

Güvenlik, Gizlilik ve Veri Koruma

Google Workspace Son Kullanıcı Eğitim Programı

Süre	Seviye	Ön koşul	Modül çıktısı
2 saat	Temel	Modül 1 ve 3	Kişisel güvenlik kontrol listesi ve gözden geçirilmiş paylaşım izinleri

Hazırlayan: Mikail Lekesiz · Sürüm 1.0 · Ekim 2026

Bu belgede

Modüle genel bakış.....	2
1. Tehditleri tanıma: kimlik avı, sahte oturum açma, uygulama izni ve QR saldırıları.....	2
2. Gmail uyarıları, kimlik avını bildirme ve Tümünü yanıtla gizlilik kontrolü.....	4
3. Hesap güvenliği: 2 Adımlı Doğrulama, geçiş anahtarı, üçüncü taraf erişimi ve cihaz oturumları.....	5
4. Paylaşım hijyeni: en az yetki, son kullanma tarihi, dış paylaşım, DLP ve etiketler.....	6
5. KVKK ve kurum politikaları: kişisel veri, aydınlatma, kayıt ve transkript.....	7
6. Yapay zekâ ve veri: Workspace taahhütleri, hesap ayrımı ve gizli bilgi kuralları.....	8
7. Mobil cihaz güvenliği ve cihaz kaybında yapılacaklar.....	9
Uygulama çalışması: Kişisel güvenlik denetimi.....	10
Bilgi kontrolü.....	12
Sık sorulan sorular.....	13
Akılda kalsın.....	13
Ek: Eğitim materyalleri.....	13
Kaynaklar.....	16

Modüle genel bakış

Güvenlik, yalnızca BT ekibinin kurduğu teknik kontrollerden ibaret değildir. Kimlik avı bağlantısına tıklamamak, bir dosyayı gereğinden geniş paylaşmamak, kayıp cihazdaki oturumu kapatmak ve yapay zekâ aracına gizli bilgi girmemek günlük kullanıcı kararlarıdır. Bu modülde bu kararları Google Workspace arayüzünde nasıl uygulayacağınızı ve bir olaydan şüphelendiğinizde nasıl bildirim yapacağınızı çalışacaksınız.

Anadolu Teknoloji A.Ş. yeni ürün lansmanı hazırlarken Lansman-2026 paylaşılan drive'ında bütçe, plan, sunum ve müşteri kayıtları bir arada işleniyor. Modül sonunda kendi hesabınız için bir güvenlik kontrol listesi dolduracak, artık gerekmeyen üçüncü taraf erişimlerini ve cihaz oturumlarını gözden geçirecek, gereksiz bağlantı paylaşımını Kısıtlanmış yapacak ve üç örnek dosyayı kurum sınıflandırmasına göre etiketleyeceksiniz. Üretilen çıktı, sonraki modüllerde güvenli ortak çalışma için başvuru noktasıdır.

Öğrenme hedefleri

- Kimlik avı e-postalarını, sahte oturum açma sayfalarını, kötü niyetli uygulama izin isteklerini ve QR kodlu saldırıları tanımak.
- Gmail uyarılarını yorumlamak ve şüpheli iletiyi **Kimlik avı bildir** ile bildirmek.
- Hesaba erişimi olan üçüncü taraf uygulamaları ve oturum açılmış cihazları gözden geçirmek.
- En az yetki ilkesine göre paylaşım yapmak; veri kaybını önleme (DLP) uyarılarını ve sınıflandırma etiketlerini anlamak.
- KVKK kapsamındaki kişisel ve özel nitelikli kişisel verileri kurum politikasına uygun biçimde işlemek.
- Gemini ve diğer yapay zekâ araçlarını kullanırken veri koruma kurallarını uygulamak.

Hazırlık

- Katılımcıların Anadolu Teknoloji kurumsal hesaplarında oturum açabildiğini doğrulayın. Kurumun 2 Adımlı Doğrulama, geçiş anahtarı, mobil cihaz yönetimi ve olay bildirim politikasını önceden yazılı olarak paylaşın.
- Eğitimci, Lansman-2026 paylaşılan drive'ında eğitim amaçlı kopya bir klasör hazırlamalıdır. Gerçek müşteri, çalışan, sağlık veya finans verisi kullanmayın.
- BT destek kanalını netleştirin. Bu içerikte örnek olay kanalı [#guvenlik-olaylari](#) Chat alanı ve bt-destek@anadoluteknoloji.example adresidir; gerçek kurum kanalı varsa onu kullanın.
- Business veya Enterprise sürümünü, DLP ve etiketlerin etkin olup olmadığını ve dış paylaşımın yönetici tarafından sınırlandırılıp sınırlandırılmadığını kontrol edin. Bu özellikler her Workspace sürümünde aynı şekilde sunulmaz.
- Katılımcıların denetim sırasında kullanacağı kişisel güvenlik kontrol listesini hazırlayın: 2 Adımlı Doğrulama, geçiş anahtarı, üçüncü taraf erişimi, cihaz oturumları, kurtarma bilgileri, Drive paylaşımı ve olay bildirim kanalı.

1. Tehditleri tanıma: kimlik avı, sahte oturum açma, uygulama izni ve QR saldırıları

🕒 Süre: 20 dakika

Kimlik avı, gerçek kişi veya kuruluş gibi görünerek şifre, finans bilgisi, dosya erişimi ya da hesap yetkisi elde etmeye çalışır. Saldırgan bağlantı tıklatabilir, sahte giriş sayfasına bilgi yazdırabilir, QR kodla telefonda oturum açtırabilir veya Gmail ve Drive erişimi isteyen bir uygulama kullanabilir. Aciliyet dili, görünen ad ile adres uyuşmazlığı, beklenmeyen ek veya bağlantı gibi işaretleri birlikte değerlendirin. QR kod da bir bağlantıdır; oturum açmanız isteniyorsa bilinen adresi kendiniz açın.

Nasıl yapılır?

Bir iletiyi değerlendirirken önce içerik güvenliğini koruyun.

