YAPAY ZEKÂ RİSK DEĞERLENDİRME KILAVUZU

Yapay zekâ uygulamalarının ön inceleme, risk puanlama, kontrol, karar ve gözden geçirme süreçlerine yönelik kurumsal yönlendirme

Sürüm	01
Yayın Tarihi	29 Haziran 2026
Görüş ve İletişim	Yapay Zekâ Yetkinlik Birimi
Belge Koordinasyonu	Yapay Zekâ Yetkinlik Birimi
Teknik ve Hukuki Değerlendirme	Bilgi İşlem Daire Başkanlığı ve Hukuk Müşavirliği

Kılavuzu Nasıl Kullanmalısınız?

Bu Kılavuz, Bahçeşehir Üniversitesi bünyesinde kullanılan veya kullanılması planlanan yapay zekâ araçları, gömülü yapay zekâ özellikleri ve yapay zekâ destekli kullanım senaryolarının hangi durumlarda kurumsal değerlendirmeye tabi tutulacağını ve EK-1'de yer alan Risk Değerlendirme Formunun nasıl uygulanacağını açıklar.

Düşük riskli günlük kullanım için tam form aranmaz

Kamuya açık veya kişisel veri içermeyen bilgilerle çalışan, kişiler hakkında karar vermeyen, kurumsal sistemlerde işlem yapmayan ve çıktısı kolaylıkla kontrol edilebilen günlük kullanımlar; ilgili kullanıcı rehberleri çerçevesinde yürütülür. Bu tür kullanımlar için ayrıca tam risk değerlendirmesi yapılması gerekmez.

Değerlendirme Akışı

Adım	Sorumlu	Çıktı
1. Ön bildirim	Talep eden birim / uygulama sahibi	Kullanım amacı, ihtiyaç, hedef kullanıcı ve beklenen fayda
2. Ön sınıflandırma	Talep eden birim ve YZ Yetkinlik Birimi	Düşük, kontrollü, yüksek veya kabul edilemez ön risk seviyesi
3. Risk puanlama	Değerlendirme ekibi	Tekil risklerin olasılık ve etki puanları ile kontrol planı
4. Uzman incelemesi	BİDB, Hukuk Müşavirliği ve ilgili uzman birimler	Teknik, hukuki, veri koruma, etik, pedagojik veya diğer görüşler
5. Karar	Risk seviyesine göre yetkili birim veya kurul	Kullanım, pilot, revizyon, geçici durdurma veya ret kararı
6. Kayıt ve izleme	YZ Yetkinlik Birimi ve uygulama sahibi	Envanter kaydı, izleme yöntemi ve gözden geçirme tarihi

İçindekiler

1. Amaç ve Belgenin Konumu

Bu Kılavuzun amacı; Bahçeşehir Üniversitesi bünyesinde bir yapay zekâ aracının, gömülü yapay zekâ özelliğinin veya yapay zekâ destekli kullanım senaryosunun kurumsal kullanıma alınmasından önce risklerinin sistematik biçimde belirlenmesi, değerlendirilmesi, puanlanması ve karara bağlanmasına yönelik ortak yöntemi belirlemektir.

Bu Kılavuz ve EK-1'de yer alan Yapay Zekâ Risk Değerlendirme Formu, Sorumlu Yapay Zekâ Uygulama Usul ve Esaslarında anılan Yapay Zekâ Risk Değerlendirme Şablonunun uygulama aracıdır.

Kılavuz; Bahçeşehir Üniversitesi Yapay Zekâ Politikası, Sorumlu Yapay Zekâ Uygulama Usul ve Esasları, Yapay Zekâ Yönlendirme Komitesi Çalışma Usul ve Esasları, kişisel verilerin korunması, bilgi güvenliği, akademik dürüstlük, bilimsel etik ve fikrî haklara ilişkin diğer Üniversite düzenlemeleriyle birlikte uygulanır.

