yetkili onayı tamamlanmadan karar veya uygulamaya dönüştürülemez.

Temel ayırım

Kurumsal Microsoft 365 hesabı, gelişmiş Microsoft 365 Copilot lisansı değildir. Bir özelliğin kullanıcı arayüzünde görünmesi de her türlü kurumsal kullanım için onaylandığı anlamına gelmez.

İçindekiler

1. Kılavuzun Amacı.....	5
2. Kapsam.....	5
3. Copilot'a Kurumsal ve Kişisel Erişim.....	5
3.1. BAU Kurumsal Microsoft 365 Ortamı.....	5
3.2. Microsoft 365 Copilot Chat.....	6
3.3. Kişisel Hesaplar ve Bireysel Abonelikler.....	6
3.4. Kişisel Hesapla BAU Amaçlı Kullanım.....	6
4. Temel Yaklaşım: Copilot Destekler, Sorumluluk İnsanda Kalır.....	6
4.1. Amaçlı ve Ölçülü Kullanım.....	6
5. Kullanım İçeriklerinin Gizliliği ve Teknik Yönetim.....	7
5.1. BAU'nun Kurumsal Yaklaşımı.....	7
5.2. Teknik ve Toplu Kullanım Verileri.....	7
5.3. İstisnai Durumlar.....	7
6. Hesap, Erişim ve Lisans Kullanımı.....	7
6.1. Kurumsal Hesap.....	7
6.2. Kişisel Hesap.....	8
6.3. Gelişmiş Microsoft 365 Copilot Lisansı.....	8
6.4. Erişimin Gözden Geçirilmesi.....	8
7. Copilot'un Kurumsal Veriyle Çalışma Biçimi.....	8
7.1. Mevcut Erişim Yetkileri.....	8
7.2. Kurumsal Veri Koruması.....	8
7.3. Birleştirilmiş Bilginin Hassasiyeti.....	9
8. Bilginin Niteliğine Göre Güvenli Kullanım.....	9
8.1. Ortak Veri Kuralları.....	9
9. Etkin Kullanım Alanları.....	9
9.1. Akademik ve Öğretim Faaliyetleri.....	9
9.2. Araştırma ve Bilimsel Üretim.....	10
9.3. İdari ve Kurumsal Faaliyetler.....	10
9.4. Erişilebilirlik ve Dil Desteği.....	10
10. Microsoft 365 Uygulamalarında Kullanım Hatırlatmaları.....	10
11. İnsan Denetimi, Doğrulama ve Kalite Güvencesi.....	11
11.1. Copilot Kullanımının Açıklanması.....	11
12. Teams Toplantıları, Kayıt, Transkripsiyon ve Özetleme.....	11
12.1. Kullanımdan Önce.....	11
12.2. Hassas Toplantılar.....	12
12.3. Toplantı Çıktıları.....	12
13. Copilot Ajanları, Eklentiler ve Bağlayıcılar.....	12
13.1. Ajan Oluşturmadan Önce.....	12

13.2. Temel Kurallar.....	12
13.3. Ajan Paylaşımı.....	12
13.4. Eklenti ve Bağlayıcılar.....	13
14. Kayıt, Saklama ve Paylaşım.....	13
14.1. Paylaşmadan Önce.....	13
15. Kullanılmaması Gereken Durumlar.....	13
16. Hata, Olay ve İhlal Bildirimi.....	13
İlk adımlar.....	14
17. Kurumsal Roller ve Sorumluluklar.....	14
17.1. Kullanıcılar.....	14
17.2. Akademik ve İdari Birimler.....	14
17.3. Bilgi İşlem Daire Başkanlığı.....	14
17.4. Yapay Zekâ Yetkinlik Birimi.....	14
17.5. BAUPRO.....	14
17.6. Hukuk Müşavirliği.....	14
18. Destek ve Eğitim.....	15
19. Kullanmadan Önce Kısa Kontrol Listesi.....	15

Teknik özellikler, lisanslama ve arayüzler zaman içinde değişebilir. Güncel kurumsal kullanım koşullarında Bilgi İşlem Daire Başkanlığı duyuruları ve Bahçeşehir Üniversitesi düzenlemeleri esas alınır.

1. Kılavuzun Amacı

Bahçeşehir Üniversitesi, Microsoft 365 Copilot ve Copilot Chat hizmetlerini akademik, araştırma, idari ve kurumsal süreçlerde insan kapasitesini destekleyen üretkenlik araçları olarak değerlendirir. Bu Kılavuzun amacı, Copilot hizmetlerinin aşağıdaki amaçlarla güvenli ve etkin biçimde kullanılmasına yönelik uygulama yönlendirmesi sağlamaktır:

- Güvenli ve amaçla uyumlu kullanımın yaygınlaştırılması,
- Kurumsal verilerin ve kişisel verilerin korunması,
- İnsan değerlendirmesi ve nihai sorumluluğun sürdürülmesi,
- Üretilen içerik, analiz ve önerilerin doğrulanması,
- Hesap, erişim, paylaşım ve lisansların uygun şekilde yönetilmesi,
- Eğitim, araştırma ve idari süreçlerde ölçülü ve verimli kullanımın desteklenmesi.

Bu Kılavuz; Bahçeşehir Üniversitesi Yapay Zekâ Politikası, Sorumlu Yapay Zekâ Uygulama Usul ve Esasları, Çalışanlar İçin Yapay Zekâ Kullanım Rehberi, Öğrenciler İçin Yapay Zekâ Kullanım Rehberi, Kişisel Verilerin Korunması ve Veri Mahremiyeti Politikası ile bilgi güvenliği, fikrî ve sınai mülkiyet, akademik dürüstlük ve kayıt yönetimine ilişkin diğer Üniversite düzenlemeleriyle birlikte uygulanır.

2. Kapsam

Bu Kılavuz, kendilerine ilgili hizmet veya özelliğe erişim sağlandığı ölçüde aşağıdaki kullanıcıları kapsar:

- Akademik personel,
- İdari personel,
- Akademik ve idari yöneticiler,
- Araştırmacılar,
- Lisans ve lisansüstü öğrencileri,
- Üniversite adına proje veya hizmet yürüten yetkilendirilmiş kişiler.