1. Bağlantıya tıklamadan gönderenin görünen adını ve gerçek adresini kontrol edin. Gmail'de gönderen adının üzerine gelerek adresi inceleyin.
2. Konu satırındaki aciliyet, tehdit, olağan dışı ödeme veya parola talebini işaretleyin.
3. Bağlantının üzerine tıklamadan gelin. Tarayıcının alt kısmında görünen adres ile beklenen alan adını karşılaştırın. Benzer harf kullanan veya beklenmeyen bir alan adına dikkat edin.
4. Ek dosyayı açmadan önce mesajı beklediğiniz kanaldan doğrulayın. Örneğin Ayşe Demir gerçekten bir dosya gönderdiyse ona yeni bir Gmail iletilisiyle değil, kurumun bilinen Chat alanından sorun.
5. QR kod varsa taramayın. Gerekliyse kodun yönlendirdiği adresi kurumun BT ekibine olay incelemesi için iletin; ekrandaki oturum açma formuna bilgi yazmayın.
6. Şüpheli varsa iletiyi yanıtlamayın, ekini indirmeyin, gönderenin istediği numarayı aramayın ve **Kimlik avı bildir** seçeneğini kullanın.

Sahte oturum açma sayfasını ayırt etmek için tarayıcı adres çubuğunu kullanın.

1. Sayfanın adres çubuğuna bakın. Kilit simgesi tek başına sayfanın Google'a ait olduğunu kanıtlamaz.
2. Alan adının son bölümünü okuyun. Beklenen kurum veya hizmet alan adı yerine alakasız bir alan adı, uzun bir alt alan adı ya da yazım hatası varsa sayfayı kapatın.
3. Şifre yöneticisi beklenen site için otomatik doldurmuyorsa bunu bir uyarı olarak değerlendirin. Şifreyi elle yazıp denemeyin.
4. Bilgi girdiyseniz hemen kurumun olay kanalına bildirin, Google Hesabı şifrenizi güvenilir bir cihazdan değiştirin ve BT ekibinin yönlendirmesini izleyin.

Kötü niyetli uygulama izinlerini de aynı mantıkla inceleyin.

1. Uygulama Google ile oturum açma ekranı gösterdiğinde istenen ürünleri ve izinleri okuyun. Gmail, Drive, Takvim veya Kişiler erişimi iş ihtiyacıyla ilgili değilse devam etmeyin.
2. Uygulama sizden Google Hesabı şifrenizi doğrudan kendi formuna yazmanızı istiyorsa işlemi durdurun. Güvenilir bağlantı, Google'ın kendi yetkilendirme ekranına yönlendirir.
3. Uygulamanın geliştiricisini, kurum tarafından onaylanıp onaylanmadığını ve istediği erişimin kapsamını doğrulayın.

DİKKAT QR kod, logo, kilit simgesi ve tanıdık görünen bir gönderen adı güven kanıtı değildir. Şifreyi, 2 Adımlı Doğrulama kodunu veya geçiş anahtarını başka bir kişiye vermeyin.

EĞİTMEN NOTU Altı örneği gösterin; katılımcılardan işaretleri ve karar gerekçelerini isteyin. Ek bölümündeki kurgusal adları kullanın.

İpuçları ve sık yapılan hatalar

- Eski bir yazışma zinciri, yeni eki veya bağlantıyı güvenilir yapmaz.
- Yönetici adı, logo, kilit simgesi veya QR kod güven kanıtı değildir; isteği ikinci kanaldan doğrulayın.

2. Gmail uyarıları, kimlik avını bildirme ve Tümünü yanıtla gizlilik kontrolü

⌚ Süre: 15 dakika

Gmail bazı iletileri spam veya kimlik avı şüphesiyle işaretler, ancak uyarı olmaması güvenlik garantisi değildir. **Kimlik avı bildir** kandırma ve bilgi çalma girişimini, **Spam bildir** ise istenmeyen iletiyi sınıflandırır. Bcc alıcısı diğer kişiler tarafından görünmez. Alıcı veya Cc satırında olmayan kişi **Tümünü yanıtla** seçeneğine bastığında Gmail, dahil edildiğini herkese açıklayabileceğini bildiren bir uyarı gösterebilir.

Nasıl yapılır?

Kimlik avı olarak bildirme adımları şöyledir.

1. Bilgisayarda Gmail'i açın ve şüpheli iletiyi açın.
2. Yanıtla simgesinin yanındaki **Diğer** simgesini tıklayın.
3. **Kimlik avı bildir** seçeneğini tıklayın.
4. Kurum prosedürü istiyorsa iletiyi ayrıca [#güvenlik-olaylari](#) alanına iletin veya bt-destek@anadoluteknoloji.example adresine olayın saatini ve kısa açıklamasını gönderin. İletiyi yeni kişilere yönlendirirken ek bilgi sızdırmamaya dikkat edin.

Yanlışlıkla kimlik avı bildirimi yaptıysanız düzeltme adımları şöyledir.

1. İletiyi Gmail'de açın.
2. Yanıtla simgesinin yanındaki **Diğer** simgesini tıklayın.
3. **Kimlik avı olmadığını bildir** seçeneğini tıklayın.
4. Kurum BT ekibine yanlış bildirimi ve nedenini haber verin. Şüpheli bir dosyayı güvenilir diye işaretlemekten önce yeniden doğrulayın.

Tümünü yanıtla öncesi alıcı kontrolü yapın.

1. İletiyi açın ve **Tümünü yanıtla** seçeneğine tıklamadan önce Alıcı, Cc ve varsa Bcc bilgisini inceleyin.
2. "Alıcı listesinde değilsiniz..." uyarısı görünürse gönderimin sizi görünür kılacağını varsayın.
3. Herkese yanıt vermek gerekmiyorsa **Yanıtla** seçeneğini kullanın veya yeni bir ileti oluşturun.
4. Alıcı listesini elle kontrol edin. Gizli bir alıcının adresini başkalarına açıklayabilecek bir yanıt göndermeyin.
5. Yanıt içeriğinde kişisel, finansal veya kurum içi bilgi varsa gönderimden önce alıcıları son kez doğrulayın.

İPUCU Şüpheli iletinin ekran görüntüsünü almak yerine mümkünse ileti başlıklarını ve Gmail bildirimini kurumun olay prosedürüne göre paylaşın. Ekran görüntüsünde başka kişilerin adresleri bulunabilir.

EĞİTMEN NOTU Bir örneği Bcc alıcısı olacak şekilde canlandırın. Katılımcılardan uyarı çıktığında "Gönder" yerine hangi güvenli seçimi yapacaklarını söylemelerini isteyin. İşlev tüm Workspace müşterileri ve kişisel hesaplarda varsayılan olarak sunulsa da arayüz dili ve dağıtım zamanı farklı görünebilir.

İpuçları ve sık yapılan hatalar

- Kimlik avı bildiriminden önce iletiyi yanıtlamayın.
- Tümünü yanıtla uyarısı Bcc dışında yönlendirme veya yetki devriyle iletiyi alan kişilerde de görülebilir.