2. Kapsam ve Uygulama Eşiği

2.1. Kılavuzun Uygulandığı Durumlar

Bu Kılavuz aşağıdaki durumlarda uygulanır:

- Üniversite tarafından satın alınması, lisanslanması, geliştirilmesi veya kurumsal kullanıma sunulması planlanan YZ araçları ve sistemleri;
- Satın alınan veya kullanılan yazılımlara sonradan eklenen gömülü YZ özellikleri;
- Öğrencilere, personele, araştırmacılara, mezunlara, dış paydaşlara veya kamuya hizmet sunacak YZ uygulamaları;
- Kurumsal veri, kişisel veri veya kamuya açık olmayan bilgi kullanan uygulamalar;
- Üniversitenin bilgi sistemleri, veri kaynakları, ajanları, bağlayıcıları veya otomasyonlarıyla bütünleşen uygulamalar;
- Akademik, idari, mali veya yönetsel kararları destekleyen ya da kişiler üzerinde etki doğurabilecek kullanım senaryoları;
- Onaylanmış bir uygulamanın amacı, veri kapsamı, kullanıcı grubu, tedarikçisi, modeli, entegrasyonu veya işlem yetkisinde önemli değişiklik yapılması;
- Gözden geçirme takvimine göre yeniden değerlendirilmesi gereken kontrollü ve yüksek riskli uygulamalar.

2.2. Tam Değerlendirme Aranmayan Kullanımlar

Düşük riskli günlük kullanımlar için ayrı bir tam risk değerlendirmesi aranmaz. Bununla birlikte onaylı araç kullanımı, veri güvenliği, çıktı doğrulama, insan sorumluluğu ve ilgili kullanıcı rehberlerindeki kurallar uygulanır.

> **Teknik olarak mümkün olmak, kurumsal olarak uygun olmak değildir**
> Bir yapay zekâ özelliğinin bir yazılım içinde görünür veya kullanılabilir olması; kullanımın otomatik olarak onaylandığı, gerekli lisansın bulunduğu ya da verinin bu sistemle işlenebileceği anlamına gelmez.

3. Temel Kavramlar

Uygulama sahibi	YZ uygulamasının amacı, kapsamı, kontrolleri, insan denetimi, izlenmesi ve önemli değişikliklerinin bildirilmesinden kurumsal olarak sorumlu birim veya kişi.
Kurumsal Yapay Zekâ Envanteri	Üniversitede kullanılan, geliştirilen, değerlendirilen, pilotlanan veya planlanan YZ araçları ve kullanım senaryolarına ilişkin sahiplik, amaç, kullanılan veri, risk düzeyi, değerlendirme kararı ve gözden geçirme bilgilerinin Yapay Zekâ Yetkinlik Birimi tarafından tutulduğu ve güncellendiği merkezî kayıt listesi.
Kurumsal risk seviyesi	Uygulamanın bütünü için; kullanım amacı, etkilenen kişi ve gruplar, kullanılan veri, sistemin özerklik düzeyi ve muhtemel sonuçlar dikkate alınarak belirlenen düşük, kontrollü, yüksek veya kabul edilemez seviye.
Tekil risk puanı	Belirli bir riskin olasılık ve etki puanlarının çarpılmasıyla elde edilen ve riskin önceliklendirilmesi ile kontrol planının hazırlanmasında kullanılan skor.
Önemli değişiklik	Kullanım amacı, kullanıcı grubu, veri kaynağı, model, tedarikçi, entegrasyon, işlem yetkisi, ölçek veya güvenlik koşullarında önceki değerlendirmeyi etkileyebilecek değişiklik.

4. Değerlendirme Süreci ve Sorumluluklar

4.1. Talep Eden Birim ve Uygulama Sahibi

- Çözülmek istenen ihtiyacı, kullanım amacını, hedef kullanıcıları ve beklenen kurumsal faydayı açıklar.
- Formdaki bilgi ve belgelerin doğruluğunu sağlar; riskleri ve mevcut kontrolleri bildirir.
- Onaylanan kontrol, sınır ve koşulları uygular; insan denetimini sağlar.
- Önemli değişiklik, hata, olay ve beklenmeyen etkileri gecikmeksizin bildirir.

