AI DANIŞMAN

ÜCRETSİZ SÜRÜM

Kurumsal İşyerleri için Yapay Zekâ

KVKK ve yurt dışına aktarım, NIST ve ISO çerçeveleri, veri sınıflandırma, tek sayfalık politika, tedarik zinciri soruları, sektör yükümlülükleri ve 90 günlük uyum planı.

AI Danışman — Ücretsiz Eğitim Serisi

Eylül 2026 · aidanisman.pages.dev · t.me/aidanisman

İÇİNDEKİLER

01 Düzenleme yok, kural var

Türkiye'de yapay zekâya özgü, yürürlükte tek bir kanun bulunmuyor. TBMM'de farklı yaklaşımlarda teklifler var; Mart 2026'da yayımlanan TBMM Yapay Zekâ Araştırma Komisyonu raporu bir Türkiye Yapay Zekâ Kurumu kurulmasını ve Avrupa Konseyi Yapay Zekâ Çerçeve Sözleşmesi'nin onaylanmasını öneriyor. Ayrıca **Türkiye Yapay Zekâ Eylem Planı (2026–2030)** 18 Ağustos 2026 tarihli Resmî Gazete'de genelge olarak yayımlandı.

Kurumların buradan çıkardığı sonuç çoğu zaman yanlış oluyor:

> EN PAHALI KURUMSAL YANILGI
>
> **"Yapay zekâ kanunu yok" ile "kural yok" aynı şey değil.** Yapay zekâ kullanımı bugün zaten yürürlükteki mevzuata tabi: **KVKK**, iş hukuku, fikri mülkiyet, sektörel düzenlemeler ve imzalanmış gizlilik sözleşmeleri. Yeni bir kanunu beklemek, mevcut yükümlülüğü ertelemiyor.

Düzenleyicinin kendisi de sessiz değil. Kişisel Verileri Koruma Kurumu, **24 Kasım 2025** tarihinde **"Üretken Yapay Zekâ ve Kişisel Verilerin Korunması Rehberi (15 Soruda)"** başlıklı rehberini yayımladı. Rehber, üretken yapay zekâ sistemlerinin yaşam döngüsünü, kullanım alanlarını ve risklerini 6698 sayılı Kanun çerçevesinde ele alıyor ve veri sorumlularını *insan merkezli, şeffaf ve kontrol edilebilir* bir yaklaşıma yönlendiriyor.

Çoğu kurum bu belgenin varlığından haberdar değil. Uyum çalışmasının ilk adımı onu okumak.

02 Asıl mesele: yurt dışına aktarım

Bu bölüm, yabancı kaynaklı hiçbir yapay zekâ eğitiminde bulunmayan ama Türkiye'de faaliyet gösteren her kurumu doğrudan ilgilendiren konu.

Rejim 2024'te değişti

7499 sayılı Kanun (12 Mart 2024) KVKK'nın 9. maddesini baştan yazdı; yeni yurt dışına aktarım rejimi **1 Haziran 2024**'te yürürlüğe girdi. Yapı üç kademeli:

Kademe	Araç	Bugünkü durum
1	Yeterlilik kararı — Kurul'un bir ülke, sektör veya uluslararası kuruluş için verdiği karar	**Hiçbir ülke için verilmiş değil**
2	Uygun güvenceler — standart sözleşme, bağlayıcı şirket kuralları, taahhütname, kamu kurumları arası anlaşma	Fiilen kullanılan yol
3	Arızi durumlar (m. 9/6) — tek seferlik, istisnai hâller	Süreklilik arz eden aktarımda kullanılamaz

Bunun yapay zekâ ile ilgisi

Kurumların kullandığı üretken yapay zekâ araçlarının neredeyse tamamı yurt dışı merkezli. Ve **hiçbir ülke için yeterlilik kararı verilmiş değil.** Dolayısıyla:

Çıkarım: Kişisel veri içeren bir metin, yurt dışı merkezli bir yapay zekâ aracına girdiği anda *yeterlilik kararı bulunmayan bir ülkeye aktarım* gerçekleşiyor. Bu, doğrudan ikinci kademeyi — **uygun güvence**

yükümlülüğünü — devreye sokuyor.

