Zorlu Holding · Teknoloji ve Dijital İş Geliştirme Grup Başkanlığı

YAPAY ZEKA YÖNETİM ÇERÇEVESİ

AI Governance Framework

ZORLU

2026

İÇİNDEKİLER

İçindekiler

01 · NEDEN BİR YAPAY ZEKA YÖNETİM ÇERÇEVESİ?

Neden Bir Yapay Zeka Yönetim Çerçevesi?

Kurumların çoğu için asıl soru yapay zekayı kullanıp kullanmamak değil, onu nasıl güvenli, etik ve hukuka uygun biçimde kullanacağıdır.

Yapay zeka, kurumların çalışma biçimini hızla dönüştürüyor. Bu dönüşüm önemli fırsatlar sunarken; veri güvenliği, kişisel verilerin korunması, ayrımcılık, fikri mülkiyet ve itibar gibi alanlarda yeni riskler de doğuruyor.

Zorlu Holding olarak bu soruya sistematik bir yanıt vermek amacıyla bir Yapay Zeka Yönetim Çerçevesi oluşturduk. Bu çerçeve, yapay zeka sistemlerinin fikir aşamasından devre dışı bırakılmasına kadar tüm yaşam döngüsü boyunca hangi ilkelerle yönetileceğini, kimin neyden sorumlu olduğunu, risklerin nasıl sınıflandırılıp yönetileceğini ve raporlamanın nasıl işleyeceğini tanımlar.

Aşağıdaki bölümler, çerçevenin başlıca unsurlarını özetler: uluslararası standartlarla uyumlu risk sınıflandırması, sorumlu yapay zeka ilkeleri, yönetişim yapısı, proje yaşam döngüsü, veri güvenliği, ajan ve MCP yönetimi, çalışan farkındalığı ve gölge yapay zekanın önlenmesi.

BU BELGE HAKKINDA

Bu doküman, Zorlu Holding'in kurum içi Yapay Zeka Yönetim Çerçevesi'nin kamuya açık özetidir. Kurumsal yapay zeka yönetişimine yaklaşımımızı ana hatlarıyla paylaşmayı ve alanında çalışan meslektaşlarımıza kullanışlı bir referans sunmayı amaçlar. Kuruma özgü uygulama parametreleri, iç kontrol eşikleri ve operasyonel detaylar bu sürümün dışında tutulmuştur. Bu doküman hukuki görüş niteliği taşımaz.

KONUMLANDIRMA NOTU

Bu çerçevedeki bazı uygulamalar hâlihazırda kurum bünyesinde hayata geçirilmiş, bir kısmı ise hedef durum olarak tanımlanmıştır. Çerçeveyi, olgunluğumuzu adım adım artırdığımız bir kılavuz olarak izliyoruz. Bu belgeyi kamuoyuyla paylaşma amacımız, aynı yolda ilerleyen kurumlara ve meslektaşlara yararlı bir referans sunmaktır.

02 · TEMEL YAKLAŞIMIMIZ VE DAYANDIĞIMIZ STANDARTLAR

Temel Yaklaşımımız ve Dayandığımız Standartlar

Çerçeve, tek bir kaynağa değil; uluslararası kabul görmüş çerçevelere dayanır. Böylece hem küresel iyi uygulamalarla hizalanmayı hem de düzenleyici gelişmelere hazır olmayı hedefliyoruz.

EU AI Act

Kabul edilemez, yüksek, sınırlı ve minimum risk katmanları çerçevemizin risk kategorileriyle birebir eşlenmiştir. Yüksek riskli sistemlerde Madde 9-15 gereksinimlerini referans alıyoruz.

OECD ve UNESCO

Sorumlu yapay zeka ilkelerimizin temel dayanağını oluşturur; insan denetimi, şeffaflık, adalet ve hesap verebilirlik bu çerçevelerle uyumludur.

KVKK · GDPR · SMK · FSEK

6698 sayılı KVKK ve GDPR kapsamında veri koruma; 6769 sayılı SMK ve 5846 sayılı FSEK kapsamında fikri mülkiyet yükümlülükleri sürecin ayrılmaz parçasıdır.

OWASP LLM Top 10 ve MCP güvenliği

Geliştiriciler ve veri bilimciler için güvenlik eğitim ve kontrollerimizin temelini oluşturur.

CRISP-DM, TDSP, OSEMN

Proje ve veri bilimi süreçlerimizi bu yerleşik metodolojiler üzerine kuruyoruz; proje yaşam döngümüz bu yaklaşımlarla uyumludur.