Kılavuz aşağıdaki hizmet ve kullanım alanlarına uygulanır:

- Microsoft 365 Copilot Chat,
- Microsoft 365 Copilot,
- Word, Excel, PowerPoint, Outlook, Teams, OneDrive, SharePoint, OneNote ve Loop içindeki Copilot işlevleri,
- Copilot ajanları,
- Microsoft 365 Copilot ile ilişkili eklenti, bağlayıcı ve haricî veri bağlantıları,
- Microsoft tarafından sonradan kullanıma sunulan ve Üniversite tarafından etkinleştirilen ilgili Copilot özellikleri.

Bu Kılavuz, erişimin Üniversite tarafından sağlanan kurumsal hesap veya lisans üzerinden ya da kullanıcının kişisel hesabı ve bireysel aboneliği üzerinden gerçekleşmesine bakılmaksızın, Bahçeşehir Üniversitesiyle bağlantılı eğitim, araştırma, çalışma, proje, hizmet ve kurumsal görevlerdeki Copilot kullanımlarına uygulanır.

Tamamen kişisel amaçlı ve Üniversiteyle bağlantısı bulunmayan kullanımlar kurumsal iş akışı kapsamında değildir. Bununla birlikte kişisel verilerin korunması, bilgi güvenliği, fikrî haklar ve mesleki sorumluluklara ilişkin yükümlülükler devam eder.

3. Copilot'a Kurumsal ve Kişisel Erişim

3.1. BAU Kurumsal Microsoft 365 Ortamı

Bahçeşehir Üniversitesi, çalışanları ve öğrencileri için kurumsal Microsoft 365 hesapları ve hizmetleri sağlamaktadır. Word, Excel, PowerPoint, Outlook, Teams, OneDrive, SharePoint, OneNote ve diğer Microsoft 365 uygulamaları Üniversitenin kurumsal dijital çalışma ve öğrenme ortamının bir parçasıdır.

Kurumsal Microsoft 365 hesabına sahip olmak, Microsoft 365 Copilot'un bütün gelişmiş özelliklerine veya ek lisans gerektiren işlevlerine otomatik erişim sağlandığı anlamına gelmez. Kullanılabilir Copilot özellikleri; Üniversitenin sahip olduğu lisanslara, kullanıcıya yapılan lisans atamasına ve Bilgi İşlem Daire Başkanlığı tarafından uygulanan teknik yapılandırmalara göre değişebilir.

3.2. Microsoft 365 Copilot Chat

Microsoft 365 Copilot Chat, Üniversitenin lisans ve teknik yapılandırmaları kapsamında uygun kullanıcıların kurumsal iş veya okul hesaplarıyla erişebildiği konuşma tabanlı yapay zekâ hizmetidir.

Copilot Chat'in web, kurumsal dosya, ajan veya diğer iş verileriyle çalışma kapasitesi; kullanıcının lisansına, erişim yetkilerine ve Üniversite tarafından etkinleştirilen özelliklere bağlıdır.

3.3. Kişisel Hesaplar ve Bireysel Abonelikler

Çalışanlar ve öğrenciler, kişisel Microsoft hesapları üzerinden Microsoft Copilot'a erişebilir veya uygun bireysel Microsoft 365 aboneliklerini kendi imkânlarıyla satın alarak kişisel kullanıma yönelik Copilot özelliklerinden yararlanabilirler.

Kişisel Microsoft hesabı ile BAU tarafından sağlanan kurumsal iş veya okul hesabı ayrı hesap ve hizmet ortamlarıdır. Kişisel abonelik satın alınması, ilgili hesabı BAU tarafından sağlanan veya kurumsal kullanım için onaylanan bir hesap hâline getirmez.

3.4. Kişisel Hesapla BAU Amaçlı Kullanım

Kişisel hesap veya bireysel abonelik üzerinden BAU göreviyle bağlantılı bir çalışma yapılması, kullanıcının Üniversite düzenlemelerinden doğan sorumluluklarını ortadan kaldırmaz. Kişisel hesaplar, BAU ile bağlantılı düşük riskli görevlerde sadece aşağıdaki nitelikleri taşıyan bilgilerle kullanılabilir:

- Kamuya açık,
- Kişisel veri içermeyen,
- Gizli veya sınırlı erişimli olmayan,
- Sözleşme, lisans veya fikrî hak kısıtlaması bulunmayan.

Kişisel abonelik kurumsal yetki sağlamaz

Kullanıcının kişisel abonelik için ödeme yapmış olması; BAU'ya ait kurum içi dosya, kişisel veri, gizli bilgi veya sınırlı erişimli içeriği kişisel hesaba aktarma yetkisi vermez.

4. Temel Yaklaşım: Copilot Destekler, Sorumluluk İnsanda Kalır

Copilot; fikir geliştirme, taslak hazırlama, bilgi yapılandırma, metin sadeleştirme, dil ve anlatım iyileştirme, özetleme, tablo ve veri analizi, sunum hazırlama, görev planlama, araştırma desteği ve tekrarlayan görevlerin kolaylaştırılması amacıyla kullanılabilir.

Bununla birlikte Copilot aşağıdaki unsurların yerine geçmez:

- Akademik veya mesleki uzmanlık,
- İnsan muhakemesi,
- Bilimsel sorumluluk,
- Yetkili karar sahibi,
- Kurumsal onay, yetki ve imza sorumluluğu.

Kullanıcı, Copilot çıktısını anlayabilecek, sorgulayabilecek, doğrulayabilecek, değiştirebilecek veya reddedebilecek durumda olmalıdır.

Sorumluluk devredilemez

Bir içeriğin Copilot tarafından hazırlanmış olması, içeriği kullanan, paylaşan, onaylayan veya karara dönüştüren kişinin akademik, idari, hukuki ya da kurumsal sorumluluğunu ortadan kaldırmaz.