Çoğu kurumda bu adım hiç atılmamış durumda. Ekip kullanıyor, kurum bilmiyor, sözleşme yok.

Standart sözleşme yolunun pratiği

- Kurul'un **04.06.2024 tarihli 2024/959 sayılı kararı** ile standart sözleşme metinleri, bağlayıcı şirket kuralları başvuru formları ve yardımcı kılavuzlar kabul edildi.
- Standart sözleşme, **imzalandıktan sonra 5 iş günü içinde Kurul'a bildirilmek zorunda.**
- Bildirim yükümlülüğünün ihlali idari para cezasına bağlanmış durumda. Tutarlar her yıl yeniden değerleme oranıyla güncelleniyor — güncel aralık için **kvkk.gov.tr**.
- KVKK'nın konuya özel rehberi: **Kişisel Verilerin Yurt Dışına Aktarılması Rehberi** (KVKK Yayınları No: 48).

> PRATİKTE EN HIZLI ÇÖZÜM
>
> Aktarımı hukuki bir sürece bağlamak zaman alıyor. Bu arada riski sıfıra yaklaştıran operasyonel karar şu: **kişisel veriyi bu araçlara hiç göndermemek.** Veri sınıflandırması ve anonimleştirme, uyum çalışması tamamlanana kadar kurumu ayakta tutan şey. Bölüm 3'ün amacı bu.

03 Uluslararası çerçeveler: kurumsal alıcının duyduğu üç ad

Türkiye'de KVKK'yı konuşuyoruz. Ama kurumsal bir alıcı, bir denetçi ya da AB'li bir müşteri üç ad daha telaffuz ediyor. Bunları bilmek, hazırlıklı olmakla hazırlıksız yakalanmak arasındaki fark.

1. NIST Yapay Zekâ Risk Yönetimi Çerçevesi

ABD kaynaklı, gönüllü, ama fiilen küresel referans. Kurumsal eğitim ve danışmanlık programlarının çoğu bunun üzerine kurulu. Dört çekirdek fonksiyonu var:

Fonksiyon	Ne demek	Kurumdaki karşılığı
GOVERN — Yönet	Sorumluluk, politika, kültür	Sahip belirleme, tek sayfalık politika, eğitim
MAP — Haritala	Bağlam ve riskleri tanımlama	Kullanım envanteri, veri sınıflandırma
MEASURE — Ölç	Riski analiz etme ve izleme	Denetim kayıtları, olay sayıları, kalite ölçümü
MANAGE — Yönet/Müdahale	Riske önceliklendirerek müdahale	Olay müdahale akışı, düzeltici önlemler

Dikkat: bu rehberdeki 90 günlük planın adımları bu dört fonksiyona zaten karşılık geliyor. Yani ayrı bir iş yapmıyorsun — **yaptığın işi bu dille anlatabiliyorsun.**

2. ISO/IEC 42001 — Yapay Zekâ Yönetim Sistemi

Denetlenebilir bir standart. Kurumsal alıcı ve tedarik süreçlerinde giderek daha sık soruluyor. Bizim açımızdan iki maddesi doğrudan önemli:

Madde	Ne istiyor	Pratik karşılığı
7.2 — Yetkinlik	Yapay zekâ yönetim sistemini etkileyen işi yapan herkesin ilgili yetkinliği *gösterebilmesi*	Eğitim kaydı tutmak — katılım listesi, tarih, içerik
7.3 — Farkındalık	Kişinin kendi rolünün politikaya ve hedeflere nasıl katkı verdiğini anlaması	Politikanın tebliğ edilmesi ve rol bazlı anlatılması

Çıkarım: Bu iki madde, "eğitim kaydı neden tutulur" sorusunun cevabı. Rehberdeki eğitim bölümü iyi niyetli bir öneri değil — denetlenebilir bir standart bağlamında **belgelenmesi gereken bir yükümlülük.** Katılım listesi tutmayan kurum, eğitimi vermiş olsa bile gösteremiyor.