Türkiye Yapay Zekâ Eylem Planı (2026–2030)

18 Ağustos 2026 tarihli Cumhurbaşkanlığı Genelgesi ile yürürlüğe giren planın ekseni ve ilkeleri (etik sorumluluk, dijital egemenlik, sürdürülebilirlik, yaygınlaştırma) çerçevemizle hizalanır.

YAKLAŞIMIMIZIN ÖZÜ

Riski yaşam döngüsü boyunca yönetmek: Bir yapay zeka fikri ortaya çıktığı andan itibaren riski değerlendirilir, risk seviyesine orantılı kontroller uygulanır ve sistem canlıya alındıktan sonra da izlenmeye devam edilir.

03 · HER ÇALIŞAN İÇİN TEMEL KURALLAR

Her Çalışan İçin Temel Kurallar

İyi bir yönetişim çerçevesinin sahada karşılığı, her çalışanın günlük işinde akılda tutabileceği sade kurallardır.

Aşağıdaki temel kuralları, dokümanın tamamı okunmadan da hatırlanabilecek biçimde tasarladık.

KONU	TEMEL KURAL
Onaylı araç kullanımı	Yalnızca kurum tarafından onaylanmış yapay zeka araçları, kurumsal hesapla kullanılır. Kişisel hesaplarla şirket verisi işlenmez.
Gizli veri girişi	Gizli veya kısıtlı veri, genel kullanıma açık yapay zeka araçlarına aktarılmaz. Müşteri, finansal ve çalışan verisi ile ticari sır bu kapsamdadır.
Kişisel veri	Kimlik numarası, IBAN, telefon, e-posta, sağlık verisi gibi kişisel veriler, sisteme girilmeden önce maskelenir veya anonimleştirilir.
Karara güven	İşe alım, terfi, performans, finansal onay veya sağlıkla ilgili kararlar yapay zekaya bırakılmaz. Çıktı karar destek niteliğindedir; nihai kararı yetkili kişi verir.
Çıktı doğruluğu	Yapay zeka çıktısı yayımlanmadan veya karara esas alınmadan önce kaynağından doğrulanır. Yapay zeka halüsinasyon üretebilir.
Şeffaflık	Yapay zeka ile üretilen içerik (görsel, metin, kod) ayırt edilebilir biçimde etiketlenir.
Olay bildirimi	Veri sızıntısı şüphesi, hatalı veya ayrımcı çıktı ya da beklenmedik davranışta olay bildirim kanalından kayıt açılır.

04 · RİSK SINIFLANDIRMA MATRİSİ

Risk Sınıflandırma Matrisi

Çerçeve, tüm yapay zeka kullanım senaryolarını EU AI Act'in dört kademeli yaklaşımıyla birebir eşlenen dört kategoriye ayırır. Her proje, fikir aşamasında bir Risk Değerlendirme Formu ile bu kategorilere göre değerlendirilir; risk yükseldikçe uygulanan kontroller yoğunlaşır ve bulguların kapatılma süresi kısalır.

KATEGORİ	TANIM VE ÖRNEKLER	ZORUNLU KONTROLLER
A · Kabul Edilemez	AI Act Madde 5 kapsamında yasaklı uygulamalar: sosyal puanlama, bilinçaltı manipülasyon, işyerinde duygu tanıma, kişilik veya suç eğilimi profillemesi.	Tam yasak. Geliştirme, tedarik veya kullanım durumunda derhal durdurulur.
B · Yüksek Risk	İK kararları, kritik altyapı, erişim kararları (kredi, sigorta, sağlık, eğitim), biyometrik kategorilendirme.	THED ve VKED, tam teknik dokümantasyon, insan denetimi, log saklama, OWASP LLM Top 10 kontrolleri.
C · Sınırlı Risk	Kullanıcı ile doğrudan etkileşen sistemler, içerik üreten sistemler, karar destek sistemleri.	AI Act Madde 50 şeffaflık yükümlülüğü; kullanıcı bilgilendirilir, sentetik içerik etiketlenir.
D · Düşük Risk	Operasyonel destek, kod tamamlama, iç taslak üretimi, standart analitik uygulamalar.	Standart güvenlik ve veri sınıflandırma kuralları, envantere kayıt.

NEDEN ÖNEMLİ?