4.1. Amaçlı ve Ölçülü Kullanım

Copilot, işin niteliğine gerçek bir katkı sağladığında kullanılmalıdır. Kullanıcılar aynı isteği gereksiz yere tekrar etmekten, değer üretmeyen uzun ve amaçsız konuşmalardan ve daha basit yöntemle yapılabilecek işleri gereksiz biçimde YZ'ye aktarmaktan kaçınmalıdır.

Amaçlı ve hedefli kullanım; zamanın, işlem kaynaklarının ve kurumsal kapasitenin daha verimli kullanılmasını destekler.

5. Kullanım İçeriklerinin Gizliliği ve Teknik Yönetim

5.1. BAU'nun Kurumsal Yaklaşımı

Bahçeşehir Üniversitesi, olağan kullanım ve rutin kurumsal yönetim kapsamında kullanıcıların Copilot üzerindeki bireysel istemlerini, sohbetlerini, dosyalarını, taslaklarını, çalışma yöntemlerini ve ürettiği metin, analiz veya kodları içerik düzeyinde incelemeyiz; çalışan performansını veya öğrenci başarısını bu içeriklere dayanarak değerlendirmeyiz.

Çalışma içeriği performans ölçütü değildir

Kullanıcıların bireysel Copilot sohbetleri, istemleri veya çalışma içerikleri olağan yönetim kapsamında performans ya da başarı değerlendirmesi amacıyla kullanılmaz.

5.2. Teknik ve Toplu Kullanım Verileri

Kurumsal lisansların, güvenliğin, kaynakların ve hizmet sürekliliğinin yönetilmesi amacıyla aşağıdaki türden teknik veya toplu bilgiler izlenebilir:

- Hesabın veya lisansın etkinlik durumu,
- Belirli bir dönemde kullanım gerçekleşip gerçekleşmediği,
- Toplam veya grup düzeyindeki kullanım göstergeleri,
- Lisans ve kaynak kullanımı,
- Oluşturulan veya paylaşılan kurumsal ajanların adı, sahibi ve erişim durumu,
- Güvenlik veya uygunsuz kullanım uyarıları,
- Teknik hata ve hizmet kesintileri.

Bu veriler; lisans planlaması, kullanıcı desteği, eğitim ihtiyacının belirlenmesi, bilgi güvenliği ve hizmetin sürdürülebilirliği amacıyla kullanılabilir.

5.3. İstisnai Durumlar

Hukuki yükümlülük, bilgi güvenliği olayı, yetkili kurumsal inceleme, resmî soruşturma veya kullanıcının açık talebi ve izni bulunan istisnai durumlarda gerekli işlem yalnızca yetkili süreçler çerçevesinde ve gerekli olan ölçüde yürütülür.

BAU'nun kurumsal içerik gizliliği yaklaşımı, kişisel Microsoft hesapları ve kullanıcının kendi satın aldığı bireysel abonelikler için aynı kurumsal güvenceyi oluşturmaz. Bu hesaplarda hizmet sağlayıcının bireysel kullanım, saklama ve gizlilik koşulları geçerlidir.

6. Hesap, Erişim ve Lisans Kullanımı

6.1. Kurumsal Hesap

BAU görevleri kapsamında kurum içi bilgi, kurumsal belge veya Microsoft 365 içeriğiyle çalışılacaksa Üniversite tarafından sağlanan kurumsal Microsoft 365 hesabı kullanılmalıdır.

Kullanıcılar:

- Kişisel Microsoft hesaplarına kurumsal bilgi aktarmamalı,
- Kurumsal dosyaları kişisel bulut hesaplarına taşımamalı,
- Başka bir kişi adına oturum açmamalı,
- Hesap ve kimlik doğrulama bilgilerini paylaşmamalıdır.

Paylaşımlı kullanıcı hesabı, ortak oturum veya başka bir kullanıcı adına Copilot kullanımına izin verilmez.

6.2. Kişisel Hesap

Kişisel Microsoft hesapları ve bireysel abonelikler, BAU ile bağlantılı düşük riskli görevlerde sadece kamuya açık ve korunması gerekmeyen bilgilerle kullanılabilir. Kurum içi, kişisel, gizli veya sınırlı erişimli içerikler kişisel hesaba aktarılmamalıdır.

6.3. Gelişmiş Microsoft 365 Copilot Lisansı

Word, Excel, PowerPoint, Outlook, Teams ve diğer Microsoft 365 uygulamalarında kurumsal iş verisine dayalı gelişmiş Copilot özelliklerinden yararlanılması, uygun bir Microsoft 365 Copilot lisansının kullanıcıya atanmasını gerektirebilir.

Gelişmiş lisans talepleri aşağıdaki unsurlar dikkate alınarak değerlendirilir:

- Görevin niteliği ve iş ihtiyacı,
- Beklenen kullanım alanı ve kurumsal fayda,
- Lisans kapasitesi ve bütçe,
- Bilgi güvenliği ve veri gereksinimleri,
- Gerekli eğitim ve kullanıcı hazırlığı.

Teknik lisans atama, hesap ve yetkilendirme işlemleri Bilgi İşlem Daire Başkanlığı tarafından yürütülür. Yapay Zekâ Yetkinlik Birimi, kullanım ihtiyacının ve sorumlu kullanım koşullarının değerlendirilmesine katkı verir.

6.4. Erişimin Gözden Geçirilmesi

Aşağıdaki durumlarda erişim veya lisans gözden geçirilebilir:

- Üniversiteyle ilişkinin sona ermesi,
- Görev veya rol değişikliği,
- Lisans ihtiyacının ortadan kalkması,
- Uzun süreli etkin olmayan kullanım,
- Bilgi güvenliği riski,
- İlgili özelliğin Üniversite tarafından durdurulması,
- Gerekli eğitim veya kullanım koşullarının tamamlanmaması.