3. AB Yapay Zekâ Tüzüğü — okuryazarlık maddesi

Tüzüğün 4. maddesi, yapay zekâ sistemi **kullanan** kuruluşlara personelinin okuryazarlığını geliştirmeyi destekleme yükümlülüğü getiriyor. Kapsam geniş: çalışanlar, dış işbirlikçiler ve **alt yükleniciler.** Eğitimin role ve riske orantılı olması bekleniyor.

> **TÜRKİYE'DEKİ KURUMA ETKİSİ — DİKKATLİ OKUMA GEREKİYOR**
>
> Bu bir AB düzenlemesi ve kurumunuza uygulanıp uygulanmadığı **hukuki bir değerlendirme.** Bu rehber onu yapamaz. Ama pratik gerçek şu: AB'ye satan, AB'de müşterisi veya iştiraki olan ya da AB'li bir şirkete alt yüklenici olan kurumlarda bu soru *zaten* sorulmaya başlandı — çoğu zaman doğrudan mevzuattan değil, **müşteri sözleşmesi yoluyla.**
>
> *Not: Temmuz 2026'daki bir değişiklikle ifade "okuryazarlığın gelişimini desteklemek" biçimine getirildi ve belirli bir bireysel seviyenin garanti edilmesi gerekmediği belirtildi. Yükümlülük duruyor, ölçütü yumuşadı.*

Üçünün ortak dediği şey

Farklı kaynaklardan gelen bu üç çerçeve aynı dört şeyi istiyor:

1. **Sahip belli olsun** — kim sorumlu
2. **Risk haritalansın** — nerede ne kullanılıyor, hangi veriyle

3. **Ölçüm ve kayıt olsun** — denetim izi, eğitim kaydı
4. **Müdahale yolu tanımlı olsun** — olay olduğunda ne yapılacak

Bu dördü, KVKK uyumunun da omurgası. Yani ayrı ayrı dört program kurmuyorsun — **tek bir program kuruyorsun ve dört dilde anlatabiliyorsun.**

04 Veri sınıflandırma

Kurum düzeyinde tek en yüksek getirili çalışma bu. Politika yazmadan önce yapılır, çünkü politikanın içeriğini bu belirliyor.

Seviye	İçerik	Yapay zekâ aracına
K1 — Açık	Yayımlanmış içerik, web sitesi metni, basın bülteni, açık mevzuat	Serbest
K2 — İç	Süreç tarifi, iç eğitim, şablon, toplantı notu (kişi/müşteri adı çıkarılmış)	Kurumsal hesapta serbest
K3 — Gizli	Sözleşme, fiyatlandırma, strateji, açıklanmamış ürün, finansal detay	Yalnız anonimleştirilerek; kurumsal hesap zorunlu
K4 — Özel	Kişisel veri, özel nitelikli kişisel veri, özlük, sağlık, müşteri kimliği, erişim bilgisi	**Yasak**

Sınıflandırmayı işe yarar kılan üç kural

1. **Dört seviyeden fazlası kullanılmıyor.** Yedi seviyeli şemalar kâğıtta güzel duruyor, sahada kimse hatırlamıyor.
2. **Her seviyenin bir örneği yazılı olmalı.** Tanım değil, örnek. Çalışan tanımı okuyup karar veremiyor; örneği görünce veriyor.
3. **Karar verilemeyen içerik K4 sayılır.** Tereddüt, bir üst seviyeye yuvarlanır. Bu tek cümle, sınıflandırmayı güvenli hâle getiriyor.

