

Kişisel Verileri Koruma Kurumunun 2026/2035 sayılı ilke kararı hakkında

Kişisel Verileri Koruma Kurumu'nca işverenler tarafından çalışanlara tahsis edilen kurumsal e-posta hesapları başta olmak üzere, işin yürütülmesi amacıyla kullanılan iletişim kanallarının denetlenmesinde uyulması gereken usul ve esaslar hakkında 16/09/2026 tarihli ve 2026/2035 sayılı ilke kararı yayımlanmıştır (Ek:1).

Kararda **işverenler tarafından çalışanlara tahsis edilen kurumsal e-posta hesapları** başta olmak üzere, işin yürütülmesi amacıyla kullanılan iletişim kanallarının (WhatsApp Grupları, sosyal medya hesapları ve benzerleri gibi) **denetlenmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyetlerinin** Kişisel Verileri Koruma Kanunu ve ilgili mevzuata uygun şekilde yürütülmesi için aşağıdaki hususların dikkate alınması gerektiği vurgulanmaktadır:

- **Kanun kapsamındaki yükümlülükler:** İşverenin işin gereği yapacağı denetleme faaliyetleri, Kanun'da öngörülen kişisel veri işleme şartlarına ve genel ilkelere tabi olduğu gibi, ilgili durumlarda aydınlatma ve veri güvenliği yükümlülüklerinin de yerine getirilmesini gerektirmektedir. **İletişim aracının (telefon, bilgisayar) işverene ait olması veya işyerinde kullanılması, işverene çalışanların iletişim faaliyetleri üzerinde sınırsız bir denetim yetkisi sağlamamaktadır.**
- **İş amaçlı ve özel amaçlı kullanım ayrımı:** Denetimin kapsamı belirlenirken iletişim aracının hangi amaçla tahsis edildiği ve kullanımına ilişkin kuralların neler olduğu dikkate alınmalıdır. Bu kapsamda **"iş amaçlı kullanım"** ile **"özel amaçlı kullanım"** arasında ayrım yapılması önem taşımaktadır.
- **Özel amaçlı kullanıma ilişkin kurallar:** İşveren, yönetim hakkı kapsamında işyeri iletişim araçlarının özel amaçlı kullanımına ilişkin kuralları belirleyebilir; ancak bu kuralların açık, anlaşılır ve çalışan tarafından bilinebilir olması gerekmektedir. Özel amaçlı kullanımın yasaklandığı durumlarda dahi işverenin denetim yetkisi ölçülülük ilkesiyle sınırlıdır. **İş amaçlı kullanım ile özel amaçlı kullanımın birbirinden kesin olarak ayıramadığı hâllerde ise denetim yetkisinin kapsamı daha dar değerlendirilmelidir.**
- **Teknik erişim yetkisi ile hukuki erişim yetkisinin ayrılması:** İşverenin belirli bir cihaz, oturum, ağ veya kurumsal sistem üzerinde teknik erişim imkanına sahip olması, çalışanın kişisel e-posta hesabı, kişisel anlık mesajlaşma uygulaması, sosyal medya hesabı veya benzeri özel iletişim alanlarında bulunan yazışma içeriklerine serbestçe erişebileceği anlamına gelmemektedir. Bu nedenle teknik olarak erişilebilir olma ile hukuken erişilebilir olma yetkilerinin birbirinden ayrılması gerekmektedir.
- **Önceden bilgilendirme:** Çalışanların gerçekleştirilecek denetim faaliyeti hakkında önceden bilgilendirilmiş olması, denetimin hukuka uygunluğunun tespitinde önem taşıyan unsurlardan biridir.
- **Aydınlatmanın kapsamı:** İşveren tarafından yapılacak aydınlatmada, kişisel veri işleme faaliyetinin hukuki sebebi, amacı, kapsamı ve yöntemi ile iletişim içeriklerine hangi hallerde erişilebileceği, verilerin saklama süresi ve ilgili kişilerin Kanun'un 11'inci maddesi kapsamındaki hakları açık, anlaşılır ve somut biçimde ortaya konulmalıdır.
- **Genel nitelikli bildirimlerin yeterli olmaması:** Çalışanlara, yalnızca kurumsal e-posta hesabının işveren tarafından denetlenebileceğine ilişkin genel bir bildirimde bulunulması, somut olayın özelliklerine göre önceden bilgilendirme bakımından yeterli olmayacağı gibi, Kanun'un 10'uncu maddesi kapsamındaki aydınlatma yükümlülüğünün de yerine getirildiği sonucunu kendiliğinden doğurmayacaktır.