4.2. Yapay Zekâ Yetkinlik Birimi

- Başvuru, ön inceleme ve risk sınıflandırma sürecini koordine eder.
- Gerekli uzman görüşlerinin alınmasını sağlar ve değerlendirme kayıtlarını izler.
- Kontrollü ve yüksek riskli uygulamaları değerlendirme aşamasından itibaren Kurumsal Yapay Zekâ Envanterine kaydeder.
- Yüksek riskli veya stratejik uygulamaları Yapay Zekâ Yönlendirme Komitesi gündemine hazırlar.

4.3. Uzman Birimler ve Yetkili Kurullar

Uygulamanın niteliğine göre Bilgi İşlem Daire Başkanlığı, Hukuk Müşavirliği ve ilgili akademik veya idari birimler; bilgi güvenliği, teknik mimari, kişisel verilerin korunması, sözleşme, etik, akademik dürüstlük, ölçme-değerlendirme, fikrî haklar, satın alma, lisanslama ve erişilebilirlik alanlarında görüş verir.

İlgili mevzuat veya Üniversite düzenlemeleri uyarınca Senato, Rektörlük, etik kurul, disiplin organı, satın alma makamı veya başka bir yetkili kurulun kararı gerekiyorsa bu Kılavuz kapsamında yapılan değerlendirme söz konusu kararın yerine geçmez.

5. Kurumsal Risk Seviyeleri

Seviye	Temel ölçüt	Örnek yaklaşım	Asgari süreç
Seviye 1: Düşük risk	Kamuya açık veya kişisel veri içermeyen bilgi; kişiler hakkında karar yok, kurumsal sistemlerde işlem yok, çıktı kolay doğrulanabilir.	Fikir, ilk taslak, kamuya açık metin özeti, dil iyileştirme, örnek veriyle kodlama.	Tam form aranmaz; kullanıcı rehberleri ve genel kontroller uygulanır.
Seviye 2: Kontrollü risk	Belirli ders, birim veya kullanıcı grubuna hizmet; kurum içi içerik, doğrudan kullanıcı etkileşimi; sınırlı ancak anlamlı etki.	Ders asistanı, birim içi doküman asistanı, kişileri değerlendirmeyen öğrenci hizmeti asistanı.	Ön değerlendirme, uygulama sahibi, veri ve erişim sınırları, pilot ve dönemsel izleme.
Seviye 3: Yüksek risk	Özel nitelikli veya büyük ölçekli kişisel veri; profil/tahmin; akademik veya çalışma hayatını etkileme, sağlık; biyometri, işlem yetkisi, ciddi etki.	Not/burs/ilerleme karar desteği, işe alım veya performans desteği, sağlık ve psikolojik destek verisi, kurumsal sistemde işlem yapan ajan.	Tam değerlendirme, uzman görüşleri, belgelenmiş insan denetimi, kontrollü pilot ve Komite değerlendirmesi.
Seviye 4: Kabul edilemez kullanım	Nihai insan kararının tamamen YZ'ye bırakılması; izinsiz duygu veya kişilik çıkarımı, yetkisiz gözetim, veri/kanıt uydurma; güvenlik kontrollerini aşma, görünüşte insan denetimi.	Kurumsal kullanıma alınamaz. Araştırma amaçlı inceleme ancak gerçek kişiler üzerinde kullanılmama ve gerekli onaylarla ayrıca değerlendirilir.	Süreç durdurulur; kapsam yeniden tasarlanır veya talep reddedilir.

6. Risk Puanlaması ve Yorumlama

EK-1'de her tekil risk için olasılık ve etki 1 ile 5 arasında puanlanır. Risk skoru, olasılık ile etki puanının çarpılmasıyla hesaplanır. Puanlama; risklerin önceliklendirilmesi, ek kontrollerin belirlenmesi ve önlem sonrası kalıntı riskin izlenmesi amacıyla kullanılır.