05 Politika: tek sayfa yeter

Kurumların yaptığı ikinci hata: yirmi sayfalık bir yapay zekâ politikası yazmak. Kimse okumuyor, kimse uygulamıyor, ve yazılmış olması riski azaltmıyor.

Çalışan davranışını değiştiren politika tek sayfa ve altı başlık:

#	Başlık	Cevaplanması gereken
1	**Kapsam**	Hangi araçlar, hangi hesaplar, kimler
2	**Veri kuralı**	Sınıflandırmaya atıf — hangi seviye nereye girer
3	**Yasak kullanımlar**	Kısa ve mutlak liste
4	**Denetim**	Dışarı giden çıktıyı kim, neye göre kontrol eder
5	**Sorumluluk**	Çıktının sorumlusu gönderen kişidir
6	**Bildirim**	Hata veya veri sızıntısı olursa kime, ne kadar sürede

Yasak listesinin kısa olması şart

Uzun yasak listesi, çalışanın listeyi hiç okumaması demek. Dört madde yetiyor: kişisel veri girilmez · müşteri kimliği girilmez · erişim bilgisi girilmez · çıktı denetlenmeden dışarı gitmez.

> TAMAMEN YASAKLAMANIN SONUCU
>
> Kullanımı tümden yasaklayan kurumlarda kullanım bitmiyor — **kişisel hesaplara ve kişisel cihazlara kayıyor.** O noktada kurumun ne denetim izi kalıyor, ne sözleşmesi, ne de neyin girdiğine dair bilgisi. Yasak, riski ortadan kaldırmıyor; görünmez ve yönetilemez hâle getiriyor.

06 Bilginin kaynağı: kurum içi mi, internet mi

Kurumsal yapay zekâ araçlarında çoğu kullanıcının bilmediği bir ayrım var: cevabın **kurumun kendi belgelerinden** mi yoksa internetten mi üretildiği. Bu ayrım hem doğruluk hem gizlilik açısından belirleyici.

	Kurum içi kaynaklı	İnternet kaynaklı
Cevap nereden	Kurumun belgeleri, e-postaları, dosyaları	Genel web içeriği
Doğruluk riski	Belge eskiyse cevap da eski	Kaynak güvenilmez olabilir
Gizlilik riski	**Yetkilendirme hatası:** kullanıcı görmemesi gereken belgeyi görebilir	Kurum verisi dışarı gidebilir
Denetim	Kaynak belgeyi aç ve kontrol et	Kaynağı ve güncelliği doğrula

> **KURUM İÇİ KAYNAKLI ARAÇLARIN GİZLİ RİSKİ**
>
> Araç, kullanıcının erişim yetkisi olan belgeleri okuyor. Sorun şu: kurumlarda yetkilendirme çoğu zaman olması gerekenden geniş. İnsan gözü fark etmiyor çünkü o klasörü hiç açmıyor — ama **araç açıyor ve içeriğini cevaba katıyor.**
>
> Yani bu araçlar bir yetkilendirme sorunu yaratmıyor; *var olan sorunu görünür kılıyor.* Bu yüzden kurum içi kaynaklı bir araç açılmadan önce erişim yetkilerinin gözden geçirilmesi gerekiyor — kurulum sonrası değil, öncesi.

Duyarlılık etiketleri

Kurumsal platformların bir kısmı belgelere **duyarlılık etiketi** atanmasına ve araçların bu etiketlere göre davranmasına izin veriyor. Bu, bizim K1–K4 veri sınıflandırmamızın teknik uygulaması.

Sınıf	Etiket karşılığı	Araç davranışı
K1 — Açık	Genel	Serbestçe kullanılır
K2 — İç	Kurum içi	Kurumsal araçta kullanılır, dışarı çıkmaz
K3 — Gizli	Gizli	Erişim kısıtlı; çıktı da aynı etiketi taşır
K4 — Özel	Yüksek gizli / kişisel veri	Araca hiç verilmez

Çıkarım: Sınıflandırma yalnız kâğıt üstünde kaldığında uygulanmıyor. Teknik olarak *etiketlenebiliyorsa* uygulanıyor. Bu yüzden sınıflandırma çalışmasının ikinci yarısı, etiketlerin sistemde karşılığının kurulması — ve bu genelde bilgi işlem ile birlikte yapılan bir iş.

