ORTAK ALAN · ATÖLYE

AI agent pilot kontrol listesi

Bir AI agent'ı küçük ve güvenli bir pilotla denemek için. Ortak Atölye 'AI Agent Nedir? Örnekler ve Küçük Ekip İçin Pilot' rehberinin eşlik listesidir: ortakalan.io/atolye/ai-agent-nedir/. Araçların özellikleri ve veri koşulları sık değişir; kurulumdan önce kullandığınız hizmetin resmî dokümanını ve sözleşmesini okuyun. KVKK maddeleri genel bilgilendirmedir, hukuki danışmanlık değildir.

NASIL KULLANILIR

1. Yazdırın ya da PDF düzenleyicide açın; tamamladığınız maddenin kutusunu işaretleyin.
2. Size uymayan maddeleri atlayın; sırayı kendi takviminize göre değiştirebilirsiniz.

1. İşi seçmek

Tek iş, net başlangıç ölçümü.

- [ ] Pilot için tek bir iş seçtim ve bir cümleyle tanımladım.
- [ ] İş sık tekrarlanıyor; bugün ne kadar sürdüğünü ve ne sıklıkla yapıldığını not ettim.
- [ ] Girdi büyük ölçüde metin veya doküman; karar biraz yorum gerektiriyor.
- [ ] Hatanın bedeli düşük ve geri alınabilir.
- [ ] Adımlar her seferinde aynı mı diye baktım; aynıysa önce kural tabanlı otomasyonu denedim.
- [ ] Aynı işi sohbet ekranında elle birkaç kez yaptırdım ve model işin mantığını kavradı.
- [ ] Pilotun sahibi olan kişi belli.

2. Araçlar ve izinler

En az yetki: agent yalnızca bu iş için gerekeni yapabilmeli.

- [ ] Agent'ın erişeceği her aracı ve her araçta yapabileceği işlemi (okuma, yazma, gönderme, silme) listeledim.
- [ ] Agent kişisel hesabımla değil, yetkileri sınırlanmış ayrı bir hesap veya anahtarla çalışıyor.
- [ ] Silme, ödeme, iade ve dışarıya mesaj gönderme yetkisi kapalı ya da her seferinde insan onayına bağlı.
- [ ] Agent'ın okuduğu dış içerik (e-posta, web sayfası, belge) güvenilmeyen içerik olarak ele alınıyor.
- [ ] Aynı anda hem dış içerik okuyup hem dışarıya veri gönderebilen bir kurulum yok; varsa gönderim onaya bağlı.
- [ ] Anahtar ve parolalar talimat metninde veya paylaşılan dokümanlarda yazılı değil.

3. Talimatlar ve sınırlar

- ☐ Amaç, adımlar ve karar ölçütleri yeni bir çalışana anlatır gibi yazıldı.
- ☐ Agent'ın emin olmadığında ne yapacağı yazıldı (durup sormak, işi insana devretmek).
- ☐ Deneme sayısı sınırı belli; aşılırsa iş insana geçiyor.
- ☐ Geri alınamaz ve yüksek riskli işlemler listelendi; bunlarda insan onayı zorunlu.
- ☐ Mevcut şablon yanıtlar, sık sorulan sorular ve süreç dokümanları agent'a verildi.

4. Kişisel veri (KVKK)

- ☐ Agent'ın kişisel veri işleyip işlemediğini belirledim.
- ☐ Erişilen veri, işin gerektirdiği kadarla sınırlandı.
- ☐ Kullanılan AI hizmetinin verileri nerede işlediğini ve model eğitimi için kullanıp kullanmadığını sözleşmesinden kontrol ettim.
- ☐ Yurt dışına veri aktarımı söz konusuysa bunun dayanağını uzmanla netleştirdim.
- ☐ Aydınlatma metninin bu işlemeyi kapsayıp kapsamadığına baktım.
- ☐ Agent'ın hafızasında ve kayıtlarında tutulan verinin saklama süresi belli.

5. Gölge mod ve ölçüm

Önce öneri, sonra yetki.

- ☐ İlk dönemde agent yalnızca öneri üretiyor; gönderme ve kaydetme kararını insan veriyor.
- ☐ Her çalıştırmada girdi, atılan adımlar, çağrılan araçlar ve sonuç kaydediliyor.
- ☐ Belirli sayıda örnekten sonra doğru sonuç oranını hesapladım.
- ☐ İnsanın düzeltme süresini işi elle yapma süresiyle karşılaştırdım.
- ☐ Hata türlerini listeledim ve talimatları buna göre güncelledim.
- ☐ Haftalık örneklem kontrolü için bir kişi ve gün belirlendi.

6. Karar

- ☐ Pilot sonuçlarına göre devam, genişlet ya da durdur kararını yazılı verdim.
- ☐ Yetki genişletilecekse bir seferde tek yetki ekleniyor ve yeniden gölge modda deneniyor.
- ☐ Agent'ı kapatma yolu (anahtarı iptal etme, bağlantıyı kesme) belli ve denendi.
- ☐ Satıcının otomasyon oranı iddialarını kendi pilot ölçümümle karşılaştırdım.