Kurumsal risk seviyesi ile tekil risk puanı aynı değildir

Tekil risk puanı, uygulamanın genel risk seviyesini düşürmez. Uygulama; yüksek veya kabul edilemez risk tetikleyicisi taşıyorsa sayısal puanı daha düşük hesaplanmış olsa bile ilgili yüksek seviye uygulanır.

7. Karar, Kayıt ve Gözden Geçirme

Değerlendirme sonucunda aşağıdaki kararlardan biri verilir:

- Kullanıma uygun,
- Belirli koşullarla kullanıma uygun,
- Pilot uygulamaya uygun,
- Ek bilgi veya revizyon gerekli,
- Geçici olarak uygun değil,
- Kullanıma uygun değil.

Kararda uygulama sahibi, kullanım kapsamı, gerekli kontroller, izin verilen veri ve kullanıcı sınırları, izleme yöntemi, durdurma koşulları ve gözden geçirme tarihi belirtilir.

Kontrollü ve yüksek riskli uygulamalar değerlendirme aşamasından itibaren Kurumsal Yapay Zekâ Envanterine kaydedilir. Formdaki envanter kayıt numarası, değerlendirme tamamlandıktan sonra Yapay Zekâ Yetkinlik Birimi tarafından doldurulur.

Kullanım amacı, kullanıcı grubu, veri kaynağı, model veya hizmet sağlayıcı, entegrasyon, işlem yetkisi, kullanım ölçeği ya da güvenlik ve sözleşme koşullarında önemli değişiklik olması hâlinde uygulama yeniden değerlendirilir.

8. Gözden Geçirme ve Belge Yönetimi

Kullanıma alınan YZ uygulamaları risk seviyeleriyle orantılı olarak izlenir. İzleme dönemleri, sorumluları ve beklenen çıktılar Yapay Zekâ Gözden Geçirme ve İzleme Takviminde belirlenir.

Bu Kılavuz; teknolojik gelişmeler, mevzuat değişiklikleri, uygulama deneyimleri, risk ve olay kayıtları, kullanıcı geri bildirimleri ile Üniversitenin Yapay Zekâ Politikası ve Yol Haritasındaki değişiklikler dikkate alınarak en az yılda bir kez gözden geçirilir.

EK-1

YAPAY ZEKÂ RİSK DEĞERLENDİRME FORMU

Uygulama bazlı risk, kontrol, karar ve gözden geçirme kaydı

Doldurma sırası

Bölüm A ile uygulama ve kullanım senaryosu tanımlanır; Bölüm B ile ön risk seviyesi belirlenir; Bölüm C ve D ile tekil riskler puanlanır ve kontrol planı oluşturulur; Bölüm E ile veri koruma ön taraması tamamlanır; Bölüm F ve G ile karar, kayıt ve onay süreci sonuçlandırılır.