07 Sağlayıcı ve hesap tipi

Aynı ürünün kişisel ve kurumsal sürümü hukuken aynı şey değil. Kurumun cevaplaması gereken sorular:

Soru	Neden önemli
Girdiler model eğitimine kullanılıyor mu	Kurumsal planlarda genelde kullanılmıyor; ücretsiz sürümlerde koşullar farklı
Veri nerede işleniyor, nerede saklanıyor	Aktarım analizinin girdisi
Saklama süresi ve silme	Veri minimizasyonu ve saklama politikasıyla uyum
Sözleşme kiminle imzalanıyor	Kurumsal planda kurumla; kişisel hesapta çalışanla — kurumun hiçbir hakkı olmuyor
Yönetici paneli ve erişim kaydı var mı	Denetim izi ve işten ayrılan personelin erişiminin kesilmesi
Alt işleyenler kimler	Aktarım zinciri sözleşmede görünmeli

Çıkarım: Ücretsiz kişisel hesapla kurumsal iş yapmak, maliyeti aboneliğe göre düşük ama *riski* ölçülemez biçimde yüksek bir tercih. Kurumsal hesabın asıl aldığı şey özellik değil, **sözleşme ve denetim izi.**

08 Denetim izi ve sahiplik

Bir sorun çıktığında kurumun cevaplaması gereken üç soru var ve üçü de önceden kurulmadıysa cevaplanamıyor:

1. **Kim kullandı?** — Kurumsal hesap ve kullanıcı bazlı erişim.
2. **Ne girdi?** — Politika + sınıflandırma + eğitim kaydı. Tam girdi kaydı çoğu araçta yok; kurumun dayanağı *kuralı yazmış ve duyurmuş olmak.*
3. **Kim onayladı?** — Dışarı giden çıktının sahibi belli olmalı.

Sahiplik: tek isim

Yapay zekâ uyumu bir kişiye bağlanmadığında hiç kimseye bağlanmış olmuyor. Kurumun büyüklüğü ne olursa olsun tek bir **sahip** gerekiyor — genellikle bilgi güvenliği, uyum veya hukuk tarafından biri. Sahip üç şeyden sorumlu: politikanın güncelliği, araç envanteri ve olay bildirimi.

09 Tedarik zinciri: müşteriniz de size soruyor

Kurumsal yapay zekâ uyumunun en hızlı büyüyen tetikleyicisi mevzuat değil — **müşteri sözleşmeleri.** Büyük alıcılar tedarikçilerine yapay zekâ soruları sormaya başladı ve bu sorular sözleşmelere giriyor.

Tedarikçi değerlendirme formlarında çıkan sorular

Soru	Cevabınız yoksa
Bize verdiğiniz hizmette yapay zekâ kullanıyor musunuz, nerede	Envanteriniz yok demektir
Bizim verimiz bu sistemlere giriyor mu	Veri sınıflandırmanız yok demektir
Girdiler model eğitimine kullanılıyor mu	Sağlayıcı şartlarını okumamışsınız
Veri hangi ülkede işleniyor	Aktarım analiziniz yok
Yazılı bir politikanız var mı	En temel eksiklik
Personeliniz eğitimli mi, kaydı var mı	Eğitim kaydı tutulmuyor
Bir olay olursa bize ne kadar sürede haber verirsiniz	Olay müdahale akışınız yok

Çıkarım: Bu yedi soru, bu rehberdeki 90 günlük planın çıktılarıyla birebir örtüşüyor. Yani uyum çalışması bir maliyet kalemi değil — **bir satış önkoşulu** hâline geliyor. Cevabı hazır olan tedarikçi, cevabı hazır olmayanın önüne geçiyor.