7. Copilot'un Kurumsal Veriyle Çalışma Biçimi

7.1. Mevcut Erişim Yetkileri

Microsoft 365 Copilot, kullanıcının Microsoft 365 ortamında erişmeye yetkili olduğu içeriklerden yararlanabilir. Kullanıcının erişim yetkisinin bulunmadığı belge veya veri için yeni bir erişim hakkı oluşturmaz.

Mevcut izinleri düzeltmez

Copilot, hatalı veya gereğinden geniş verilmiş mevcut erişim yetkilerini kendiliğinden düzeltmez. Yanlış paylaşılmış bir belge, o belgeye erişebilen kullanıcıların Copilot yanıtlarında daha kolay görünür hâle gelebilir.

Bu nedenle kullanıcılar:

- Dosya ve klasör paylaşım izinlerini kontrol etmeli,
- "Herkes" veya geniş grup bağlantılarını yalnızca gerçekten gerekli olduğunda kullanmalı,
- Hassas belgelerde alıcı ve erişim gruplarını doğrulamalı,
- Görev değişikliklerinde erişimlerin güncellenmesini sağlamalıdır.

7.2. Kurumsal Veri Koruması

Kurumsal hesap üzerinden kullanılan Microsoft 365 Copilot ve Copilot Chat kapsamındaki istemler, yanıtlar ve yetkili olunan kurumsal veriler Microsoft'un kurumsal veri koruma hükümlerine tabidir. Bu veriler, Microsoft'un kurumsal taahhütleri doğrultusunda temel yapay zekâ modellerinin eğitilmesi amacıyla kullanılmaz.

Kullanıcılar, Copilot'u kullanmadan önce doğru BAU hesabıyla oturum açtıklarını ve arayüzde kurumsal veri korumasının etkin olduğunu gösteren işaretin bulunduğunu kontrol etmelidir. Kurumsal koruma göstergesi bulunmuyorsa kişisel, kurum içi veya gizli bilgi girilmemeli ve teknik destek alınmalıdır.

7.3. Birleştirilmiş Bilginin Hassasiyeti

Copilot birden fazla belge veya kaynaktan bilgi birleştirebilir. Ayrı ayrı düşük veya orta hassasiyette olan bilgilerin bir araya getirilmesi, daha hassas bir sonuç ortaya çıkarabilir.

Bu nedenle Copilot çıktısı sadece tek tek kaynakların niteliğine göre değil, birleştirildiğinde ortaya çıkardığı yeni anlam, erişim ve gizlilik riski dikkate alınarak değerlendirilmelidir.

8. Bilginin Niteliğine Göre Güvenli Kullanım

Yeni bir sınıflandırma sistemi değildir

Bu bölüm, Üniversite için yeni veya bağımsız bir resmî bilgi sınıflandırma sistemi oluşturmaz. Çalışanlar ve Öğrenciler için Yapay Zekâ Kullanım Rehberlerinde benimsenen veri koruma ve risk yaklaşımını Microsoft Copilot kullanımına uygular. Üniversitenin yürürlükteki bilgi güvenliği veya sınıflandırma düzenlemelerinde daha ayrıntılı hükümler bulunması hâlinde bu hükümler ayrıca uygulanır.

Bilginin niteliği	Örnekler	Copilot kullanım yaklaşımı
Kamuya açık veya düşük riskli bilgi	Yayımlanmış web içerikleri, kamuya açık mevzuat ve raporlar, kişisel veri içermeyen genel taslaklar, anonim veya sentetik örnekler	Kurumsal hesapla kullanılabilir. Kişisel hesapla da kullanılabilir; çıktı doğrulanmalı, telif, lisans ve ders kuralları gözetilmelidir.
Kurum içi veya kontrollü bilgi	Rutin iç yazışmalar, yayımlanmamış idari taslaklar, hassas olmayan ders materyalleri, genel toplantı notları, birime ait çalışma belgeleri	Sadece BAU kurumsal Microsoft 365 hesabında, görevle bağlantılı amaçla ve mevcut erişim yetkileri çerçevesinde kullanılmalıdır. Kişisel hesaplara aktarılmamalıdır.
Kişisel, gizli veya sınırlı erişimli bilgi	Öğrenci ve personel bilgileri, sağlık ve özel nitelikli veriler, mali kayıtlar, İK ve disiplin belgeleri, hukuk dosyaları, uygulanmamış sınav materyalleri, gizli araştırma ve buluş bilgileri, üçüncü kişilere ait gizli içerikler	Kurumsal hesabın kullanılması tek başına yeterli değildir. Hukuki dayanak, görev yetkisi, amaçla sınırlılık, veri asgarileştirme ve gerekli kurumsal kontroller bulunmadan kullanılmamalıdır.
Güvenlik bilgileri	Şifreler, çok faktörlü doğrulama kodları, API anahtarları, erişim belirteçleri, özel anahtarlar	Kurumsal veya kişisel hiçbir Copilot istemine girilmemelidir.

8.1. Ortak Veri Kuralları

- Sadece işlem için gerekli olan en az miktarda veriyi kullanın.
- Mümkünse kişisel tanımlayıcıları kaldırın.
- Anonim veya sentetik örnekleri tercih edin.
- Belgenin tamamı yerine sadece gerekli bölümünü kullanın.
- Paylaşım ve işleme yetkinizi kontrol edin.
- Üçüncü kişilere ait lisanslı veya gizli içeriklerin kullanım koşullarını inceleyin.

Kurum içi olmak, otomatik olarak Copilot'a uygun olmak anlamına gelmez

Bilginin göreviniz için gerekli olup olmadığını, kullanım yetkinizi, hesabın türünü ve çıktının kimlerle paylaşılacağını ayrıca değerlendirin.

9. Etkin Kullanım Alanları

9.1. Akademik ve Öğretim Faaliyetleri

- Ders materyali ve etkinlik taslağı hazırlama,
- Örnek soru ve sentetik vaka geliştirme,
- Öğrenme çıktılarıyla uyumlu etkinlik fikirleri oluşturma,
- Kamuya açık kaynaklardan içerik yapılandırma,
- Sunum ve görselleştirme taslağı hazırlama,
- Öğrenci geri bildirimi için taslak yapı geliştirme.