- **Açık rızanın değerlendirilmesi:** İş ilişkisindeki bağımlılık hali ve taraflar arasındaki güç dengesi dikkate alındığında, çalışanın açık rızasının kural olarak e-posta denetimi bakımından her durumda öncelikli hukuki dayanak olarak kabul edilmesi mümkün değildir. Açık rızaya dayanan durumlarda rızanın özgür iradeyle verilip verilmediği somut olayın koşulları çerçevesinde ayrıca değerlendirilmelidir. Bunun yanında, **geçerli bir açık rızanın veya Kanun'da öngörülen diğer bir kişisel veri işleme şartının bulunması da işverene sınırsız bir denetim yetkisi tanımamaktadır.**
- **Genel ilkeler ve ölçülülük:** Denetim faaliyetleri, Kanun'un 4'üncü maddesinde düzenlenen genel ilkelere uygun olarak; hukuka ve dürüstlük kurallarına uygun, belirli, açık ve meşru amaçlarla ve bu amaçla bağlantılı, sınırlı ve ölçülü bir şekilde yürütülmelidir. Elde edilen kişisel veriler, işleme amacı bakımından gerekli olan süreden daha uzun süreyle muhafaza edilmemelidir.
- **Kademeli denetim:** Denetim faaliyetlerinde kademelik esas alınmalıdır. İşverenin ulaşmak istediği meşru amaca daha az müdahaleci bir yöntemle ulaşmasının mümkün olduğu hallerde, daha ağır bir denetim yöntemine başvurulmamalıdır.
- **İçerik denetimi:** Çalışana tahsis edilen e-posta ya da diğer iletişim araçlarında yer alan içeriklerin incelenmesine, kural olarak yalnızca somut şüphe veya belirli bir olayla bağlantılı meşru bir amaç bulunması halinde ve denetimin amacıyla sınırlı olacak şekilde başvurulmalıdır. Kapsamı belirsiz, genel ve sürekli nitelikte içerik incelemelerinden kaçınılması gerekmektedir.
- **Özel nitelikli kişisel veriler ve üçüncü kişilere ait veriler:** İçerik denetiminde, incelenen içerik veya eklerinde Kanun'un 6'ncı maddesi kapsamında özel nitelikli kişisel verilerin (sağlık gibi) bulunabileceği dikkate alınmalıdır. Bunun yanı sıra, çalışanların iletişimleri çoğu zaman iletişimin karşı taraflarına veya başka üçüncü kişilere ait kişisel veri de içerebileceğinden, denetimin bu kişiler bakımından doğurabileceği etkiler de göz önünde bulundurulmalıdır.
- **Erişim yetkilendirmesi ve veri güvenliği:** Kurumsal e-posta hesapları ve işin yürütülmesi amacıyla kullanılan diğer iletişim kanallarından elde edilen verilere erişim, yalnızca bu konuda görev ve yetki verilmiş belli sayıdaki personelle sınırlandırılmalıdır. Erişim yetkileri görev tanımları doğrultusunda belirlenmeli, erişim işlemlerine ilişkin kayıtlar tutulmalı ve verilere erişen kişilerin gizlilik yükümlülükleri güvence altına alınmalıdır.
- **İş ilişkisinin sona ermesi:** İş ilişkisinin sona ermesinden sonra çalışana tahsis edilmiş kurumsal e-posta hesabı ve bu hesap kapsamında elde edilmiş veya tutulmakta olan verilere ilişkin gerçekleştirilen kişisel veri işleme faaliyetlerinin hukuki dayanağı ayrıca değerlendirilmelidir. İş ilişkisinin sona ermesi, söz konusu verilerin süresiz olarak erişilebilir veya işlenebilir olduğu anlamına gelmemektedir.