3. Hesap güvenliği: 2 Adımlı Doğrulama, geçiş anahtarı, üçüncü taraf erişimi ve cihaz oturumları

⌚ Süre: 15 dakika

Hesap güvenliği katmanlıdır. 2 Adımlı Doğrulama şifreye ikinci bir adım ekler; geçiş anahtarı kişisel cihazın ekran kilidini kullanır. Üçüncü taraf erişimleri ve eski cihaz oturumları düzenli olarak incelenmelidir.

Nasıl yapılır?

2 Adımlı Doğrulama'yı kontrol etmek veya açmak için aşağıdaki yolu kullanın.

1. myaccount.google.com adresini açın ve doğru kurumsal hesabı seçin.
2. **Güvenlik ve oturum açma** bölümüne gidin.
3. **Google'da oturum açma** bölümünde **2 Adımlı Doğrulama'yı açın** veya mevcut ayarı seçin.
4. Ekrandaki kimlik doğrulama adımlarını tamamlayın. Mümkünse kurumun onayladığı Google istemi, geçiş anahtarı veya güvenlik anahtarını tercih edin.
5. Yedek kodları oluşturduysanız bunları parola yöneticisi veya kurumun onaylı güvenli saklama yöntemi dışında bir yerde paylaşmayın.

İş, okul veya grup hesabında 2 Adımlı Doğrulama seçeneği görünmeyebilir. Kurum yöneticisi bu özelliği zorunlu kılabilir, yöntemleri sınırlandırabilir veya kurulumu kendi politikasıyla yönetebilir. Bu durumda ayarı değiştirmeye çalışmak yerine BT ekibine başvurun.

Geçiş anahtarı oluşturmak için:

1. myaccount.google.com/signinoptions/passkeys adresini açın.
2. Gerekirse kimliğinizi doğrulayın ve **Geçiş anahtarı oluştur** seçeneğini seçin.
3. Yalnızca size ait, ekran kilidi bulunan bir cihazda devam edin.
4. Parmak izi, yüz tanıma veya cihaz PIN'i ile onaylayın.
5. Paylaşılan bilgisayarda geçiş anahtarı oluşturmayın. Cihaz kaybolursa başka bir güvenilir cihazdan hesabınızdaki geçiş anahtarlarını inceleyip kayıp cihazdakini kaldırın.

Üçüncü taraf uygulamaları incelemek için:

1. myaccount.google.com/linkedapps adresini açın.
2. **Bağlı uygulamalarınızı görüntüleyin** bağlantısına gidin ve listelenen uygulamayı seçin.
3. Uygulamanın hangi Google ürünlerine ve hangi izin düzeyinde eriştiğini okuyun.
4. Artık kullanılmayan veya kurum tarafından onaylanmamış uygulamada **Erişimi kaldır** ya da arayüzde görünen eşdeğer kaldırma seçeneğini kullanın.
5. Uygulama iş için gerekliyse kaldırmadan önce BT ekibine sorun. Erişimi kaldırmak uygulamadaki verileri veya uygulama hesabını mutlaka silmez.

Cihaz oturumlarını incelemek için:

1. myaccount.google.com adresini açın.
2. **Güvenlik ve oturum açma** bölümünde **Cihazlarınız** panelini bulun.

3. **Tüm cihazları yönet** seçeneğini tıklayın.
4. Cihaz veya oturum ayrıntılarını açın. Aynı cihaz adı altında birden fazla oturum olabileceğini dikkate alın.
5. Kayıp, artık kullanılmayan veya size ait olmayan cihazı seçin ve **Oturumu kapat** seçeneğini kullanın.
6. Tanımadığınız bir oturum varsa önce oturumu kapatın, ardından şifreyi güvenilir bir cihazdan değiştirin ve BT ekibine olay bildirimini yapın.

DİKKAT Bir cihazı tanımamanız her zaman saldırı anlamına gelmez. Seyahat, yeni tarayıcı, gizli pencere veya arka plan senkronizasyonu farklı konum ve zaman gösterebilir. Yine de emin olmadığınız oturumu kapatmak ve BT'ye bildirmek güvenli yaklaşımdır.

EĞİTMEN NOTU Katılımcılara kendi ekranlarında gerçek uygulama adlarını ve erişim kapsamını göstermelerini söyleyin; herhangi bir uygulamayı sınıf önünde kaldırmaları zorunlu olmasın. Demo hesabında “artık kullanılmayan deneme uygulaması” ve eski cihaz oturumu bulundurun.

İpuçları ve sık yapılan hatalar

- Geçiş anahtarı diğer giriş faktörlerini otomatik olarak silmez; hesap yöntemlerini ayrıca kontrol edin.
- Oturum kapatma, cihazın fiziksel olarak kilitlenmesi veya uzaktan silinmesi değildir.

4. Paylaşım hijyeni: en az yetki, son kullanma tarihi, dış paylaşım, DLP ve etiketler

🕒 **Süre: 20 dakika**

En az yetki ilkesi, gereken en düşük erişimi, gerektiği süre boyunca vermektir. Görüntüleyen veya Yorumcu yeterliyse Düzenleyen vermeyin. **Bağlantıya sahip olan herkes** seçeneği bağlantıyı alan kişilerin dosyayı açabilmesine yol açabilir. Drive izinleri klasörden dosyaya devredilir; DLP ve sınıflandırma etiketleri yönetici politikalarına bağlıdır.

Nasıl yapılır?

Bir dosyanın paylaşımını denetlemek için:

1. Google Drive'da dosyayı bulun. Örnek dosya [2026-11-03_Lansman_Plan_v01](#) olsun.
2. Dosyayı seçin ve **Paylaş** seçeneğini açın.
3. Her kişi için rolü inceleyin. Gerekmiyorsa Düzenleyen'i Yorumcu veya Görüntüleyen'e indirin.
4. **Genel erişim** bölümünü kontrol edin. Gerekli değilse **Kısıtlanmış** seçin.
5. Kurum dışı bir kişi gerekiyorsa yalnızca o kişinin kurumsal veya onaylı dış adresini ekleyin. Pusula Ajans'tan Selin Koç gibi dış ortaklarda kurum politikasını kontrol edin.
6. İzin geçici ise kişinin yanındaki aşağı oku açın ve **Geçerlilik bitiş tarihi ekle** seçeneğini kullanın. Bu seçenek iş veya okul hesaplarında yönetici ve lisans ayarlarına bağlı olabilir.
7. Gerekirse **Ayarlar** bölümünde **Düzenleyenlerin paylaşmasına ve izinleri değiştirmesine izin ver** seçeneğini kapatın. Üst klasör izinlerinin bu ayarı geçersiz kılabileceğini unutmayın.
8. **Bitti** seçeneğini tıklayın ve dosyanın bağlantısını yalnızca gerekli kişilere gönderin.