Bölüm A — Genel Bilgiler

Değerlendirme No	[YZR-YYYY-###]
Tarih	[GG.AA.YYYY]
Talep Eden Birim	[Birim adı]
Uygulama Sahibi	[Birim / Ad Soyad / Unvan]
Değerlendirmeyi Yapan(lar)	[Ad Soyad / Unvan]
Araç / Senaryo Adı	[Ad]
Tedarikçi ve Sürüm / Plan	[Tedarikçi, sürüm veya abonelik planı]
Konu Türü	☐ Yeni araç ☐ Gömülü YZ özelliği ☐ Kullanım senaryosu ☐ Değişiklik ☐ Periyodik gözden geçirme
Çözülmek İstenen İhtiyaç	[Mevcut sorun, ihtiyaç veya fırsat]
Kullanım Amacı ve Kapsamı	[Aracın veya senaryonun amacı, kapsamı ve beklenen çıktısı]
Beklenen Kurumsal Fayda	[Eğitim, araştırma, hizmet, verimlilik, kalite veya diğer fayda]
Başarı Ölçütleri	[Uygulamanın başarılı sayılacağı göstergeler]
Hedef Kullanıcılar	☐ Akademik personel ☐ İdari personel ☐ Araştırmacılar ☐ Öğrenciler ☐ Dış paydaşlar ☐ Kamu
Etkilenen Gruplar	☐ Öğrenciler ☐ Personel ☐ Hastalar ☐ Adaylar ☐ Araştırma katılımcıları ☐ Kamu ☐ Diğer: _____
Kullanılacak Bilgi veya Verinin Niteliği	☐ Kamuya açık / düşük riskli ☐ Kurum içi / kontrollü ☐ Kişisel veri ☐ Özel nitelikli kişisel veri ☐ Gizli / sınırlı erişimli kurumsal bilgi ☐ Araştırma verisi ☐ Fikrî hak unsuru ☐ Üçüncü kişiye ait sözleşmeyle korunan bilgi ☐ Güvenlik veya erişim bilgisi ☐ Veri kullanılmayacak ☐ Diğer: _____
Veri İşleme Konumu	☐ Türkiye ☐ Yurt dışı ☐ Bilinmiyor / teyit edilecek
Verilerin Model Eğitiminde Kullanımı	☐ Sözleşmeyle engellenmiş ☐ Ayarla kapatılabilir ☐ Engellenemiyor ☐ Bilinmiyor
Sistem İşlevi / Özerklik Düzeyi	☐ Taslak veya içerik desteği ☐ Öneri ☐ Karar desteği ☐ Otomatik işlem / eylem
Mevcut Durum	☐ Fikir / ön inceleme ☐ Pilot ☐ Üretim kullanımı ☐ Değişiklik değerlendirmesi ☐ Periyodik gözden geçirme

Bölüm B — Ön Sınıflandırma

B.1. Kabul Edilemez Kullanım Kontrolü

Aşağıdakilerden herhangi biri işaretlenirse kullanım kapsamı yeniden tasarlanır veya talep reddedilir. Yalnızca araştırma amacıyla inceleme, gerçek kişiler üzerinde kullanılmama ve gerekli etik, hukuki ve güvenlik onaylarıyla ayrıca değerlendirilebilir.

Kabul edilemez kullanım	İşaret
Not, kabul, burs, disiplin, işe alım, performans, terfi veya iş ilişkisinin sona ermesi gibi kişileri önemli ölçüde etkileyen nihai kararların tamamen YZ sistemine bırakılması.	☐
Kişiler hakkında genel güvenilirlik, değer, uygunluk veya davranış puanı oluşturulması.	☐
Eğitim veya çalışma ortamlarında kişilerin duygu, kişilik veya hassas özelliklerinin izinsiz biçimde çıkarılması ve karar süreçlerinde kullanılması.	☐
Yetkisiz biyometrik izleme, kitlesel gözetim veya kişilerin kırılganlıklarından yararlanılarak davranışlarının yönlendirilmesi.	☐
Kişisel, gizli veya kamuya açık olmayan kurumsal verilerin gerekli değerlendirme ve yetkilendirme olmadan YZ sistemleriyle işlenmesi.	☐
YZ aracılığıyla veri, kaynak, atıf, delil, kimlik veya resmî kayıt uydurulması ya da güvenlik kontrollerinin aşılması.	☐
İnsan denetiminin yalnızca görünüşte bulunduğu ve YZ çıktısının sorgulanmadan uygulandığı karar süreci.	☐

B.2. Yüksek Risk Göstergeleri

Aşağıdaki sorulardan herhangi birine “Evet” yanıtı verilmesi hâlinde uygulama kural olarak yüksek riskli değerlendirilir ve Bölüm C-E eksiksiz doldurulur. Nihai sınıflandırma somut kullanım senaryosu üzerinden yapılır.