Yukarıda belirtilen hususların ve ekli ilke kararının ivedilikle değerlendirilerek gerekli uyumun sağlanması, geçmiş dönem verilerin taranarak ilke kararına belirtilen hususları taşımayan bilgilerin **derhal silinmesi önem arz etmektedir.**

Saygılarımızla.

Beta Yeminli Mali Müşavirlik Ltd. Şti.

KURUL KARARI**Kişisel Verileri Koruma Kurumundan:****İşverenler Tarafından Çalışanlara Tahsis Edilen Kurumsal E-Posta Hesapları Başta Olmak Üzere, İşin Yürütülmesi Amacıyla Kullanılan İletişim Kanallarının Denetlenmesi Suretiyle Gerçekleştirilen Kişisel Veri İşleme Faaliyetlerinde Uyulması Gereken Usul ve Esaslar Hakkında İlke Kararı****Karar No: 2026/2035****Karar Tarihi: 16/09/2026**

Bilindiği üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (6698 sayılı Kanun) 15'inci maddesinin altıncı fıkrası "*Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi hâlinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar...*" hükmünü amirdir. Öte yandan 6698 sayılı Kanun'un Kişisel Verileri Koruma Kurulunun (Kurul) görev ve yetkilerini düzenleyen 22'nci maddesinin birinci fıkrasının (e), (f) ve (g) bentlerinde sırasıyla Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda, veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla ve veri sorumlusu ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapma yetkisi düzenlenmiştir.

Bu çerçevede, işverenler tarafından çalışanlara tahsis edilen kurumsal e-posta hesapları başta olmak üzere, işin yürütülmesi amacıyla kullanılan iletişim kanallarının denetlenmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyetlerine ilişkin olarak Kurul tarafından aşağıdaki tespit ve değerlendirmelerde bulunulmuştur.

Çalışanlara tahsis edilen kurumsal e-posta hesabı, bir iletişim aracının ötesinde; çalışanın mesleki ve zaman zaman kişisel ilişki ağını, çalışma örüntüsünü ve yazışma içeriklerini barındıran bir veri kaynağı niteliği taşımaktadır. Bu hesapların işveren tarafından denetlenmesi, işverenin yönetim hakkı ile çalışanın Anayasa'nın 20 ve 22'nci maddelerinde güvence altına alınan kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti arasındaki dengenin gözetilmesini gerektiren bir kişisel veri işleme faaliyetidir. Diğer taraftan, işyerinde kullanılan iletişim kanalları yalnızca kurumsal e-posta hesaplarından ibaret değildir. Kurum içi mesajlaşma uygulamaları, kurumsal anlık iletişim hesapları, müşteri ilişkileri veya talep yönetim sistemleri, toplantı platformlarındaki sohbet ve kayıt alanları da somut olayın özelliklerine göre denetime konu olabilecek iletişim kanalları arasında yer almaktadır. Öte yandan, kişisel kullanıma da elverişli uygulamalar bakımından, söz konusu hesabın işveren tarafından iş amacıyla tahsis edilip edilmediği, çalışanın kişisel hesabı üzerinden kullanılıp kullanılmadığı ve çalışanın makul mahremiyet beklentisi ayrıca değerlendirilmelidir.