“Bağlantıya sahip olan herkes” erişimini Kısıtlanmış yapmak için:

1. Dosyayı seçin ve **Paylaş** seçeneğini tıklayın.
2. **Genel erişim** bölümündeki aşağı oku açın.
3. **Kısıtlanmış** seçeneğini seçin.
4. Erişmesi gereken kişilerin tek tek listede bulunduğunu kontrol edin.
5. **Bitti** seçeneğini tıklayın.

Etiket uygulamak için:

1. Drive'da dosyayı seçin ve sağ tıklayın.
2. **Etiketler > Etiketleri uygula** seçeneğini tıklayın.
3. Kurumun yayımladığı sınıflandırma etiketini seçin.
4. Alan varsa uygun değeri seçin, örneğin **Kurum içi** veya **Gizli**.
5. **Uygula** ya da arayüzde görünen kaydetme seçeneğini tıklayın. Etiketler görünmüyorsa yönetici henüz etiket yayımlamamış veya size erişim vermemiş olabilir.

DİKKAT DLP uyarısını yalnızca “engel” olarak görmeyin. Uyarı, paylaşımın riskli veri içerdiğini bildirir. Dosya sahibi, alıcı, üst klasör, ortak drive ve bağlantı erişimini birlikte incelemekten dış paylaşımı sürdürmeyin.

EĞİTMEN NOTU Demo olarak **Lansman Başlangıç Toplantısı** dosyasını önce “Bağlantıya sahip olan herkes” yapıp risk sorusu sorun, sonra Kısıtlanmış'a döndürün. Ardından **Lansman Bütçesi** için Mehmet Kaya'ya Düzenleyen, Zeynep Arslan'a Yorumcu, Elif Şahin'e Görüntüleyen rolleri verilecek bir örnek tasarlayın.

İpuçları ve sık yapılan hatalar

- Klasör veya paylaşılan drive izni dosya ayarını geçersiz kılabilir.
- Etiket tek başına şifreleme veya erişim değişikliği değildir; DLP ilişkisini BT ekibinden öğrenin.

5. KVKK ve kurum politikaları: kişisel veri, aydınlatma, kayıt ve transkript

⌚ Süre: 20 dakika

6698 sayılı Kanun bakımından kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin bilgidir. Ad, kurumsal e-posta, telefon, müşteri kaydı, ses kaydı ve toplantı transkripti bağlama göre kişisel veri olabilir. Sağlık, biyometrik ve genetik veriler; ceza mahkûmiyeti; siyasi veya dini inanç ve sendika üyeliği gibi veriler özel nitelikli kişisel veri kapsamındadır. Aydınlatma bilgi vermeyi; kayıt ve transkript erişim ve saklama kontrolünü gerektirir.

Nasıl yapılır?

Bir dosyayı veya iletiyi Workspace'e koymadan önce veri minimizasyonu kontrolü yapın.

1. İşlem amacını tek cümleyle yazın: örneğin “Lansman kayıt formundan teslimat planı yapmak”.
2. Amaç için zorunlu olmayan alanları kaldırın veya anonimleştirin. T.C. kimlik numarası, sağlık bilgisi veya tam doğum tarihi gerekmiyorsa toplamayıp paylaşmayın.
3. Kurumun aydınlatma metninin ilgili kişiye sunulup sunulmadığını kontrol edin. Bu metin yoksa veri toplamayı durdurup KVKK sorumlusuna sorun.

4. Dosyayı yalnızca işi olan kişilerle paylaşın ve sınıflandırma etiketi uygulayın.
5. Saklama süresini ve silme sorumlusunu kayda geçirin. “Sonsuza kadar Drive’da dursun” bir saklama politikası değildir.
6. Dış hizmet, uygulama veya yapay zekâ aracı kullanılacaksa kurumun onaylı araç listesinde olup olmadığını kontrol edin.

Meet kaydı veya transkripti için:

1. Toplantı davetinde kaydın veya transkriptin gerekip gerekmediğini belirtin.
2. Katılımcılara kayıt başladığında ekrandaki bildirimi ve kurum politikasını açıklayın.
3. Kayıt dosyasının kimde olduğunu, kimlerin erişeceğini ve hangi klasöre gideceğini kontrol edin.
4. Görüşmede gereksiz kişisel veya özel nitelikli veri paylaşılmasını önleyin. Bir katılımcı sağlık veya disiplin bilgisi açıklarsa bunu yeniden paylaşmayın.
5. Toplantı sonrasında dosyayı Kısıtlanmış erişimde tutun, gerekli kişileri ekleyin ve saklama süresi dolduğunda kurum prosedürüne göre silin veya arşivleyin.

Bir veri olayı fark ettiğinizde:

1. Dosyayı daha fazla kişiye iletmeyin ve kanıtı değiştirmeyin.
2. Yanlış alıcıya gönderilen iletiye hemen BT ve kurumun KVKK olay kanalına haber verin.
3. Olayın zamanını, dosya veya ileti adını, alıcıları ve yaptığınız ilk işlemi yazın.
4. Kendi başınıza ilgili kişiye hukuki bildirim yapmayın. Kurumun veri sorumlusu veya olay müdahale ekibinin talimatını bekleyin.

NOT Bu bölüm eğitim amaçlı bir çalışma çerçevesidir, hukuki görüş değildir. Veri sorumlusu, veri işleyen, açık rıza, aydınlatma, saklama ve yurt dışına aktarım değerlendirmelerini Anadolu Teknoloji’nin yetkili KVKK ve hukuk ekipleri yapar.

EĞİTMEN NOTU Katılımcılara gerçek kişisel veri göstermeden **Lansman Kayıt Formu** için üç alan verin: ad-soyad, şirket e-postası, teslimat tercihi. Hangi alanın neden gerekli olduğunu ve hangi bilginin örnek olarak hiç toplanmaması gerektiğini tartışın. Kurumun aydınlatma metnini ve olay kanalını yazılı olarak dağıtın.

İpuçları ve sık yapılan hatalar

- “Kurumsal hesapta duruyor” ifadesi tek başına KVKK uyumu anlamına gelmez.
- Meet transkripti, konuşmadaki kişisel verileri aranabilir yeni bir dosya biçiminde çoğaltır.