Soru	Evet	Hayır
Ölçme-değerlendirme, kabul, burs, akademik ilerleme, disiplin veya hizmete erişim kararlarını etkiliyor mu?	☐	☐
İşe alım, görevlendirme, performans, terfi veya çalışma ilişkisini etkiliyor mu?	☐	☐
Sağlık, psikolojik danışmanlık veya özel destek ihtiyacına ilişkin veri ya da süreç içeriyor mu?	☐	☐
Özel nitelikli kişisel veri veya kişisel verileri geniş ölçekte ya da sistematik biçimde işliyor mu?	☐	☐
Kişiler hakkında profil, tahmin, sınıflandırma veya risk değerlendirmesi üretiyor mu?	☐	☐
Biyometrik veri, kimlik doğrulama veya davranış izleme işlevi kullanıyor mu?	☐	☐
Kurumsal bilgi sistemlerinde kayıt oluşturma, değiştirme, silme veya işlem yapma yetkisi var mı?	☐	☐
Hatalı çıktısı kişilerin hakları veya Üniversitenin hukuki, mali, akademik, güvenlik ya da itibari durumu üzerinde önemli etki doğurabilir mi?	☐	☐
Çıktının bağımsız olarak doğrulanması veya açıklanması güç mü?	☐	☐

B.3. Ön Risk Seviyesi Sonucu

Risk seviyesi	Ölçüt ve uygulanacak süreç
☐ Seviye 4 – Kabul edilemez kullanım	B.1’de en az bir işaret vardır. Kullanım kapsamı yeniden tasarlanır veya talep reddedilir; gerekçe Bölüm F’de belirtilir.

Risk seviyesi	Ölçüt ve uygulanacak süreç
☐ Seviye 3 – Yüksek risk	B.2'de yüksek risk göstergesi vardır. Tam değerlendirme, ilgili uzman görüşleri, kontrollü pilot, belgelenmiş insan denetimi ve gerektiğinde Komite değerlendirmesi uygulanır.
☐ Seviye 2 – Kontrollü risk	Belirli ders, birim veya kullanıcı grubuna hizmet; kurum içi kaynak; doğrudan etkileşim; ajan/entegrasyon veya sınırlı ancak anlamlı etki vardır. Ön değerlendirme, sahiplik, veri ve erişim sınırları, pilot ve dönemsel izleme uygulanır.
☐ Seviye 1 – Düşük risk	Yalnızca kamuya açık veya kişisel veri içermeyen bilgi kullanılır; kişiler hakkında karar yoktur; kurumsal sistemde işlem yapılmaz; çıktı kolay doğrulanır. Tam değerlendirme kural olarak aranmaz.

Bölüm C — Puanlama Ölçekleri ve Risk Matrisi

Puanlama notu
Bu bölümdeki skorlar tekil risk bulgularının önceliklendirilmesi için kullanılır. Tekil risk puanı, uygulamanın B.3'te belirlenen genel risk seviyesini düşürmez.

C.1. Olasılık Ölçeği

Puan	Düzey	Tanım
1	Nadir	Yalnızca istisnai koşullarda gerçekleşebilir.
2	Düşük	Gerçekleşme olasılığı düşüktür; bilinen örnek azdır.
3	Orta	Normal kullanımda makul olasılıkla gerçekleşebilir.
4	Yüksek	Birçok kullanım durumunda gerçekleşmesi beklenir.
5	Neredeyse kesin	Önlem alınmazsa normal kullanımda kaçınılmazdır.

C.2. Etki Ölçeği

Puan	Düzey	Tanım
1	Çok düşük	İhmal edilebilir etki; kişisel veri yok, küçük ve kolay geri alınabilir iç verimlilik etkisi.
2	Düşük	Sınırlı, yerel ve kolay giderilebilir etki; önemli hak, güvenlik veya hizmet sonucu doğurmaz.
3	Orta	Birim düzeyinde aksama; sınırlı sayıda kişi üzerinde olumsuz etki, anlamlı hizmet, öğrenme veya itibar etkisi.
4	Yüksek	Kişisel veri ihlali olasılığı; kişiler için hak kaybı, önemli akademik, hukuki, mali, güvenlik veya itibar etkisi.
5	Kritik	Özel nitelikli veya büyük ölçekli veri ihlali; kişiler için ciddi sonuç, ağır hukuki, güvenlik, akreditasyon veya kurumsal süreklilik etkisi.