Ters yön: siz de sormalısınız

Aynı sorular sizin tedarikçilerinize de sorulmalı — özellikle sizin adınıza veri işleyenlere. Bir yazılım sağlayıcınız arka planda yapay zekâ kullanıyorsa ve sizin verinizi ona veriyorsa, o zincir **sizin sorumluluğunuzda.**

Tedarikçi tipi	Sorulacak
Yazılım / SaaS sağlayıcısı	Ürününüzde yapay zekâ özelliği var mı, verimiz oraya giriyor mu
Ajans / danışman	Bizim materyallerimizi bu araçlara giriyor musunuz
Çağrı merkezi / dış hizmet	Müşteri kayıtları hangi sistemlerde işleniyor
Muhasebe / hukuk	Belgelerimiz üçüncü taraf araçlara yükleniyor mu

> **SESSİZ ZİNCİR**
>
> En sık gözden kaçan risk burada: kurum kendi kullanımını sıkı biçimde düzenliyor ama **tedarikçilerinin ne yaptığını bilmiyor.** Ajansınıza gönderdiğiniz brief, muhasebecinize verdiğiniz belge, danışmanınıza anlattığınız strateji — hepsi sizin kontrolünüz dışındaki bir araca girmiş olabilir. Sözleşmelere bir madde eklemek, bu zinciri görünür kılmanın en hızlı yolu.

10 Yaygınlaştırma

Politika yazıldıktan sonra en sık yapılan hata onu e-posta ile duyurup bitmiş saymak. Davranışı değiştiren üç mekanizma var:

Mekanizma	Nasıl
Örnek üzerinden eğitim	Kavram anlatma; kurumun kendi işlerinden 5 gerçek örnek göster — biri de "bu yapılmaz" örneği olsun
Birim temsilcisi	Her birimde bir kişi soruların ilk adresi olsun; merkezî ekip yetişemez
Görünür izin	Yöneticiler kendi kullanımlarını açıkça anlatsın — gölge kullanımı bitiren tek şey bu

> OTOMATİK KARAR SINIRI
>
> KVKK'nın 11. maddesi, ilgili kişiye *münhasıran otomatik sistemlerle analiz sonucu kendisi aleyhine bir sonuç doğmasına itiraz* hakkı veriyor. Kuruma pratik sonucu net: özgeçmiş eleme, risk skorlama, performans değerlendirme gibi işlerde model **hazırlık yapabilir, karar veremez.** Kararın insan tarafından verildiği gösterilebilir olmalı.

11 Kurumsal hesaba geçiş — pratik kararlar

Uyum çalışmasının en somut ve en hızlı getirili adımı bu. Ama "kurumsal hesap alalım" kararı, uygulamada birkaç alt karar içeriyor.

Kimlere verilir

Yaklaşım	Sonucu	Öneri
Herkese	Yüksek maliyet, düşük kullanım	Kaçın — en sık yatırım hatası
Sadece yöneticilere	Asıl kullanan kişiler dışarıda kalır	Kaçın
Bir birime pilot	Ölçülebilir, kontrollü	**Başlangıç için doğru**
Süreç kuranlara	Kullanım yüksek, yayılım organik	**Genişleme için doğru**

Geçişte yapılacak beş iş

1. **Kişisel hesap kullanımını durdur.** Kurumsal hesap açıldıktan sonra kişisel hesapla kurum işi yapılmayacağı açıkça duyurulur.

2. **Yönetici panelini kur.** Kim kullanıyor, ne zaman — bu kayıt denetim izinin temeli.
3. **Ayrılma sürecine ekle.** Personel ayrıldığında erişimin kesilmesi, çıkış kontrol listesine girmeli.
4. **Veri işleme ekini al ve sakla.** Tedarikçi değerlendirme formunda ilk istenen belge bu.
5. **Sağlayıcı şartlarını okuyup özetle.** Girdiler eğitime kullanılıyor mu, saklama süresi ne, veri nerede — bu üç cevap yazılı olsun.