İşverenin, çalışanına ait e-postanın içeriğine erişmeksizin yalnızca trafik/log kayıtlarını işlemesi dahi başlı başına bir kişisel veri işleme faaliyetini oluşturmaktadır. Bu itibarla e-posta denetimi gerek trafik verisine gerek içeriğe yönelik olsun, 6698 sayılı Kanun'un 4'üncü maddesindeki genel ilkelere, 5'inci ve 6'ncı maddelerindeki işleme şartlarına, 10'uncu maddesindeki aydınlatma yükümlülüğüne ve 12'nci maddesindeki veri güvenliğine ilişkin yükümlülüklerle tabidir.

İletişim araçlarının işverene ait olması ya da işyerinde bulunması, tek başına işverene sınırsız ve mutlak bir denetim yetkisi tanımamaktadır. Nitekim gerek Anayasa Mahkemesinin gerek Avrupa İnsan Hakları Mahkemesinin konuya ilişkin kararlarında; işverenin denetim yetkisinin, çalışanın önceden açık biçimde bilgilendirilmesi, denetimin meşru bir amaca dayanması, amaçla sınırlı ve ölçülü olması ile daha az müdahaleci yolların önceliği ölçütlerine bağlandığı; içeriğin denetlenmesinin ise trafik verisi denetimine kıyasla daha ağır bir gerekçe gerektirdiği ortaya konulmuştur.

Bu çerçevede, işverenler tarafından çalışanlara tahsis edilen kurumsal e-posta hesapları başta olmak üzere, işin yürütülmesi amacıyla kullanılan iletişim kanallarının denetlenmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyetlerinde;

1. Kurumsal e-posta hesaplarının denetlenmesinin, içeriğe erişilmeksizin yalnızca trafik/log kayıtlarının işlenmesi hâlinde dahi başlı başına bir kişisel veri işleme faaliyeti oluşturduğu ve her hâlikârda 6698 sayılı Kanun'un işleme şartlarına, genel ilkelerine, aydınlatma ve veri güvenliği yükümlülüklerine tabi olduğu; iletişim araçlarının işverene ait olmasının veya işyerinde kullanılmasının işverene sınırsız bir denetim yetkisi tanımadığı,
2. Denetim faaliyetinin kapsamı belirlenirken, işyeri iletişim araçlarının kullanım amacına göre "iş amaçlı kullanım" ve "özel amaçlı kullanım" ayrımının dikkate alınması gerektiği; işveren tarafından özel amaçlı kullanımın yasaklanmış, belirli sınırlar içinde serbest bırakılmış veya bu konuda açık bir düzenleme yapılmamış olmasının denetimin hukuka uygunluk değerlendirmesinde farklı sonuçlar doğurabileceği,
3. İşverenin yönetim hakkı kapsamında işyeri iletişim araçlarının özel amaçlı kullanımına ilişkin kurallar belirleyebileceği; ancak bu kuralların açık, anlaşılır ve çalışan tarafından bilinebilir nitelikte olması gerektiği; özel amaçlı kullanımın yasaklanması, sınırlandırılması veya belirli zaman, kapsam ve yöntem koşullarına bağlanması halinde bu hususun çalışanı açıkça duyurulması gerektiği; özel amaçlı kullanımın yasaklanmış olduğu hallerde dahi işverenin denetim yetkisinin ölçülülük ilkesiyle sınırlı olduğu; denetimin sürekli ve aralıksız gözetim şeklinde yürütülmesinin ölçülü kabul edilemeyeceği; özel kullanım yasağının ihlal edildiği içerik dışı unsurlardan anlaşılabiliriyorsa, yazışma içeriğine ayrıca erişilmesinin gerekli ve orantılı kabul edilemeyeceği; özel amaçlı kullanıma izin verilen hallerde, iş amaçlı iletişim ile özel amaçlı iletişimin birbirinden ayrılabilir olması durumunda denetimin yalnızca iş amaçlı iletişimle sınırlı tutulması; çalışanın özel nitelikteki yazışmalarının denetim dışında bırakılması gerektiği; iş amaçlı kullanım ile özel amaçlı kullanımın birbirinden ayrılmadığı hâllerde ise işverenin denetim yetkisinin daha dar yorumlanması gerektiği,
4. İşverenin belirli bir cihaz, oturma, ağ ya da kurumsal sistem üzerinde teknik yetkiye sahip olmasının, çalışanın kişisel e-posta hesabı, kişisel anlık mesajlaşma uygulaması, sosyal