C.3. Risk Matrisi (Skor = Olasılık × Etki)

Etki \ Olasılık	1	2	3	4	5
5 – Kritik	5	10	15	20	25
4 – Yüksek	4	8	12	16	20

Etki \ Olasılık	1	2	3	4	5
3 – Orta	3	6	9	12	15
2 – Düşük	2	4	6	8	10
1 – Çok düşük	1	2	3	4	5

C.4. Tekil Risk Bantları ve Gerekli Aksiyonlar

Skor	Düzey	Gerekli aksiyon
1–4	Düşük	Kabul edilebilir. Mevcut kontroller sürdürülür ve kayıt altına alınır.
5–9	Orta	Ek kontrollerle kabul edilebilir. Önlemler ve sorumlular belirlenir.
10–15	Yüksek	Risk azaltım planı zorunludur. İlgili uzman birim incelemesi ve koşullu karar gerekir.
16–25	Çok yüksek	Kabul edilemez tekil risk. Kullanım yeniden tasarlanır; kalıntı risk bu bantta bırakılamaz.

Bölüm D — Risk Kaydı

Aşağıdaki kayıt yaygın risk başlıklarıyla önceden doldurulmuştur. İlgili olmayan satırlar “UD” (uygulanamaz) olarak işaretlenir; senaryoya özgü riskler eklenir. O = Olasılık, E = Etki; Kalıntı = kontroller sonrası beklenen skor.

No	Risk tanımı	O	E	Skor	Mevcut kontroller ve ek önlemler	Sorumlu / Termin	Kalıntı
1	Kişisel, gizli veya sınırlı erişimli bilginin yetkisiz biçimde araca girilmesi						
2	Yanlış veya uydurma çıktının doğrulanmadan kullanılması						
3	Önyargılı çıktı nedeniyle haksız veya ayrımcı değerlendirme						
4	İnsan denetiminin yetersiz veya yalnızca biçimsel kalması						
5	Akademik dürüstlük ihlallerinin kolaylaşması						
6	Gerekli YZ açıklaması veya etiketlemesinin yapılmaması						
7	Telif, lisans veya fikrî hak ihlali taşıyan girdi ya da çıktı						
8	Hesap ele geçirme, veri sızıntısı, oltalama veya yetkisiz erişim						
9	Hizmet kesintisi ve tedarikçiye aşırı bağımlılık						
10	Sözleşmede veri işleme, saklama veya aktarım güvencelerinin eksikliği						

No	Risk tanımı	O	E	Skor	Mevcut kontroller ve ek önlemler	Sorumlu / Termin	Kalıntı
11	Uygunsuz veya sentetik içerik kaynaklı kurumsal itibar kaybı						
12	Öğrencilere yönelik kullanımın öğrenci kurallarıyla çelişmesi						
13	[Senaryoya özgü risk]						
14	[Senaryoya özgü risk]						

Bölüm E — Kişisel Verilerin Korunması ve Veri Güvenliği Ön Taraması

Herhangi bir soruya “Evet” yanıtı verilmesi hâlinde kullanım senaryosu, uygulamanın niteliğine göre Hukuk Müşavirliği, Bilgi İşlem Daire Başkanlığı ve Üniversitenin ilgili veri koruma süreçleri tarafından değerlendirilir. Kişisel veri işlenmesi hâlinde hukuki sebep, amaçla sınırlılık, veri asgarileştirme, saklama, aktarım, güvenlik tedbirleri ve gerekli bilgilendirme süreçleri ayrıca incelenir.