6. Yapay zekâ ve veri: Workspace taahhütleri, hesap ayrımı ve gizli bilgi kuralları

🕒 **Süre: 15 dakika**

Workspace içindeki Gemini ile kişisel hesapta kullanılan Gemini uygulamasının veri koşulları aynı olmayabilir. Workspace’te Gemini mevcut erişim denetimlerini izler; bu, yanlış paylaşımı veya kişisel hesaba kopyala-yapıştır riskini ortadan kaldırmaz. Hesap türünü, kurumun onaylı aracı ve verinin sınıflandırmasını her istemden önce kontrol edin.

Nasıl yapılır?

Gemini'a istem göndermeden önce “veri sınıfı, amaç, hesap, çıktı” kontrolü yapın.

1. Sağ üst profil menüsünden kurumsal @anadoluteknoloji.example hesabını ve isteme gireceğiniz verinin sınıflandırmasını kontrol edin. “Gizli” veya özel nitelikli içeriği açık izin yoksa yapıştırmayın.
2. Veriyi en aza indirin; gerçek ad, e-posta, müşteri numarası veya sözleşme ayrıntısı yerine anonimleştirilmiş örnek kullanın.
3. İstemi, “Lansman Planı” gibi kullanıcının erişebildiği onaylı Workspace özelliğinde gönderin; harici Gemini veya üçüncü taraf eklenti kullanmayın.
4. Yanıtı gerçek kabul etmeyin. Dosyaya eklemekten önce paylaşım izinlerini, etiketi ve DLP uyarısını kontrol edin.
5. Gereksiz kişisel bilgi görünüyorsa çıktıyı paylaşmayın; istemi ve yanıtı kurumun gizlilik kanalına sorun.

Üçüncü taraf yapay zekâ aracı için:

1. Uygulamanın kurum tarafından onaylandığını, hangi hesapla oturum açtığınızı ve Gmail, Drive, Takvim veya Kişiler izinlerini kontrol edin.
2. Gizli dosya yüklemekten önce BT veya KVKK ekibine danışın; gerekli değilse erişim vermeyin ve verilen izni **Bağlı uygulamalar** sayfasından gözden geçirin.

GEMINI Güvenli örnek istem: “Aşağıdaki anonimleştirilmiş lansman görevlerini önem ve son tarihe göre gruplandır. Kişi adlarını, müşteri adlarını ve iletişim bilgilerini çıktıda tekrar etme.”
Gerçek **Lansman Bütçesi** içeriğini kişisel hesaba yapıştırmayın.

DİKKAT “Workspace verileri model eğitimi için kullanılmaz” taahhüdü, kişisel hesapla kullanılan Gemini uygulaması veya onaysız başka bir yapay zekâ hizmeti için otomatik olarak geçerli değildir. Hesap türünü, hizmeti ve yönetici politikasını ayırın.

EĞİTMEN NOTU İki istemi karşılaştırın: biri gerçek müşteri e-postalarını içerir, diğeri alanları anonimleştirir. Katılımcılardan hangi bilgileri çıkarmaları gerektiğini ve hangi hesabı kullanacaklarını açıklamalarını isteyin. Gemini özelliği görünmüyorsa bunun lisans, yönetici ayarı, dil veya kademeli dağıtım nedeniyle olabileceğini belirtin.

İpuçları ve sık yapılan hatalar

- Gemini'in bir dosyayı görebilmesi, dosyanın herkese açık olması gerektiği anlamına gelmez.
- Özellik görünürlüğü hesap, lisans, yönetici ayarı ve kademeli dağıtıma bağlı olabilir.

7. Mobil cihaz güvenliği ve cihaz kaybında yapılacaklar

🕒 **Süre: 10 dakika**

Telefon ve tabletler Gmail, Drive, Chat, Meet ve 2 Adımlı Doğrulama bildirimlerine erişebilir. Kayıp cihazda önce hesabı ve açık oturumları koruyun; ardından BT'nin uzaktan kilitleme veya silme prosedürünü uygulayın.

Nasıl yapılır?

Kayıp veya çalınmış cihaz için ilk dakikalarda şu sırayı izleyin.

1. Başka bir güvenilir cihazda myaccount.google.com adresini açın; başkasının cihazında gizli tarama kullanın.
2. **Güvenlik > Cihazlarınız > Tüm cihazları yönet** yoluyla kayıp cihazı seçin ve **Oturumu kapat** seçeneğini kullanın.
3. Google Hesabı şifresini değiştirin; geçiş anahtarlarını, 2 Adımlı Doğrulama yöntemlerini ve üçüncü taraf erişimlerini kontrol edin.
4. Cihazın son görüldüğü zamanı ve yaptığınız işlemleri BT'ye bildirin; kurumun uzaktan kilitleme veya silme talebini açın.
5. Cihaz bulunursa BT kontrolü tamamlanmadan yeniden kullanmayın.

Önleyici ayarlar için:

1. Güçlü ekran kilidi ve otomatik kilit kullanın; işletim sistemi ile Workspace uygulamalarını güncel tutun.
2. Kilit ekranında Gmail, Chat ve doğrulama bildirimlerinin içeriğini göstermemeyi, ortak cihazlarda oturum açık bırakmamayı değerlendirin.
3. Cihazı devretmeden önce kurumun çıkış ve uzaktan silme prosedürünü uygulayın.

DİKKAT Cihazdaki oturumu kapatmak, kayıp cihazın içindeki yerel dosyaları veya başka uygulamaların kayıtlı şifrelerini otomatik olarak silmeyebilir. BT ekibinin uzaktan kilitleme, silme ve cihaz yönetimi adımlarını ayrıca uygulaması gerekir.

EĞİTMEN NOTU Kayıp cihaz kartında cihaz seçme, oturum kapatma, şifre değişikliği, üçüncü taraf erişimi ve olay kanalı sırasını katılımcılarla doldurun.

İpuçları ve sık yapılan hatalar

- Kayıp cihazı bulmayı beklemek hesabı koruma işlemini geciktirir.
- Google Hesabı oturum kapatma ile işletim sisteminin uzaktan silinmesi farklı işlemlerdir.

Uygulama çalışması: Kişisel güvenlik denetimi

Anadolu Teknoloji A.Ş. lansman hazırlığında Ayşe Demir'in proje ekibi, Mehmet Kaya'nın finans çalışmaları, Zeynep Arslan'ın pazarlama içeriği ve Pusula Ajans'tan Selin Koç'un dış katkılarıyla çalışıyor. Bu görevlerde gerçek veri kullanmayın. Eğitmenin paylaştığı kopya dosyalar, kurgusal e-posta örnekleri ve eğitim hesabı kullanılmalıdır.