Risk kategorilerini uluslararası bir düzenlemeyle birebir eşlemek, hem iç tutarlılık sağlar hem de düzenleyici gelişmelere uyum yükünü azaltır. Bu eşleme, çerçeveyi hem denetlenebilir hem de gelecek düzenlemelere hazır kılar.

05 · SORUMLU VE ETİK YAPAY ZEKA İLKELERİ

Sorumlu ve Etik Yapay Zeka İlkeleri

Yapay zeka sistemlerinin adil, açıklanabilir ve insan gözetimi altında çalışmasını güvence altına almak için sekiz temel ilke tanımladık. Bu ilkeler, yaşam döngüsünün her aşamasında uygulanır ve OECD ile UNESCO çerçeveleriyle uyumludur.

01 İnsan denetimi ve kontrolü

İnsan hakları, istihdam, finansal onay ve sağlık kararlarında yapay zeka çıktısı yalnızca karar destek niteliğindedir; nihai kararı yetkili insan verir ve gerekçesini kaydeder.

02 Şeffaflık ve açıklanabilirlik

Kullanıcı, bir yapay zeka sistemiyle etkileşimde olduğunu bilir (AI Act Md. 50); sentetik içerik etiketlenir; yüksek riskli sistemlerde açıklama hakkı tanınır.

03 Adalet ve ayrımcılık karşıtlığı

Cinsiyet, yaş, din, dil, ırk, engellilik gibi nedenlerle ayrım yapılmaz; modeller alt grup performans farkları için düzenli test edilir.

04 Gizlilik ve veri koruma

Veri minimizasyonu, amaç sınırlaması ve en az ayrıcalık ilkeleri uygulanır; eğitim verisinde kişisel veri kullanılacaksa anonimleştirme zorunludur.

05 Hesap verebilirlik

Her yapay zeka sisteminin tanımlı bir iş sahibi, bir risk sahibi ve bir teknik sahibi bulunur.

06 Güvenlik ve sağlamlık

Sistemler adversarial ataklara, prompt injection'a, veri zehirlenmesine ve model çalmaya karşı test edilir; yüksek riskli sistemlerde kırmızı takım çalışması yapılır.

07 Sürdürülebilirlik

Büyük modellerin enerji tüketimi izlenir; aynı iş değerini üreten daha küçük ve verimli modeller tercih edilir; karbon etkisi yıllık raporlanır.

08 Toplumsal değer ve çocuk koruması

18 yaş altı bireylerin hedef olduğu sistemlerde yaşa uygun dil, duygusal manipülasyondan kaçınma, profilleme yasağı ve veli onayı uygulanır.

İYİ UYGULAMA ÖRNEĞİ

Özgeçmiş ön elemesinde bir yapay zeka skorlaması, yetkili insan değerlendirmesi olmadan hiçbir adayı eleyemez. Bu, insan denetimi ilkesinin uygulamadaki karşılığıdır.

06 · YAPAY ZEKA YÖNETİŞİM YAPISI

Yapay Zeka Yönetişim Yapısı

Yapay zeka projeleri, uygulamalar ve altyapı ihtiyaçları tanımlı roller ile yönetilir. Bu yapının merkezinde, Dijital Dönüşüm Komitesi altında konumlandırılmış Yapay Zeka Yönetişim Komitesi bulunur.

Yapay Zeka Yönetişim Komitesi

Yapay Zeka Yönetişim Komitesi, çerçevenin hâlihazırda hayata geçirdiğimiz merkezî unsurlarından biridir. Komite, kurum genelinde yapay zeka kullanımının stratejik yönünü belirleyen, riskleri gözeten ve farklı fonksiyonları ortak bir masada buluşturan karar organıdır. Çok disiplinli yapısı sayesinde teknoloji, hukuk, risk, veri koruma ve iş birimlerinin bakış açıları tek bir yönetişim noktasında birleşir.

Komitede asgari olarak şu fonksiyonlar temsil edilir:

- Teknoloji ve Dijital İş Geliştirme
- Yapay Zeka ve Teknoloji
- Risk, Uyum ve İç Denetim
- Bilgi Güvenliği
- Hukuk
- Veri Koruması
- İnsan Kaynakları
- Strateji ve Finans
- Sektörler

Komitenin başlıca rol ve sorumlulukları

Strateji ve yön belirleme

Kurumun yapay zeka stratejisini ve yol haritasını belirler, önceliklerini tanımlar ve gerektiğinde günceller.