Öğrenci kişisel verileri, henüz uygulanmamış nihai sınav soruları, cevap anahtarları ve korunan soru havuzları gerekli kontroller olmadan kullanılmamalıdır.

9.2. Araştırma ve Bilimsel Üretim

- Araştırma sorusu ve arama terimleri geliştirme,

- Literatürün yapılandırılması,
- Kod ve analiz taslağı oluşturma,
- Yöntem ve görselleştirme seçeneklerini değerlendirme,
- Proje veya fon başvurusu taslağı hazırlama,
- Dil ve anlatım iyileştirme,
- Hakem yanıtı için taslak oluşturma.

Kaynaklar, atıflar, yöntemler, hesaplamalar ve bilimsel iddialar birincil kaynaklardan doğrulanmalıdır. Gizli hakemlik belgeleri, tescilsiz buluş bilgileri ve yetkisiz araştırma verileri kullanılmamalıdır.

9.3. İdari ve Kurumsal Faaliyetler

- Yazışma, rapor, e-posta ve duyuru taslağı hazırlama,
- Toplantı gündemi ve eylem listesi oluşturma,
- Kamuya açık veya yetkili olunan bilgileri özetleme,
- Kontrol listesi ve süreç taslağı hazırlama,
- Sunum ve tablo oluşturma,
- Sık sorulan sorulara yanıt taslağı hazırlama,
- Düşük riskli veriler üzerinde sınıflandırma ve analiz yapma.

Copilot tarafından hazırlanan içerik, yetkili insan incelemesinden geçmeden resmî yazı, kurumsal görüş, karar, talimat veya taahhüt olarak kullanılmamalıdır.

9.4. Erişilebilirlik ve Dil Desteği

Copilot; sade dil, özet, alternatif anlatım, metin yapısının iyileştirilmesi ve düşük riskli içeriklerde çeviri taslağı amacıyla kullanılabilir. Hukuki, sağlıkla ilgili, güvenlik kritik, kurumsal itibarı etkileyen veya resmî nitelikteki çeviriler yalnızca Copilot çıktısına dayandırılmamalı; yetkin insan kontrolünden geçirilmelidir.

10. Microsoft 365 Uygulamalarında Kullanım Hatırlatmaları

Bahçeşehir Üniversitesi, çalışanları ve öğrencileri için kurumsal Microsoft 365 hizmetlerini ve hesaplarını sağlamaktadır. Microsoft 365 lisansına sahip olunması, bütün Copilot özelliklerine otomatik erişim sağlandığı anlamına gelmez.

Copilot Chat, uygulama içi Copilot özellikleri, kurumsal veriye dayalı yanıtlar, Teams toplantı özetleri, gelişmiş ajanlar ve diğer işlevlerin kullanılabilirliği; kullanıcının lisansına ve Üniversitenin teknik yapılandırmasına göre değişebilir. Ek lisans veya onay gerektiren özellikler, yalnızca kullanıcı arayüzünde görünür olmaları nedeniyle kurumsal olarak yetkilendirilmiş kabul edilmez.

Uygulama veya hizmet	Etkin kullanım	Özel dikkat noktası
Copilot Chat- kurumsal hesap	Fikir geliştirme, taslak hazırlama, web araştırması ve lisansın izin verdiği ölçüde dosya veya iş verisiyle çalışma	BAU hesabıyla oturum açıldığını ve kurumsal veri korumasının etkin olduğunu kontrol edin. Özelliklerin lisansa göre değişebileceğini dikkate alın.
Microsoft Copilot- kişisel hesap	Kamuya açık bilgilerle kişisel veya düşük riskli destek	BAU'ya ait kurum içi, kişisel, gizli veya sınırlı erişimli içerikleri kullanmayın. Kişisel abonelik kurumsal yetkilendirme sağlamaz.
Word	Taslak, özet, yeniden yapılandırma, anlatım iyileştirme	Kaynak, kişi, tarih, yükümlülük ve resmî ifadeleri doğrulayın.
Excel	Formül taslağı, tablo analizi, eğilim ve görselleştirme önerileri	Formülleri, veri aralıklarını, eksik değerleri ve hesaplamaları test edin.
PowerPoint	Sunum yapısı, slayt taslağı, görsel fikir ve konuşma notu	Kurumsal kimlik, doğruluk, erişilebilirlik ve görsel haklarını kontrol edin.
Outlook	E-posta taslağı, konu satırı, özet ve yanıt hazırlığı	Alıcıları, ekleri, taahhütleri, tarihleri ve gizli bilgileri gönderim öncesinde kontrol edin.
Teams	Toplantı hazırlığı, uygun toplantılarda transkripsiyon ve eylem maddeleri	Katılımcı bilgilendirmesi, kayıt yetkisi, gizlilik ve saklama kurallarını değerlendirin.

Uygulama veya hizmet	Etkin kullanım	Özel dikkat noktası
OneDrive ve SharePoint	Yetkili olunan belgeler üzerinden çalışma	Paylaşım izinlerini, anonim bağlantıları, eski kullanıcı erişimlerini ve veri sahibini kontrol edin.
Görsel üretim	Kavramsal görsel, sunum taslağı ve eğitim materyali	Gerçek kişi veya olayı yanıltıcı göstermeyin; görseli kanıt veya resmî kayıt gibi sunmayın.

11. İnsan Denetimi, Doğrulama ve Kalite Güvencesi

Copilot gerçek olmayan kaynak üretebilir, mevcut bir kaynağı yanlış aktarabilir, güncelliğini yitirmiş bilgi sunabilir, sayısal veya mantıksal hata yapabilir, dosyanın bağlamını eksik yorumlayabilir, önyargılı çıktı üretebilir ve ikna edici bir dille yanlış bilgi verebilir.