Görevler

1. Eğitmenin paylaştığı altı örnek e-postayı inceleyin; en az dört kimlik avı, en az bir meşru ve bir sınırda/şüpheli örneği gerekçeleriyle belirleyin.
2. Google Hesabı > Güvenlik ve oturum açma > Üçüncü taraf uygulamalar ve hizmetler bağlantıları ekranında artık kullanmadığınız uygulamaların erişimini kaldırın.
3. **Cihazlarınız** bölümünde tanımadığınız veya artık kullanmadığınız cihazlardaki oturumu kapatın.

4. Drive'da sahibi olduğunuz eğitim dosyaları arasında **Bağlantıya sahip olan herkes** erişimine açık olanları bulun ve gerekli olmayanları **Kısıtlanmış** yapın.
5. Kurumun veri sınıflandırma düzeylerine göre üç örnek dosyayı etiketleyin: **Lansman Planı**, **Lansman Bütçesi** ve **Lansman Yönetici Sunumu**.
6. Kişisel güvenlik kontrol listesini doldurun ve üç ayda bir tekrar etmek için Google Takvim'e hatırlatıcı ekleyin.

Çözüm anahtarı

Görev 1: Örnek e-postaları sınıflandırma

1. Ek bölümündeki altı örnek e-postayı açın; bağlantılara, eklere ve QR kodlara tıklamayın.
2. Gönderen adresi, konu, talep ve doğrulanabilirlik işaretlerini not edin.
3. En az dört örneği kimlik avı, bir örneği meşru, bir örneği sınırda/şüpheli olarak sınıflandırın.
4. Şüpheli örnekte **Diğer > Kimlik avı bildir** seçeneğini kullanın; sınırda örneği bilinen kanaldan doğrulamadan paylaşmayın.

Görev 2: Üçüncü taraf erişimini kaldırma

1. myaccount.google.com/linkedapps adresini açın ve Anadolu Teknoloji hesabını seçin.
2. **Bağlı uygulamalarınızı görüntüleyin** bağlantısını tıklayın.
3. Öğretmenin "Lansman Geri Bildirim Denemesi" olarak işaretlediği artık kullanılmayan uygulamayı seçin.
4. Erişim kapsamını okuyun ve **Erişimi kaldır** seçeneğini tıklayın.
5. Onaylayın ve uygulama listesinde erişimin kaldırıldığını kontrol edin. İş için gerekli bir uygulamayı kaldırıyorsanız BT'ye haber verin.

Görev 3: Cihaz oturumlarını gözden geçirme

1. myaccount.google.com adresini açın.
2. **Güvenlik ve oturum açma** bölümüne gidin.
3. **Cihazlarınız** panelinde **Tüm cihazları yönet** seçeneğini tıklayın.
4. Öğretmenin "eski dizüstü bilgisayar" olarak belirttiği oturumu seçin.
5. **Oturumu kapat** seçeneğini tıklayın ve onaylayın. Aynı ad altında tanımadığınız oturum varsa hepsini kapatıp BT'ye bildirin.

Görev 4: Drive genel erişimini düzeltme

1. Google Drive'da **Lansman-2026** paylaşılan drive'ını ve eğitim için açılmış dosyaları bulun.
2. Dosyayı seçin ve **Paylaş** seçeneğini tıklayın.
3. **Genel erişim** bölümünde **Bağlantıya sahip olan herkes** seçiliyse dosyanın iş gereksinimini değerlendirin.
4. Gerekli olmayan dış erişim için aşağı oku tıklayın ve **Kısıtlanmış** seçeneğini seçin.
5. Gerekli kişileri uygun rollerle ekleyin, **Bitti** seçeneğini tıklayın ve üst klasör veya paylaşılan drive izinlerini **Erişimi yönet** ekranında kontrol edin.

Görev 5: Dosyaları sınıflandırma etiketiyle işaretleme

1. Drive'da **Lansman Planı**, **Lansman Bütçesi** ve **Lansman Yönetici Sunumu** eğitim kopyalarını bulun.

2. İlk dosyayı seçin, sağ tıklayın ve **Etiketler > Etiketleri uygula** seçeneğini tıklayın.
3. Kurumun “Veri sınıflandırması” etiketini seçin.
4. Üç dosyada politika gerektiren değeri seçin, **Uygula** seçeneğini tıklayın. Etiket menüsü yoksa etiketi kendiniz oluşturmayın ve yöneticiden erişim isteyin.

Görev 6: Kontrol listesi ve üç aylık hatırlatıcı

1. Kontrol listenize 2 Adımlı Doğrulama, geçiş anahtarı, üçüncü taraf erişimi, cihaz oturumları, Drive genel erişimleri, sınıflandırma etiketleri ve olay kanalını yazın.
2. Google Takvim'de **Oluştur > Etkinlik** seçeneğini tıklayın; başlığa “Kişisel güvenlik denetimi” yazıp üç ay sonraki tarihi seçin.
3. **Tekrarlanmaz > Özel** yoluyla üç aylık tekrarı ayarlayın, açıklamaya kontrol listesini ve BT kanalını yazın; şifre eklemeyin.
4. **Kaydet** seçeneğini tıklayın ve hatırlatıcıyı kontrol edin.

Başarı ölçütleri

- ☐ Altı e-postanın sınıflandırmasını, en az üç somut işaretle gerekçelendirdim.
- ☐ Artık kullanılmayan üçüncü taraf uygulamasının erişimini kaldırdım veya neden kaldıramadığımı kaydettim.
- ☐ Tanımadığım veya eski cihaz oturumunu kapattım ve gerektiğinde BT'ye bildirdim.
- ☐ Gereksiz “Bağlantıya sahip olan herkes” erişimini Kısıtlanmış yaptım.
- ☐ Üç dosyaya kurum politikasına uygun sınıflandırma etiketi uyguladım.
- ☐ Kişisel güvenlik kontrol listesini doldurdum ve üç aylık hatırlatıcı ekledim.