Risk ve onay kararları

Kurumsal risk iştahını yansıtan yönetişim yaklaşımını belirler; yüksek riskli sistemlerin ve kritik projelerin devreye alınmasına ilişkin nihai kararı verir.

Onaylı araç yönetimi

Kurum genelinde kullanılabilecek onaylı yapay zeka araçları listesini onaylar; yeni araç ve lisans taleplerini değerlendirir.

İlke ve etik gözetimi

Sorumlu ve etik yapay zeka ilkelerinin uygulanmasını gözetir; ilkelerle çelişen kullanımları değerlendirir ve yönlendirir.

Olay yönetimi ve müdahale

Kritik yapay zeka olaylarında yönlendirme yapar; acil durumlarda durdurma (kill-switch) yetkisini kullanır.

İzleme ve raporlama

Yönetişim KPI'larını izler, üst yönetime düzenli durum raporu sunar ve çerçevenin sürekli iyileştirilmesini sağlar.

Rehberlik ve istisna yönetimi

Politikaların yorumlanmasında ortaya çıkan belirsizlikleri karara bağlar ve istisnaları değerlendirir.

06 · YAPAY ZEKA YÖNETİŞİM YAPISI

Karar mekanizması

Komite düzenli periyodik toplantılarla çalışır; kritik vaka veya olay durumunda olağanüstü toplanır. Kararlar çoğunluk esasına göre alınır; yüksek riskli sistemlerde risk ve denetim fonksiyonunun mutabakatı aranır, mutabakat sağlanamayan konular üst yönetim organlarına taşınır. Alınan tüm kararlar gerekçeleriyle birlikte tutanak altına alınır.

Roller ve Sorumluluk Matrisi (RACI)

Ana süreçler için sorumluluk atamaları RACI yöntemiyle yapılır. Bu netlik, sorumluluk boşluklarını ve çakışmalarını önlemeyi amaçlar.

BELİRLEYİCİ İLKE

Her sürecin bir ve yalnızca bir hesap veren tarafı olur.

PAYDAŞ	TEMEL SORUMLULUK
Yapay Zeka Yönetişim Komitesi	Stratejiyi ve yol haritasını belirler, kritik projeleri önceliklendirir, onaylı araç listesini onaylar.
BT Servis Operasyonları	Teknik altyapıyı yönetir, veri kaybı önleme sistemlerini uygular, güvenli araç listesi önerisi hazırlar.
İç Denetim, Kontrol ve Risk	Risk değerlendirmelerine katılır, denetim çalışmalarını yürütür, etik ihlal iddialarını inceler.
Hukuk	Sözleşmeleri fikri mülkiyet ve rekabet hukuku boyutuyla inceler, hukuki görüş verir.
Veri Koruma	Veri koruma regülasyonlarını takip eder, gizlilik ve sözleşme süreçlerini yürütür.
İnsan Kaynakları	Zorunlu yapay zeka eğitimlerini kurumsal eğitim programı içinde organize eder.
Sektör BT Temsilcileri	Proje taleplerini tanımlı süreçle iletir, entegrasyonu sağlar.

THED VE VKED NE ZAMAN ZORUNLUDUR?

Temel Hak Etki Değerlendirmesi (THED), yüksek riskli tüm sistemlerde; kişiler hakkında fırsat, erişim veya hak sonucu doğuran sistemlerde; 18 yaş altını hedefleyen ve biyometrik veri, duygu analizi veya profilleme içeren sistemlerde zorunludur. Veri Koruma Etki Değerlendirmesi (VKED) ise özel nitelikli veri işleyen, büyük ölçekli, sistematik izleme yapan veya kişisel veriyi yurt dışına aktaran sistemlerde gerekir. Bu değerlendirmeler tamamlanmadan geliştirme aşamasına geçilemez.

07 · YAPAY ZEKA PROJELERİ YAŞAM DÖNGÜSÜ

Yapay Zeka Projeleri Yaşam Döngüsü

Yapay zeka, ileri analitik ve makine öğrenmesi projeleri; standart, izlenebilir ve ölçülebilir bir yöntemle yürütülür. Projelerde CRISP-DM, TDSP ve OSEMN gibi yerleşik veri bilimi metodolojilerinden yararlanılır. Yaşam döngüsü yedi aşamadan oluşur ve her aşama tanımlı bir karar noktasıyla sonlanır.