> ÜÇÜNCÜ MADDE EN ÇOK ATLANAN
>
> Ayrılan personelin erişiminin kesilmesi, klasik bilgi güvenliği pratiği — ama yeni açılan yapay zekâ hesapları genelde çıkış kontrol listesine **eklenmiyor.** Sonuç: kurumun belgelerine erişebilen ve artık kurumda çalışmayan hesaplar. Bu, denetimde ilk sorulan şeylerden biri.

Maliyet konuşması

Kurumsal hesabın maliyeti genelde kişisel sürümlerin birkaç katı ve bu, yönetime zor gelen bir kalem. Doğru çerçeve şu: **ödenen şey özellik değil, sözleşme.**

Ücretsiz/kişisel hesapla gelen risk	Bedeli
Kurumun sözleşmesi yok	Veri kullanımına dair hiçbir taahhüt yok
Denetim izi yok	Bir olayda "kim, ne girdi" sorusu cevapsız
Ayrılan personel erişimi	Kesilemiyor
Tedarikçi sorularına cevap	Verilemiyor — satış riski

Bu tabloyu yönetime göstermek, lisans maliyetini bir *gider* olmaktan çıkarıp bir *risk azaltma* kalemine dönüştürüyor. Ve dördüncü satır, mali gerekçeyi de veriyor.

12 Doksan günlük uyum planı

Dönem	İş	Çıktı
1–15. gün	Envanter: hangi birim hangi aracı, hangi hesapla kullanıyor. Yargılamadan sor.	Araç ve kullanım envanteri
16–30. gün	Veri sınıflandırma (4 seviye, her seviyeye örnek)	Tek sayfalık sınıflandırma
31–45. gün	Tek sayfalık politika + kısa yasak listesi	Yayımlanmış politika
46–60. gün	Hesap tipi kararı; kurumsal hesaba geçiş; sağlayıcı sorularının cevaplanması	Sözleşmeli kurumsal erişim
61–75. gün	Aktarım analizi: kişisel veri gidiyor mu, gidiyorsa hangi güvenceyle	Aktarım kararı ve gerekiyorsa standart sözleşme süreci
76–90. gün	Örnek üzerinden eğitim, birim temsilcileri, olay bildirim yolu	Çalışan farkındalığı ve sahiplik

Doksanıncı günün sonunda kurumun elinde envanter, sınıflandırma, politika, sözleşmeli erişim, aktarım kararı ve eğitim kaydı olur. Bu altı belge, hem denetimde hem de bir olay yaşandığında kurumun elindeki tek gerçek savunma.

13 Sektöre göre ek yükümlülükler

Genel çerçeve her kurum için aynı; ama bazı sektörlerde üstüne binen ek katmanlar var. Bu tablo, hangi soruların ayrıca sorulması gerektiğini gösteriyor.

Sektör	Ek dikkat	Pratik sonuç
Sağlık	Sağlık verisi özel nitelikli kişisel veri	Hasta verisi hiçbir koşulda araca girmez; anonimleştirme bile dikkatli değerlendirilir
Finans / sigorta	Sektörel düzenleme + otomatik karar sınırı	Kredi, risk ve fiyat kararlarında insan kararı zorunlu; düzenleyici bildirim gerekebilir
Hukuk	Meslek sırrı ve müvekkil gizliliği	Dosya içeriği araca girmez; uydurulan mevzuat riski en yüksek burada
Eğitim	Öğrenci verisi, çocuk verisi	Reşit olmayanlara ait veri için ek hassasiyet; veli bilgilendirmesi
Kamu / kamuya iş yapan	İhale şartnameleri ve gizlilik taahhütleri	Şartnamede yapay zekâ maddesi olabilir; sözleşme öncesi kontrol
Savunma / kritik altyapı	Güvenlik sınıflandırması	Sınıflandırılmış bilgi hiçbir dış sisteme girmez
İlaç / medikal cihaz	Ruhsatlandırma ve kayıt yükümlülükleri	Belgelendirme süreçlerinde kullanılan araçların kaydı