Bu nedenle kullanıcı:

1. Kritik iddiaları güvenilir ve birincil kaynaklardan doğrulamalıdır.
2. Kaynak, mevzuat, yayın ve bağlantıların gerçekten mevcut olduğunu kontrol etmelidir.
3. Sayısal sonuçları, formülleri, kodları ve analizleri test etmelidir.
4. Kurumsal bilgi için güncel ve yetkili BAU kaynaklarını esas almalıdır.
5. Tarih, kişi, görev, yetki, tutar ve kurumsal taahhütleri kontrol etmelidir.
6. Çıktıda önyargı, ayrımcılık veya dışlama riski bulunup bulunmadığını değerlendirmelidir.
7. Nihai metni amaç, hedef kitle ve kurumsal bağlama göre yeniden düzenlemelidir.
8. Önemli veya yüksek etkili işlerde doğrulama adımlarını gerektiğinde kayıt altına almalıdır.

Akıcı metin doğruluk garantisi değildir

Copilot'un akıcı, profesyonel ve ikna edici bir metin üretmesi, içeriğin doğru, güncel veya kurumsal olarak onaylanmış olduğu anlamına gelmez.

11.1. Copilot Kullanımının Açıklanması

Sadece yazım düzeltme, sadeleştirme veya fikir geliştirme gibi düşük düzeyli kullanımın her durumda ayrıca açıklanması gerekmez. Bununla birlikte Copilot kullanımı aşağıdaki durumlarda uygun biçimde açıklanmalıdır:

- Akademik veya bilimsel çıktının önemli bir bölümüne katkı sağlamışsa,
- Analiz, yöntem, kod veya yorum üretiminde belirleyici rol oynamışsa,
- Kamuya açık veya kurumsal öneme sahip içeriğin önemli kısmını oluşturmuşsa,
- Kişiler üzerinde etkisi bulunan bir karar destek sürecinde kullanılmışsa,
- İlgili ders, yayıncı, fon sağlayıcı veya kurumsal süreç açıklama talep ediyorsa,
- İçeriğin bütünüyle insan tarafından üretildiği izlenimi yanıltıcı olacaksa.

12. Teams Toplantıları, Kayıt, Transkripsiyon ve Özetleme

Teams toplantılarında Copilot, kayıt veya transkripsiyon özelliklerinin kullanımı toplantının mahiyeti dikkate alınarak değerlendirilmelidir.

12.1. Kullanımdan Önce

- Katılımcılar açık biçimde bilgilendirilmelidir.
- Toplantının kayıt veya transkripsiyona uygun olup olmadığı değerlendirilmelidir.
- Kullanımın amacı belirlenmelidir.
- Kişisel veri ve saklama koşulları kontrol edilmelidir.
- BAU dışından katılımcılar bulunuyorsa sözleşmesel ve gizlilik yükümlülükleri ayrıca değerlendirilmelidir.

12.2. Hassas Toplantılar

Gerekli özel yetkilendirme veya hukuki değerlendirme bulunmadıkça aşağıdaki konuların görüşüldüğü toplantılarda kayıt, transkripsiyon veya Copilot özetleme kullanılmamalıdır:

- Sağlık ve psikolojik danışmanlık bilgileri,
- Disiplin süreçleri,
- İnsan kaynakları ve performans değerlendirmeleri,
- Öğrenciye özgü hassas değerlendirmeler,
- Hukuki danışmanlık ve dava stratejileri,
- Avukat-müvekkil gizliliği kapsamındaki görüşmeler,
- Tescilsiz buluş veya gizli araştırma bilgileri,
- Üçüncü kişilere ait sözleşmeyle korunan bilgiler,
- Güvenlik olayları ve hassas sistem yapılandırmaları.

12.3. Toplantı Çıktıları

Copilot tarafından üretilen toplantı özeti resmî tutanak yerine geçmez; katılımcıların görüşlerini yanlış aktarabilir, karar ve görevleri yanlış kişilere bağlayabilir veya eksik sonuç üretebilir. Resmî veya kurumsal kaydolarak kullanılmadan önce toplantı sorumlusu tarafından kontrol edilmelidir.

13. Copilot Ajanları, Eklentiler ve Bağlayıcılar

Copilot ajanları, belirli bilgi kaynaklarını kullanmak, görevleri desteklemek veya iş akışlarını kolaylaştırmak amacıyla oluşturulabilir. Bir ajanın oluşturulmuş olması, kurumsal olarak onaylandığı veya Üniversite genelinde paylaşılabilmesi anlamına gelmez.

13.1. Ajan Oluşturmadan Önce

- Ajanın amacı ve kullanım kapsamı,
- Kurumsal sahibi, sorumlu kişi ve yedek sorumlu,
- Veri ve bilgi kaynakları,
- Hedef kullanıcı grubu ve erişim düzeyi,
- İnsan denetimi, bilinen sınırlar ve riskler,
- Güncelleme sıklığı ve geri bildirim kanalı,
- Kullanım dışı bırakma koşulları.

13.2. Temel Kurallar

Copilot ajanları:

- Kişileri etkileyen nihai kararları kendi başına veremez.
- Yetkisiz işlem başlatacak biçimde yapılandırılmaz.
- Şifre, erişim anahtarı veya kişisel kimlik bilgisi içeren talimatlarla kurulamaz.
- Görev amacıyla ilgisiz kurumsal kaynaklara bağlanamaz.
- Veri sahibinin bilgisi ve gerekli değerlendirme olmadan sınırlı erişimli kaynakla paylaşamaz.
- Bilinen sınırlarını kullanıcıdan gizleyemez.

13.3. Ajan Paylaşımı

- Kullanıcıların ajanın dayandığı kaynaklara erişim yetkisi doğrulanmalı,
- Sınırlı erişimli kaynak kullanılıyorsa veri veya içerik sahibinin görüşü alınmalı,
- Gereğinden geniş kullanıcı grupları seçilmemeli,
- Ajanın amacı ve sınırları kullanıcıya açıklanmalı,
- Erişim grupları belirli aralıklarla gözden geçirilmelidir.