1. **Fikir ve ön değerlendirme**
   Problem tanımı, hedef çıktı, beklenen fayda ve proje sınıfı belirlenir; risk değerlendirme formu doldurulur ve onaya sunulur.
2. **Proje başlatma ve kavramsal tasarım**
   Proje yöneticisi atanır; iş problemi analitik probleme dönüştürülür; kapsam, başarı kriterleri ve iş hedefleri tanımlanır.
3. **Veri toplama ve hazırlık**
   Veri kaynakları, erişim yetkileri ve veri kalitesi analiz edilir; harici veri ve açık kaynak bileşenlerin lisans şartları incelenir.
4. **Geliştirme ve modelleme**
   Çözüm mimarisi belirlenir, farklı modeller karşılaştırılır, performans değerlendirilir ve versiyonlar kayıt altına alınır.
5. **Test ve model değerlendirme**
   Model performansı test edilir, sonuçlar iş birimiyle doğrulanır, canlıya geçiş kriterleri değerlendirilir.
6. **Canlıya alma ve izleme**
   Çözüm canlıya alınır, entegrasyonlar tamamlanır; veri kayması ve model performans analizleri yapılır, iş hedefleri takip edilir.
7. **Proje kapanış**
   Nihai dokümantasyon tamamlanır, ders öğrenimleri kaydedilir, fayda ölçüm planı devreye alınır ve sonuçlar kurum içinde şeffaf biçimde duyurulur.

Fikri mülkiyet ve finansal yönetişim

Çalışanların onaylı araçlarla ürettiği kod, tasarım, metin ve buluşlara ilişkin haklar, başta FSEK ve SMK olmak üzere ilgili mevzuat çerçevesinde açık ve yazılı biçimde düzenlenir.

Finansal tarafta ise bulut, model eğitimi, lisans, API ve token tüketimi gibi giderlerin şeffaf ve izlenebilir olması esastır. Her proje için bir maliyet sahibi belirlenir; aynı iş değerini daha düşük maliyetle sağlayacak alternatifler düzenli değerlendirilir.

08 · VERİ GÜVENLİĞİ VE KONTROL YAKLAŞIMI

Veri Güvenliği ve Kontrol Yaklaşımı

Kurumsal veri; Genel, Şirket İçi, Gizli ve Kısıtlı olmak üzere dört sınıfa ayrılır. Her sınıf için hangi yapay zeka ortamında hangi kullanımın uygun olduğu net biçimde tanımlanır. Bu sınıflandırma, hangi verinin hangi ortamda işlenebileceğini uygulanabilir bir çerçeveye bağlar.

VERİ SINIFI	ONAYLI KURUMSAL YZ	GENEL / KAMUYA AÇIK YZ	ŞİRKET İÇİ ÖZEL LLM / RAG
Genel	İzinli	İzinli	İzinli
Şirket içi	İzinli	Kontrole tabi	İzinli
Gizli	Yalnız onaylı tenant	**Yasak**	Kontrole tabi
Kısıtlı	Özel onay ve izolasyon	**Yasak**	Yalnız izole ortam

Girdi ve çıktı güvenliği

Yapay zeka sistemlerine giden istekler; kişisel ve hassas veri taraması, içerik filtreleme ve prompt injection önleme olmak üzere katmanlı kontrollerden geçirilir. Çıktı tarafında halüsinasyon tespiti, kişisel veri ve gizli ticari bilgi sızıntısının engellenmesi ile içerik etiketleme uygulanır. Sohbet arayüzleri, içeriğin yapay zeka tarafından sağlandığını başından bildirir.

Veri kaybı önleme (DLP)

Yapay zeka araçları için veri kaybı önleme katmanlı biçimde uygulanır; kullanıcı cihazından yapılan yüklemeler, ağ trafiği ve içeriğin anlamına duyarlı kontroller birlikte çalışır. Kimlik numarası ve IBAN gibi yüksek hassasiyetli veri tiplerinde engelleme ile olay kaydı otomatik devreye girer. Semantik DLP, klasik anahtar kelime aramasının ötesine geçerek cümlenin bağlamını da değerlendirir.

Çalışan verisi konusunda özel hassasiyet

İşyerinde duygu tanıma ve biyometrik kategorilendirme, AI Act Madde 5 gereği yasaktır. Çalışan izleme amaçlı sistemler; insan kaynakları, hukuk ve çalışan temsilcisinin görüşü alınmadan devreye alınmaz. Terfi, performans, disiplin veya iş akdinin sona ermesi gibi kararlar yalnızca yapay zeka çıktısına dayandırılamaz.