medya mesaj kutusu veya benzeri özel iletişim alanlarında yer alan yazışma içeriklerine serbestçe erişebileceği anlamına gelmediği; bu nedenle teknik erişim imkânı ile hukuki erişim yetkisinin birbirinden ayrılması gerektiği,

5. Denetimin hukuka uygunluğunun değerlendirilmesinde, çalışanın denetim faaliyeti hakkında önceden bilgilendirilmiş olmasının belirleyici unsurlardan biri olduğu; bununla birlikte, Anayasa Mahkemesi içtihadında aranan bilgilendirme ile 6698 sayılı Kanun'un 10'uncu maddesinde düzenlenen aydınlatma yükümlülüğünün birebir aynı kavramlar olmadığı; her bilgilendirmenin 6698 sayılı Kanun anlamında aydınlatma sayılamayabileceği, ancak 6698 sayılı Kanun'un 10'uncu maddesinde öngörülen unsurları taşıyan ve denetim faaliyetinin amacı, kapsamı ve yöntemi hakkında açık bilgi içeren usulüne uygun bir aydınlatmanın, çalışanın denetim konusunda önceden bilgilendirilmesi şartını da karşılayabileceği,

6. İşveren tarafından yapılacak aydınlatmanın, soyut ve genel bir ifadenin ötesine geçerek; kişisel veri işleme faaliyetinin hukuki sebebini, amacını, kapsamını, denetimin trafik/log kayıtlarının incelenmesiyle mi yoksa içerik denetimiyle mi yürütüleceğini, içeriğe hangi hallerde erişilebileceğini, verilerin saklama süresini ve ilgili kişinin 6698 sayılı Kanun'un 11'inci maddesi kapsamındaki haklarını açık, anlaşılır ve somut biçimde içermesi gerektiği,

7. Çalışanın denetim faaliyeti hakkında önceden bilgilendirilmediği ve 6698 sayılı Kanun'un 10'uncu maddesine uygun şekilde aydınlatılmadığı hallerde, kişisel verilerine ve haberleşme hürriyetine müdahale edilmeyeceği yönünde makul bir beklenti taşıyacağının gözetilmesi gerektiği; yalnızca kurumsal e-posta hesabının işveren tarafından denetlenebileceği şeklindeki genel nitelikli bildirimlerin "bilgilendirme" koşulunu sağlamayacağı ve 6698 sayılı Kanun'un 10'uncu maddesi kapsamında aydınlatma yükümlülüğünün yerine getirildiği sonucunu doğurmayacağı,

8. İş ilişkisindeki bağımlılık ve taraflar arasındaki güç dengesizliği dikkate alındığında, çalışanın açık rızasının kural olarak e-posta denetimi bakımından kural olarak öncelikli hukuki dayanak olarak esas alınmaması gerektiği; açık rızaya dayanan hallerde ise rızanın özgür iradeyle açıklanıp açıklanmadığının somut olay özelinde ayrıca değerlendirilmesi gerektiği; denetim kapsamında gerçekleştirilen kişisel veri işleme faaliyetlerinin, somut olayın koşullarına göre 6698 sayılı Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan "*veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması*" (e) bendinde yer alan "*bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması*" ve (f) bendinde yer alan "*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlemenin zorunlu olması*" işleme şartlarına dayandırılabilmesi; ancak söz konusu işleme şartlarının varlığının, işverene sınırsız bir denetim yetkisi tanımayacağı,