Bilgi kontrolü

#	Soru	Beklenen yanıt
1	Bir kimlik avı e-postasının üç tipik belirtisi nedir?	Aciliyet veya tehdit dili, gönderen adresiyle görünen ad arasında uyumsuzluk ve beklenmedik ek ya da oturum açma bağlantısı.
2	Şüpheli bir e-postayı aldığınızda ne yapmalısınız?	Bağlantıya tıklamadan ve eki açmadan Kimlik avı bildir ile bildirmeli, gerekiyorsa BT ekibine haber vermelisiniz.
3	En az yetki ilkesi paylaşımında ne anlama gelir?	Kişiye işini yapması için gereken en düşük erişimi, gerektiği süre boyunca vermektir.
4	Kimlik avı bildir ile Spam bildir arasındaki fark nedir?	Kimlik avı bildir kandırma ve bilgi çalma girişimini, Spam bildir ise istenmeyen iletinin sınıflandırılmasını hedefler.
5	Bağlantıya sahip olan herkes erişimi neden risklidir?	Bağlantıyı alan kişiler, hesapta oturum açmaları gerekmeksizin dosyayı açabilir; kurum dışı paylaşım politikası da ihlal edilebilir.
6	DLP uyarısı gördüğünüzde son kullanıcı ne yapabilir?	Uyarıdaki hassas veri ve alıcıları kontrol eder, paylaşımı durdurur veya kurum politikasının izin verdiği gerekçeli işlemi yapar; DLP kuralını kendisi değiştirmez.
7	Gemini'a gizli bilgi girmeden önce hangi üç şeyi kontrol edersiniz?	Hesap türünü, kurumun onaylı araç ve yönetici politikasını, verinin sınıflandırmasını ve istem için gerçekten gerekli olup olmadığını kontrol ederim.
8	Kayıp cihazda ilk güvenlik adımları nelerdir?	Güvenilir cihazdan oturumu kapatmak, şifreyi değiştirmek, geçiş anahtarı ve üçüncü taraf erişimlerini incelemek, BT'ye bildirmek ve kurumun uzaktan kilitleme veya silme prosedürünü uygulamaktır.

Sık sorulan sorular

S: Gmail uyarı göstermediyse ileti güvenli midir?

C: Hayır. Gmail'in otomatik uyarısı bir yardımcı kontroldür. Gönderen adresini, bağlantıyı, ekleri, talebin bağlamını ve ikinci kanaldan doğrulamayı yine kontrol etmelisiniz.

S: Bir iletiyi hem spam hem kimlik avı olarak bildirebilir miyim?

C: Şüpheli ileti için öncelikle **Diğer > Kimlik avı bildir** seçeneğini kullanın. Kurum prosedürü ayrıca spam sınıflandırması istiyorsa bunu BT ekibine sorun; aynı iletiyi gereksiz yere farklı kişilere yönlendirmeyin.

S: Tanımadığım cihaz oturumunu hemen kapatmalı mıyım?

C: Ayrıntıları ve seyahat, yeni tarayıcı veya gizli pencere gibi açıklamaları kontrol edin. Emin değilseniz oturumu kapatın, şifreyi değiştirin ve BT'ye bildirin.

S: Kısıtlanmış erişim, dosyayı yalnızca benim görebileceğim anlamına mı gelir?

C: Hayır. Kısıtlanmış genel bağlantıyı kapatır; eklenmiş kişiler ve üst klasör izinleri sürebilir. **Erişimi yönet** ekranını inceleyin.

S: Etiket menüsünü göremiyorum. Ne yapmalıyım?

C: Etiketler yönetici oluşturup erişim verdiyse görünür. Kendiniz oluşturmayın; yöneticiden yayımlama ve erişim durumunu sorun.

S: Yanlış kişiye dosya gönderdim. Dosyayı hemen silmem yeterli mi?

C: Hayır. Erişimi kaldırın; dosya ve alıcı bilgilerini değiştirmeden BT ile KVKK olay kanalına bildirin ve olay ekibinin talimatını izleyin.

Akılda kalsın

- Tıklamadan önce durun; göndereni, alan adını, talebi ve eki ayrı ayrı doğrulayın.
- QR kod da bağlantıdır; kodla açılan sayfada şifre yazmadan adresi kontrol edin.
- Şüpheli iletiyi yanıtlamayın; **Diğer > Kimlik avı bildir** yolunu kullanın.
- 2 Adımlı Doğrulama, geçiş anahtarı, üçüncü taraf erişimi ve cihaz oturumlarını düzenli olarak gözden geçirin.
- Paylaşımında en düşük rolü, en dar kapsamı ve gerekiyorsa son kullanma tarihini seçin.
- “Bağlantıya sahip olan herkes” seçeneğini varsayılan değil, istisna olarak değerlendirin.

Ek: Eğitim materyalleri

Aşağıdaki örnekler kurgusaldır. Gerçek marka logoları, alan adları veya müşteri bilgileri kullanmayın; [.example](#) alan adları eğitim dışı çalışmaz.

Örnek 1: Acil hesap doğrulaması

Alan	İçerik
Gönderen adı	Anadolu Teknoloji BT Destek
Gönderen adresi	bt-destek@anadoluteknoloji-security.example
Konu	15 dakika içinde Workspace hesabınızı doğrulayın
Gövde metni	Hesabınızda olağan dışı etkinlik tespit edildi. Erişiminizin kesilmemesi için aşağıdaki QR kodu tarayın ve Google şifrenizi yeniden girin. İşlemi 15 dakika içinde tamamlamazsanız hesabınız askıya alınacaktır.

Alan	İçerik
Doğru yanıt	Kimlik avı
İpuçları	Görünen ad tanıdık olsa da alan adı kurumun gerçek alan adı değil; tehdit ve aciliyet dili var; QR kodla giriş isteniyor; şifre talep ediliyor.

Örnek 2: Sahte teslimat ücreti

Alan	İçerik
Gönderen adı	KargoHızlı Teslimat
Gönderen adresi	takip@kargohizli-odeme.example
Konu	Lansman paketi için 42,90 TL ek ücret
Gövde metni	Anadolu Teknoloji adına gelen paketiniz gümrükte bekliyor. Teslimatı bugün tamamlamak için kart bilgilerinizi aşağıdaki bağlantıda doğrulayın. Aksi halde paket iade edilecektir.
Doğru yanıt	Kimlik avı
İpuçları	Beklenmeyen ödeme ve iade tehdidi var; gönderen alan adı doğrulanmamış; kart bilgisi isteniyor; bağlantı gerçek kargo kanalından bağımsız.

Örnek 3: Kötü niyetli uygulama izni

Alan	İçerik
Gönderen adı	Lansman Geri Bildirim Portalı
Gönderen adresi	izin@lansman-anket.example
Konu	Anketi tamamlamak için Google Drive erişimi gerekli
Gövde metni	Kısa ankete katılmak için Google ile devam edin. Uygulama, Drive dosyalarınızı okuma ve değiştirme izni istiyor. Anketi kapatmak için "İzin ver" düğmesine basın.
Doğru yanıt	Kimlik avı veya kötü niyetli uygulama tuzağı
İpuçları	Basit bir anket için tüm Drive'a okuma ve değiştirme izni orantısız; uygulama kurum tarafından doğrulanmamış; izin ekranı dikkatle incelenmeli; izin verilmemeli.