09 · AJAN VE MCP YÖNETİMİ

Ajan ve MCP Yönetimi

Ajan tabanlı uygulamaların yaygınlaşması, bağlantı altyapısının yönetimini ayrı bir politika alanı haline getirdi.

Çerçeve bu alanı ayrı bir politika başlığı olarak erken aşamada ele alır.

MCP Gateway mimarisi

Tüm MCP trafiği merkezi bir geçit üzerinden yönlendirilir; doğrudan bağlantılara izin verilmez. Bu geçidin kurumsal kimlik altyapısı üzerinden kimlik doğrulama, ince taneli yetkilendirme, veri kaybı önleme entegrasyonu, kullanım sınırlama ve tam kapsamlı denetim kaydı sağlaması beklenir. Acil durumlarda trafiği anında durduran yetki yönetişim komitesine aittir.

Ajan kontrol matrisi

Ajanlar, açıkça tanımlanmış sınırlar içinde çalışır:

KONTROL	KURAL
Kapsam	Her ajan için kapsam, yetki ve kullanım amacı açıkça tanımlanır ve onaylanır.
Otonom eylemler	Veri üzerinde değişiklik yapan eylemler, tanımlı bir gözlem dönemi boyunca insan onayına tabidir. Bu sürenin ardından yalnızca düşük riskli eylemler otomasyona açılır.
Veri erişimi	Ajanlar yalnızca kayıtlı, sınıflandırılmış ve yetkilendirilmiş veri kaynaklarına, merkezi geçit üzerinden erişebilir.
Kullanım kotası	Periyodik token limitleri uygulanır; tanımlı eşikte uyarı, üst sınırda otomatik durdurma devreye girer.
Sandbox	Yeni veya güncellenen ajan konfigürasyonları, üretime alınmadan önce sandbox ortamında test edilir.

İYİ UYGULAMA ÖRNEĞİ

Otonom ajanlar için bir gözlem dönemi tanımlamak ve bu dönemde her kritik adımı insan onayına bağlamak; otomasyonun faydasından yararlanırken kontrolün korunmasını sağlar. Token kotası ve otomatik durdurma ise hem maliyet hem güvenlik açısından koruma sağlar.

10 · ÇALIŞAN FARKINDALIĞI VE GÖLGE YAPAY ZEKANIN ÖNLENMESİ

Çalışan Farkındalığı ve Gölge Yapay Zekanın Önlenmesi

Teknik kontroller ne kadar güçlü olursa olsun, yanlış bilgilendirilmiş bir çalışanın veriyi kişisel bir araca aktarması tüm yapıyı devre dışı bırakabilir.

Bu nedenle eğitim ve farkındalık, çerçevenin ayrılmaz ve sürekli bir parçasıdır.

Üç katmanlı eğitim yaklaşımı

01 Tüm çalışanlar

Yapay zeka farkındalığı, kabul edilebilir kullanım, gölge yapay zeka riski ve kişisel veri koruma temel bilgisi.

02 Onaylı araç kullanıcıları

Araca özgü kullanım, prompt güvenliği, veri sınıfı ve olay bildirimi. Kullanım öncesinde ve yıllık tekrarlanır.

03 Geliştiriciler ve veri bilimciler

OWASP LLM Top 10, MCP güvenliği, modelleme ve RAG konuları; yıllık ve güncellemelerle sürdürülür.

ÖNE ÇIKAN İLKE

Eğitimin etkisi, tamamlanma oranıyla değil, davranış değişikliğiyle ölçülmelidir.

Yapay Zeka Şampiyonları Ağı

Her departman ve iştirakten belirlenen çalışanlar Yapay Zeka Şampiyonu olarak atanır. Şampiyonlar; yerel düzeyde araç kullanım desteği, vaka tetkiki ve farkındalık etkinliklerinden sorumludur ve çeyreklik buluşmalarla bilgi paylaşımı sağlar. Bu ağ, merkezi yönetişim ile sahadaki uygulama arasında köprü işlevi görür.

Gölge yapay zekanın önlenmesi

Onaylı olmayan araçların çalışan inisiyatifiyle kullanılması gölge yapay zeka olarak tanımlanır ve kurumsal ölçekte ciddi risk oluşturur. Önleme stratejisi iki eksenlidir: Arz tarafında onaylı araç kataloğu zenginleştirilir ve iş ihtiyaçlarına hızlı yanıt verilir; talep tarafında ise eğitim ve net rehberlik sağlanır. Tespit edilen kullanımda öncelik cezalandırma değil, farkındalık ve meşru ihtiyacın karşılanmasıdır; ihtiyaç meşruysa ilgili araç komite incelemesine alınır.