Bir ajanın veya bağlayıcının erişiminin kaldırılması, ilgili dosya ve klasörlere daha önce verilmiş mevcut erişimleri kendiliğinden kaldırmayabilir. Dosya ve kaynak yetkileri ayrıca yönetilmelidir.

13.4. Eklenti ve Bağlayıcılar

Copilot ile haricî veri kaynakları veya hizmetler arasında bağlantı kuran eklenti ve bağlayıcılar; Bilgi İşlem Daire Başkanlığı tarafından teknik ve güvenlik yönünden, gerektiğinde Hukuk Müşavirliği tarafından sözleşme ve veri koruma yönünden, kullanım sahibi birim tarafından ise amaç ve veri kaynağı yönünden değerlendirilmeden kurumsal kullanıma açılmamalıdır.

Yanlış tanımlanmış bağlayıcı izinleri, hassas içeriğin amaçlanandan daha geniş kullanıcı kitlesine görünmesine neden olabilir.

14. Kayıt, Saklama ve Paylaşım

Copilot sohbetleri ve geçici çıktıları, önemli kurumsal kayıtların tek saklama alanı olarak kullanılmamalıdır.

Bir Copilot çıktısı aşağıdaki durumlarda uygun kurumsal belge veya kayıt alanına kaydedilmelidir:

- Karar sürecini etkiliyorsa,
- Resmî yazışmanın parçası oluyorsa,
- Sürekli kurumsal değere sahipse,
- Proje, araştırma veya idari işlem bakımından kanıt niteliği taşıyorsa.

Kaydedilen içerik uygun erişim düzeyiyle yönetilmeli, yalnızca yetkili kişilerle paylaşılmalı, Üniversitenin saklama ve imha kurallarına tabi tutulmalı ve güncelliğini kaybettiğinde arşivlenmeli veya kaldırılmalıdır.

14.1. Paylaşmadan Önce

- Alıcıların erişim yetkisini kontrol edin.
- Dosya bağlantısının kapsamını doğrulayın.
- Copilot'un kaynak olarak kullandığı belgelerde daha hassas bilgi bulunup bulunmadığını değerlendirin.
- Çıktının birden fazla kaynağı birleştirerek yeni bir gizlilik riski oluşturup oluşturmadığını kontrol edin.
- Gereksiz kişi, ek ve bağlantıları kaldırın.

15. Kullanılmaması Gereken Durumlar

Aşağıdaki kullanımlara izin verilmez:

- Öğrenci, personel veya üçüncü kişiler hakkında önemli sonuç doğuran nihai kararların Copilot'a devredilmesi,
- Copilot çıktısının doğrulanmadan resmî veya akademik çıktı olarak kullanılması,
- Uydurma veri, kaynak, atıf, delil, tutanak veya kayıt üretilmesi,
- Kişisel veya gizli bilgilerin gerekli yetki ve hukuki dayanak bulunmadan işlenmesi,
- Şifre, erişim anahtarı veya güvenlik belirtecinin isteme yazılması,
- Bilgi güvenliği kontrollerinin veya erişim yetkilerinin aşmaya çalışılması,
- BAU bilgilerinin kişisel hesaplara veya onaylanmamış haricî araçlara aktarılması,
- Başka kişilerin eserlerinin veya lisanslı içeriklerin hak sahibinin koşullarına aykırı biçimde kullanılması,
- Gerçek kişi veya olayları yanıltıcı biçimde taklit eden içerik üretilmesi,
- YZ tarafından üretilmiş içeriğin yanıltıcı biçimde tamamen insan ürünü olarak sunulması,
- Copilot ajanının onaylanmış amacı dışında kullanılması,
- Kurumsal veri kullanan ajanın yetkisiz veya gereğinden geniş kullanıcı grubuyla paylaşılması,
- İnsan denetiminin sadece biçimsel bir onaya indirgenmesi.

16. Hata, Olay ve İhlal Bildirimi

Aşağıdaki durumlardan biriyle karşılaşıldığında ilgili kurumsal kanala bildirim yapılmalıdır:

- Kişisel veya gizli bilginin yanlışlıkla Copilot'a girilmesi,
- Dosyanın veya ajanın yetkisiz kişilerle paylaşılması,
- Kurumsal hesabın ele geçirildiğine ilişkin şüphe,
- Hatalı yapılandırılmış ajan veya bağlayıcı,
- Copilot'un beklenmeyen biçimde hassas içerik göstermesi,
- Kurumsal etki doğurabilecek ciddi, ayrımcı veya zararlı çıktı,
- Güvenlik kontrolünü aşmaya yönelik girişim,
- Kişisel veri ihlali şüphesi.

İlk adımlar

1. İlgili işlemi durdurun.
2. Mümkünse paylaşımı kaldırın veya erişimi sınırlandırın.
3. Dosya, bağlantı, ekran görüntüsü ve zaman bilgisi gibi mevcut kayıtları koruyun.
4. İlgili birim yöneticisini ve Bilgi İşlem Daire Başkanlığını bilgilendirin.
5. Kişisel veri söz konusuysa Üniversitenin veri ihlali ve hukuki değerlendirme sürecinin başlatılmasını sağlayın.

Yapay Zekâ Yetkinlik Birimi, olayın YZ kullanım senaryosu, kullanıcı yönlendirmesi ve gerekli iyileştirme bakımından değerlendirilmesine katkı verir.

17. Kurumsal Roller ve Sorumluluklar

17.1. Kullanıcılar

- Kurumsal görevlerde uygun hesabı kullanır.
- Bu Kılavuza ve ilgili Üniversite düzenlemelerine uyar.
- Veriyi ve erişim yetkisini kontrol eder.
- Copilot çıktısını doğrular.
- Nihai sorumluluğu üstlenir.
- Olay ve hataları gecikmeksizin bildirir.
- Gerekli eğitimleri tamamlar.