Örnek 4: QR kodlu sahte toplantı daveti

Alan	İçerik
Gönderen adı	Lansman Başlangıç Toplantısı Takvim Hizmeti
Gönderen adresi	toplantilar@takvim-onay.example
Konu	Meet bağlantınız yenilendi, QR kodu tarayın
Gövde metni	Toplantı odasının değişmesi nedeniyle yeni Meet bağlantısı oluşturuldu. Telefonda daha hızlı katılmak için aşağıdaki QR kodu tarayın. Katılmak için Google hesabınızla oturum açın.
Doğru yanıt	Kimlik avı
İpuçları	Takvim davetindeki bilinen toplantı yerine yeni bir alan adı kullanılıyor; QR kod ve oturum açma birlikte isteniyor; bağlantı taranmadan Google Takvim'deki asıl etkinlik kontrol edilmeli.

Örnek 5: Kurum içi BT bakım duyurusu

Alan	İçerik
Gönderen adı	Anadolu Teknoloji BT Destek
Gönderen adresi	bt-destek@anadoluteknoloji.example
Konu	8 Kasım planlı bakım, işlem yapmanız gerekmiyor
Gövde metni	Merhaba, 8 Kasım 22.00-23.00 arasında planlı bakım yapılacaktır. Bu duyuru bilgi amaçlıdır; sizden şifre, kod, ödeme veya bağlantı üzerinden doğrulama istenmez. Sorularınız için kurum içi #bt-duyurular alanını kullanabilirsiniz.
Doğru yanıt	Meşru örnek, yine de bağlamla doğrulanır
İpuçları	Alan adı kurumla eşleşiyor; tehdit veya bilgi talebi yok; bağlantı ve QR kod yok; duyuru kurum içi kanalla tutarlı. Yine de beklenmeyen değişiklik varsa BT'den doğrulanır.

Örnek 6: Sınırdaki dış ajans dosya isteği

Alan	İçerik
Gönderen adı	Selin Koç
Gönderen adresi	selin@pusulaajans.example
Konu	Yönetici sunumunun son taslağını paylaşabilir misiniz?
Gövde metni	Merhaba Ayşe, sunumun son taslağını inceleyip lansman görsellerini yerleştireceğim. Lütfen Lansman Yönetici Sunumu bağlantısını herkesin erişimine açıp bu iletiye yanıtla.
Doğru yanıt	Sınırdaki/şüpheli; doğrulanmadan paylaşılmamalı
İpuçları	Gönderen alan adı senaryodaki Pusula Ajans ile uyumlu olsa da “herkesin erişimine aç” talebi en az yetki ilkesine aykırı; Selin Koç’u bilinen Chat alanından doğrulayın; yalnızca gerekli dosyayı belirli hesaba, uygun rolle paylaşın.

KVKK kapsamında veri örnekleri

Aşağıdaki tablo 6698 sayılı Kanun'a atıf yapan sade bir eğitim özetidir; hukuki tavsiye değildir.

Veri grubu	Sade açıklama	Workspace örneği	Kullanıcı davranışı
Kişisel veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin bilgi.	Ad-soyad, kurumsal e-posta, telefon, müşteri kaydı, ses veya Meet transkripti.	Amaçla sınırlı toplayın, gerekli kişilerle paylaşın, doğru etiket ve saklama kuralını uygulayın.
Özel nitelikli kişisel veri	Kanunda daha sıkı korumaya tabi tutulan veri grubu.	Sağlık bilgisi, biyometrik veya genetik veri, ceza mahkûmiyeti, siyasi düşünce veya sendika üyeliği bilgisi.	Açık kurum prosedürü ve yetkili KVKK değerlendirmesi olmadan toplamayı, isteme yazmayı veya paylaşmayı durdurun.
Kişisel veri olmayan örnek	Gerçek kişiyle ilişkilendirilemeyen, tek başına kişiyi belirlemeyen genel bilgi.	Ürün lansmanının genel tarih aralığı veya anonimleştirilmiş görev sayısı.	Yeniden belirlenebilirlik riskini kontrol edin; başka ayrıntılarla birleşince kişisel veriye dönüşebileceğini unutmayın.

Kaynaklar

1. Gmail kimlik avı yardımı. <https://support.google.com/mail/answer/8253?hl=tr>
2. Gmail spam bildirimi. <https://support.google.com/mail/answer/1366858?hl=tr&co=GENIE.Platform%3DDesktop>
3. 2 Adımlı Doğrulama. <https://support.google.com/accounts/answer/185839?hl=tr&co=GENIE.Platform%3DDesktop>
4. Geçiş anahtarıyla oturum açma. <https://support.google.com/accounts/answer/13548313?hl=tr>
5. Hesaba erişen cihazlar. <https://support.google.com/accounts/answer/3067630?hl=tr>
6. Üçüncü taraf bağlantılarını yönetme. <https://support.google.com/accounts/answer/13533235?hl=tr>
7. Üçüncü taraf uygulama erişimi. <https://support.google.com/accounts/answer/14012355?hl=tr>
8. Drive paylaşım yönetimi. <https://support.google.com/drive/answer/7166529?hl=tr&co=GENIE.Platform%3DDesktop>
9. Drive paylaşımını sınırlama. <https://support.google.com/drive/answer/2494893?hl=tr&co=GENIE.Platform%3DDesktop>
10. Drive dosya etiketleri. <https://support.google.com/drive/answer/13495216?hl=tr&co=GENIE.Platform%3DDesktop>
11. DLP for Drive. <https://knowledge.workspace.google.com/admin/security/about-dlp-for-drive>
12. Classification labels. <https://knowledge.workspace.google.com/admin/security/create-classification-labels-for-your-organization>
13. Workspace üretken yapay zekâ gizliliği. <https://support.google.com/a/answer/15706919?hl=tr>
14. Gemini Uygulamaları Gizlilik Merkezi. <https://support.google.com/gemini/answer/13594961?hl=tr>
15. Kayıp cihazı kilitleme veya silme. <https://support.google.com/accounts/answer/7177579?hl=tr>
16. Gmail Tümünü yanıtla uyarıları. <https://workspaceupdates.googleblog.com/2026/07/prevent-accidental-disclosures-with-new-Reply-All-BCC-warnings-in-Gmail.html>
17. 6698 sayılı Kanun. <https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law>
18. Özel nitelikli veriler rehberi. <https://www.kvkk.gov.tr/Icerik/8184/Ozel-Nitelikli-Kisisel-Verilerin-Islenmesine-Iliskin-Rehber>