11 · OLAY MÜDAHALE VE İŞ SÜREKLİLİĞİ

Olay Müdahale ve İş Sürekliliği

Yapay zeka olay müdahale planı

Model performansında ani bozulma, halüsinasyon, prompt injection, yetkisiz veri sızıntısı riski, ayrımcı çıktı artışı, gölge yapay zeka keşfi ve ajanın yetki kapsamı dışına çıkması birer yapay zeka olayı olarak değerlendirilir. Müdahale sekiz adımda yürütülür:

1 Tespit ve kayıt	**2** Sınıflandırma	**3** İzolasyon	**4** Kritik olaylarda durdurma
5 Kök neden analizi	**6** Düzeltici faaliyet	**7** Doğrulama	**8** Raporlama

Test ve onarım tamamlanmadan sistem yeniden açılmaz.

Bildirim süreleri

Kişisel veri ihlali, yüksek riskli sistem kritik olayı ve yüksek etkili prompt injection veya model çalma vakalarında tanımlı bildirim süreleri uygulanır. Bir olay birden fazla kategoriye girebileceğinden; ilgili kişi bildirimi, düzenleyici otorite bildirimi, sözleşmesel müşteri bildirimi ve iç bildirim yükümlülükleri ayrı ayrı değerlendirilir.

İş sürekliliği

Yapay zeka sistemleri, özellikle ajan tabanlı kullanımda, kesinti planlaması yapılmadan üretime alınmaz. Her kritik sistem için bağımlılık haritası tutulur; kurtarma süresi ve kabul edilebilir veri kaybı hedefleri tanımlanır. Tedarikçi bağımlılığını azaltmak için kritik servislerde alternatifler değerlendirilir ve alternatife geçiş düzenli tatbikatlarla test edilir.

ÖNE ÇIKAN İLKE

Tek sağlayıcıya kilitlenmiş bir mimari, teknik bir tercih değil, stratejik bir risktir. Veri taşınabilirliği sözleşme hükmüne bağlanır ve alternatife geçiş düzenli tatbikatlarla test edilir.

12 · DENETİM, HEDEFLER VE SÜREKLİ İYİLEŞTİRME

Denetim, Hedefler ve Sürekli İyileştirme

Yönetişimin etkinliği, tanımlı göstergelerle izlenir. Bu göstergeler, çerçevenin uygulamadaki ilerlemesini ölçülebilir kılar.

#	YÖNETİŞİM GÖSTERGESİ
01	Yapay zeka envanterine kayıt
02	Yüksek riskli sistemlerde THED tamamlanma oranı ve model kartı varlığı
03	Zorunlu eğitim tamamlama oranı
04	Sözleşmesel yapay zeka hükümleri tamamlanmış tedarikçi oranı
05	Olaylara hizmet seviyesi içinde müdahale oranı ve kritik olay bildirim uyumu
06	İç denetim bulgularının ortalama kapanış süresi ve bildirilen etik ihlal sayısı

Raporlama yapısı

Çeyreklik
Yapay zeka yetkilisi → Yapay Zeka Yönetişim Komitesi

›

Altı aylık
Yönetişim Komitesi → Dijital Dönüşüm Komitesi

›

Yıllık
Dijital Dönüşüm Komitesi → Yönetim Kurulu

Yapay zeka yetkilisi çeyreklik raporunu Yapay Zeka Yönetişim Komitesine sunar; komite altı aylık durum raporunu Dijital Dönüşüm Komitesine iletir; Dijital Dönüşüm Komitesi ise yıllık etkinlik ve uyum değerlendirmesini yönetim kuruluna sunar. Bu katmanlı raporlama, yönetişimi en üst yönetim seviyesine kadar görünür kılar.

Doküman yönetimi ve geçiş süreci

Doküman en az yılda bir kez gözden geçirilir; mevzuat değişikliği, kritik olay veya iş modeli değişikliği olağanüstü gözden geçirmeyi tetikler. Kullanımda olan yapay zeka sistemlerinin çerçeveye uyumlandırılması için tanımlı bir geçiş dönemi ve uyum tarama planı öngörülür. Bu, çerçeveyi statik bir doküman değil, yaşayan bir kılavuz haline getirir.