Soru	Evet	Hayır	Açıklama / Kanıt
Kişisel veri işlenecek mi?	☐	☐	
Özel nitelikli kişisel veri işlenecek mi?	☐	☐	
18 yaş altı kişilere ilişkin veri işlenecek mi?	☐	☐	
Yurt dışına veri aktarımı olacak mı?	☐	☐	
Profilleme veya kişiler hakkında otomatik değerlendirme var mı?	☐	☐	
Yeni bir veri toplama faaliyeti gerektiriyor mu?	☐	☐	
Aydınlatma metinlerinin veya veri işleme kayıtlarının güncellenmesi gerekiyor mu?	☐	☐	
Saklama, silme, alt hizmet sağlayıcı veya model eğitimi koşullarında belirsizlik bulunuyor mu?	☐	☐	

Bölüm F — Değerlendirme Sonucu ve Karar

Nihai Kurumsal Risk Seviyesi	☐ Seviye 1 – Düşük ☐ Seviye 2 – Kontrollü ☐ Seviye 3 – Yüksek ☐ Seviye 4 – Kabul edilemez kullanım
En Yüksek Tekil Risk Skoru	İlk skor: _____ Kalıntı skor: _____
Karar	☐ Kullanıma uygun ☐ Belirli koşullarla kullanıma uygun ☐ Pilot uygulamaya uygun ☐ Ek bilgi veya revizyon gerekli ☐ Geçici olarak uygun değil ☐ Kullanıma uygun değil
Koşullar / Gerekçe	[Karar şartları, ret gerekçesi veya tamamlanması gereken revizyonlar]
Onaylanan Kullanım Kapsamı	[Amaç, kullanıcı grubu, izin verilen işlevler]
Veri ve Erişim Sınırları	[İzin verilen veri türleri, kaynaklar ve erişim grupları]
Zorunlu Kontroller	[İnsan denetimi, teknik, hukuki, pedagojik veya diğer kontroller]

İzleme Göstergeleri ve Durdurma Koşulları	[Performans, hata, şikâyet, veri ve güvenlik göstergeleri]
Kurumsal Yapay Zekâ Envanteri Kayıt No	[Değerlendirme tamamlandıktan sonra YZ Yetkinlik Birimi tarafından doldurulur.]
İlk Gözden Geçirme Tarihi	[Yapay Zekâ Gözden Geçirme ve İzleme Takvimine göre]

Bölüm G — Görüş, Onay ve İmzalar

İmza ve görüşler uygulamanın risk seviyesi ve niteliğine göre tamamlanır. İlgili olmayan satırlar “UD” olarak işaretlenebilir.

Rol	Ad Soyad / Unvan	Görüş / Karar	Tarih	İmza
Talep Eden Birim Yöneticisi				
Uygulama Sahibi				
Yapay Zekâ Yetkinlik Birimi				
Bilgi İşlem Daire Başkanlığı (gerektiğinde)				
Hukuk Müşavirliği / ilgili veri koruma süreci (gerektiğinde)				
Akademik, etik, pedagojik veya diğer uzman görüşü (gerektiğinde)				
Yapay Zekâ Yönlendirme Komitesi / Yetkili Onay Makamı (gerektiğinde)				

Yetkili kurul ve makamlar

Bu değerlendirme; ilgili mevzuat veya Üniversite düzenlemeleri uyarınca gerekli olan Senato, Rektörlük, etik kurul, disiplin organı, satın alma makamı veya diğer yetkili kurul ve makam kararlarının yerine geçmez.

Yöntemsel Kaynaklar

1. Bahçeşehir Üniversitesi Yapay Zekâ Politikası.
2. Bahçeşehir Üniversitesi Sorumlu Yapay Zekâ Uygulama Usul ve Esasları.
3. Avrupa Birliği Yapay Zekâ Tüzüğü (Regulation (EU) 2024/1689) – risk temelli yaklaşım ve yüksek riskli kullanım alanları.
4. Kişisel Verileri Koruma Kurumu – Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler (2021) ve Üretken Yapay Zekâ ve Kişisel Verilerin Korunması Rehberi (2025).
5. Yükseköğretim Kurulu – Üretken Yapay Zekâ Kullanımına Dair Etik Rehber (2024).
6. ISO/IEC 23894:2023 – Artificial Intelligence: Guidance on Risk Management.
7. ISO/IEC 42001:2023 – Artificial Intelligence Management Systems.
8. NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0, 2023).