> **ORTAK NOKTA: ÖZEL NİTELİKLİ VERİ**
>
> Sağlık, biyometrik, genetik, din, siyasi görüş, sendika üyeliği ve ceza mahkûmiyeti gibi veriler **özel nitelikli kişisel veri** kategorisinde ve işlenmeleri daha ağır koşullara bağlı. Bu verilerin bulunduğu hiçbir metin, tablo veya ekran görüntüsü yapay zekâ araçlarına verilmez — bu, kurumun politika metnindeki en net satır olmalı.

Sektör ne olursa olsun sorulacak tek soru

"Bu bilgi yanlış ellere geçse ya da yanlış kullanılsa, kim zarar görür ve ne kadar?"

Cevap "bir insan, ciddi biçimde" ise o bilgi araca girmiyor — mevzuat ne derse desin. Uyum çalışması bu soruyu kurumsallaştırma çabasından ibaret.

14 Doksanıncı günün sonunda

Belge	Hangi çerçevenin karşılığı
Kullanım envanteri	NIST MAP · tedarikçi sorusu 1
Veri sınıflandırması	NIST MAP · KVKK · tedarikçi sorusu 2
Tek sayfalık politika	NIST GOVERN · ISO 42001 m.7.3 · tedarikçi sorusu 5
Sözleşmeli kurumsal erişim	KVKK · tedarikçi sorusu 3
Aktarım kararı	KVKK m.9 · tedarikçi sorusu 4
Eğitim kaydı	ISO 42001 m.7.2 · AB m.4 · tedarikçi sorusu 6
Olay müdahale akışı	NIST MANAGE · tedarikçi sorusu 7
Denetim kontrol listesi	NIST MEASURE

Son çıkarım: Sağ sütun, bu çalışmanın neden bir maliyet kalemi olmadığını gösteriyor. Sekiz belge üretiyorsun ve bu sekiz belge dört ayrı çerçeveye, bir mevzuata ve müşteri sorularının tamamına aynı anda cevap veriyor. **Ayrı ayrı dört program kurmuyorsun; tek bir program kurup dört dilde anlatıyorsun.**

Bundan sonra: sürdürme

Doksan gün bir kurulum süresi, bir bitiş değil. Üç şey düzenli hâle gelmezse belgeler bir yıl içinde gerçeği yansıtmayı bırakıyor:

- **Altı ayda bir denetim listesi** — politika işliyor mu, yazıldı mı değil
- **Yılda bir sağlayıcı değerlendirmesi** — şartlar sık değişiyor
- **Her yeni araçta envanter güncellemesi** — envanter en hızlı eskiyen belge

Ve en önemlisi: **sahip**. Bu üç işi takvime koyacak tek bir isim yoksa, doksan günün sonunda üretilen sekiz belge ikinci yılda birer arşiv kaydına dönüşüyor.

Buradan sonrası

Doldurulabilir politika ve sınıflandırma şablonları, aktarım karar ağacı, sağlayıcı değerlendirme formu, olay müdahale akışı, eğitim programı ve denetim kontrol listesi 'nda.

t.me/aidanisman · aidanisman.pages.dev

Bu belgedeki bilgiler eğitim amaçlıdır; hukuki tavsiye niteliği taşımaz ve avukat görüşü yerine geçmez. Mevzuat, Kurul kararları ve idari para cezası tutarları değişmektedir; uygulamaya geçmeden önce güncel metinler için **kvkk.gov.tr** adresine ve kurumunuzun hukuk danışmanına başvurun. Belgedeki mevzuat bilgileri Eylül 2026 itibarıyla derlenmiştir.