17.2. Akademik ve İdari Birimler

- Copilot kullanım ihtiyacını ve beklenen kurumsal faydayı değerlendirir.
- Lisans taleplerini görev ve ihtiyaçla ilişkilendirir.
- Kendi veri ve içerik kaynaklarının sahipliğini belirler.
- Birim tarafından geliştirilen ajanların sorumlusunu atar.
- Erişim, güncelleme ve kullanım dışı bırakma süreçlerini takip eder.

17.3. Bilgi İşlem Daire Başkanlığı (BİDB)

- Hesap, lisans ve teknik erişim işlemlerini yürütür.
- Microsoft 365 yönetici yapılandırmalarını yönetir.
- Kimlik doğrulama, erişim ve güvenlik kontrollerini uygular.
- Ajan, eklenti ve bağlayıcıların teknik değerlendirmesini yapar.
- Teknik kullanım, hizmet sürekliliği ve güvenlik göstergelerini izler.
- Bilgi güvenliği olaylarına müdahale eder.
- Kullanıcılara teknik destek sağlar.

17.4. Yapay Zekâ Yetkinlik Birimi

- Kurumsal kullanım senaryoları ve sorumlu kullanım konusunda yönlendirme sağlar.
- Kılavuz ve destek içeriklerinin geliştirilmesini koordine eder.
- Lisans taleplerinin kullanım amacı ve kurumsal fayda bakımından değerlendirilmesine katkı verir.
- Kullanıcı geri bildirimlerini ve iyi uygulamaları toplar.
- Kurumsal ajanların amaç, sahiplik ve insan denetimi yaklaşımının geliştirilmesine katkı sağlar.
- Yapay Zekâ Yönlendirme Komitesine izleme ve değerlendirme bilgisi sunar.

17.5. BAUPRO

- Microsoft 365 Copilot eğitim içeriklerini hazırlar ve uygular.
- Role ve kullanım alanına göre eğitim yolları geliştirir.
- Eğitim katılım ve tamamlama kayıtlarını tutar.
- Eğitim içeriklerini BİDB ve Yapay Zekâ Yetkinlik Birimi katkısıyla günceller.

17.6. Hukuk Müşavirliği

- Kişisel verilerin korunması, sözleşme, fikrî haklar ve hukuki riskler konusunda görüş sağlar.
- Gerekli durumlarda ajan, bağlayıcı ve veri kullanım senaryolarının hukuki değerlendirmesine katkı verir.
- Hukuki olay ve ihlal süreçlerinde ilgili kurumsal birimlerle eşgüdüm sağlar.

18. Destek ve Eğitim

Kullanıcılar aşağıdaki alanlarda Üniversitenin sunduğu eğitim ve desteklerden yararlanabilir:

- Copilot Chat kullanımı,
- Microsoft 365 uygulamalarında Copilot,
- Etkili istem yazımı,
- Kurumsal veri güvenliği,
- Akademik ve araştırma kullanımı,
- İdari verimlilik,
- Teams toplantı özellikleri,
- Copilot ajanı oluşturma,

- Çıktı doğrulama,
- Olay ve hata bildirimi.

Gelişmiş Microsoft 365 Copilot lisansı verilen kullanıcıların Üniversite tarafından belirlenen temel eğitimi tamamlaması beklenir. Belirli özellikler veya yüksek etkili kullanım senaryoları için eğitim, kullanım ön koşulu olarak tanımlanabilir.

Yeni, belirsiz veya yüksek etkili bir kullanım senaryosunda özelliği doğrudan uygulamaya almak yerine ilgili akademik veya idari yöneticiye, Bilgi İşlem Daire Başkanlığına, Yapay Zekâ Yetkinlik Birimine ve gerektiğinde Hukuk Müşavirliğine danışılmalıdır.

19. Kullanmadan Önce Kısa Kontrol Listesi

- ☐ Kurumsal BAU hesabı mı yoksa kişisel hesabım mı açık, kontrol ettim.
- ☐ Kişisel hesap kullanıyorsam sadece kamuya açık ve düşük riskli bilgi kullanıyorum.
- ☐ Kurumsal Microsoft 365 hesabımın ilgili gelişmiş Copilot lisansını içerip içermediğini kontrol ettim.
- ☐ Bir özelliğin arayüzde görünmesinin kurumsal kullanım onayı anlamına gelmediğini biliyorum.
- ☐ Kurumsal veri korumasının etkin olduğunu kontrol ettim.
- ☐ Kullanacağım bilginin niteliğini değerlendirdim.
- ☐ Bu veriyi işlemek için görev yetkim ve gerekli hukuki dayanağım bulunuyor.
- ☐ Sadece gerekli olan en az miktarda veriyi kullanıyorum.
- ☐ Şifre, erişim anahtarı veya güvenlik belirteci paylaşmadım.
- ☐ Dosya ve kaynakların paylaşım izinlerini kontrol ettim.
- ☐ Copilot'un birden fazla kaynaktan daha hassas bir sonuç üretip üretmediğini değerlendirdim.
- ☐ Çıktının doğruluğunu, güncelliğini, kaynaklarını ve hesaplamalarını kontrol edeceğim.
- ☐ Nihai insan değerlendirmesi ve sorumluluk bende veya yetkili karar sahibinde kalıyor.
- ☐ Toplantı kaydı veya transkripsiyonu kullanıyorsam katılımcıları bilgilendirdim.
- ☐ Bir ajan veya bağlayıcı kullanıyorsam amacı, sahibi, kaynakları ve kullanıcı grubu belirli.
- ☐ Çıktıyı paylaşacağım kişilerin yetkili olduğunu kontrol ettim.
- ☐ Kullanımın açıklanması gerekip gerekmediğini değerlendirdim.
- ☐ Hata veya güvenlik olayı olursa hangi kanala bildireceğimi biliyorum.

Son kontrol

Bu maddelerden herhangi birini doğrulayamıyorsanız işlemi sürdürmeden önce gerekli düzeltmeyi yapın veya ilgili kurumsal destek kanalından görüş alın.

COPILOT'TAN YARARLAN • VERİYİ KORU • DOĞRULA • SORUMLULUĞU ÜSTLEN