TERİMLER SÖZLÜĞÜ

Terimler Sözlüğü

Belgede geçen başlıca terim ve kısaltmaların kısa açıklamaları aşağıda yer alır.

TERİM	AÇIKLAMA
EU AI Act	Avrupa Birliği Yapay Zeka Yasası. Yapay zeka sistemlerini risk seviyesine göre düzenleyen AB regülasyonu.
KVKK / GDPR	Kişisel verilerin korunmasına ilişkin ulusal (6698 sayılı) ve Avrupa Birliği düzenlemeleri.
SMK / FSEK	Sınai Mülkiyet Kanunu (6769) ve Fikir ve Sanat Eserleri Kanunu (5846); fikri mülkiyet mevzuatı.
OECD / UNESCO İlkeleri	Sorumlu ve etik yapay zeka için uluslararası kabul görmüş ilke ve tavsiye çerçeveleri.
OWASP LLM Top 10	Büyük dil modeli uygulamalarında en kritik güvenlik risklerini tanımlayan güvenlik referansı.
LLM	Large Language Model (Büyük Dil Modeli). Metin üreten ve anlayan yapay zeka modeli türü.
MCP	Model Context Protocol. Yapay zeka modellerinin dış veri kaynakları ve araçlarla güvenli bağlantısını sağlayan protokol.
MCP Gateway	Tüm MCP trafiğinin kimlik doğrulama, yetkilendirme ve denetim için üzerinden geçtiği merkezî geçit.
Ajan (Agent)	Kendisine tanımlanan hedef doğrultusunda adımları planlayıp araçları kullanarak eylem gerçekleştirebilen yapay zeka sistemi.
RAG	Retrieval-Augmented Generation. Modelin yanıtını kurumsal veri kaynaklarından getirilen bilgiyle destekleyen yöntem.
THED	Temel Hak Etki Değerlendirmesi. Yüksek riskli sistemlerin temel haklar üzerindeki etkisini inceleyen değerlendirme.
VKED	Veri Koruma Etki Değerlendirmesi. Kişisel veri işlemenin gizlilik riskini analiz eden değerlendirme.
RACI	Sorumlu, Hesap Veren, Danışılan ve Bilgilendirilen rollerini netleştiren sorumluluk atama yöntemi.
DLP	Data Loss Prevention (Veri Kaybı Önleme). Hassas verinin yetkisiz biçimde dışarı çıkmasını engelleyen kontrol katmanı.
Halüsinasyon	Yapay zekanın gerçekte doğru olmayan bilgiyi güvenle üretmesi durumu.
Prompt injection	Kötü niyetli girdilerle modelin talimatlarını değiştirmeye yönelik saldırı türü.
Kill-switch	Kritik durumlarda bir yapay zeka sisteminin veya trafiğinin anında durdurulmasını sağlayan acil kontrol.
Sandbox	Yeni yapılandırmaların üretime alınmadan önce izole ortamda test edildiği güvenli alan.
Veri kayması	Zamanla verinin dağılımının veya model performansının başlangıç koşullarından sapması; canlıya alınan sistemlerde düzenli izlenir.
Model kartı	Bir modelin amacı, sınırları, performansı ve riskleri hakkında standart bilgi veren dokümantasyon.
CRISP-DM / TDSP / OSEMN	Veri bilimi ve analitik projelerinde kullanılan yerleşik proje ve süreç metodolojileri.
Gölge Yapay Zeka	Onaylı olmayan yapay zeka araçlarının çalışan inisiyatifiyle kurumsal onay dışında kullanılması.

KAPANIŞ

Bu belge, kurumsal yapay zeka yönetişimine ilişkin genel bir çerçeve sunar. Kurumların kendi risk profilleri ve tabi oldukları mevzuat doğrultusunda uyarlama yapması gerekir.

Zorlu Holding olarak bu çerçeveyi, yapay zeka alanındaki teknolojik, düzenleyici ve etik gelişmelere göre sürekli güncellenen ve olgunluğumuzla birlikte evrilen yaşayan bir kılavuz olarak ele alıyor, güncel tutmayı taahhüt ediyoruz. Alanında çalışan tüm kurum ve meslektaşlara ilham vermesini diliyoruz.

Zorlu Holding
Teknoloji ve Dijital İş Geliştirme Grup Başkanlığı
Yapay Zeka Yönetim Çerçevesi · 2026