9. Denetimin, 6698 sayılı Kanun'un 4'üncü maddesindeki genel ilkelere uygun olarak; hukuka ve dürüstlük kurallarına uygun, belirli, açık ve meşru bir amaca dayalı, bu amaçla bağlantılı, sınırlı ve ölçülü biçimde yürütülmesi ve elde edilen verilerin yalnızca amacın gerektirdiği süreyle muhafaza edilmesi gerektiği,

10. Denetimde kademeliliğin esas olduğu; işverenin ulaşmak istediği meşru amaca daha az müdahaleci bir yolla ulaşabildiği hallerde daha ağır denetim yöntemine başvurmayacağı;

içeriğe erişimin ancak trafik verisi denetiminin yetersiz kaldığı ve içeriğe erişimin zorunlu olduğu istisnai hallerde gündeme gelebileceği; çalışana iş faaliyeti kapsamında tahsis edilen iletişim araçlarının kötüye kullanımının teknik yollarla (filtreleme, engelleme vb.) önlenemediği hallerde işverenin genel bir denetim hakkının doğmayacağı,

11. İçeriğin denetlenmesinin, çalışanın özel hayatına ve haberleşme hürriyetine yönelen en yoğun müdahaleyi oluşturması nedeniyle daha güçlü ve somut bir meşru gerekçe gerektirdiği; içerik denetimine yalnızca somut şüphe bulunan hallerde ve iddiayla sınırlı olacak biçimde başvurulması, kapsamı belirsiz, genel ve süreklilik arz eden içerik incelemesinden kaçınılması gerektiği,

12. İçerik denetiminde, denetime tabi tutulan iletinin gövdesinde veya eklerinde 6698 sayılı Kanun'un 6'ncı maddesi anlamında özel nitelikli kişisel verilerin işlenmesi riskinin gözetilmesi; ayrıca yazışmaların çoğu kez muhataplara ait kişisel verileri de barındırması nedeniyle, denetimin üçüncü kişilerin verileri üzerinde doğuracağı etkinin de dikkate alınması gerektiği,

13. Çalışanın önceden bilgilendirilmediği gizli izleme yöntemleri ile çalışanın tüm işlemlerini ayırım gözetmeksizin kaydeden araçlar aracılığıyla yürütülen denetimin hukuka aykırı sayılacağı; denetimin, çalışanın bilgisi dâhilinde ve öngörülebilir bir çerçevede yürütülmesi gerektiği,

14. Kurumsal e-posta hesapları ve işin yürütülmesi amacıyla kullanılan iletişim kanalları üzerindeki elde edilen verilere erişimin, yalnızca bu görevle yetkilendirilmiş sınırlı bir personelle sınırlandırılması, erişim yetkisinin görev tanımlarıyla belirlenmesi, erişim kayıtlarının tutulması ve verilere erişen kişilerin gizlilik yükümlülüğü altına alınması gerektiği,

15. İş ilişkisinin sona ermesinin ardından, çalışana tahsis edilmiş kurumsal e-posta hesabına ilişkin veri işleme faaliyetlerinin hukuki dayanağının ayrıca değerlendirilmesi gerektiği; kural olarak ilgili hesabın çalışanın aktif kullanımına ve hesaba yeni erişimlere kapatılması, hesaba gelen iletilerin ilgisiz kişilerce görüntülenmesine imkân verilmemesi ve hukuki dayanağı kalmayan kişisel verilerin imha edilmesi gerektiği; bununla birlikte iş sürekliliğinin sağlanması, kurumsal iletişimin aksamaması, hukuki uyumsuzluklarda savunma hakkının kullanılabilmesi veya ilgili mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesi amacıyla, kurumsal e-posta hesabına ilişkin sınırlı, süreli, erişim yetkileri belirlenmiş ve kayıt altına alınmış yönlendirme, otomatik cevap, arşivleme veya muhafaza uygulamalarının somut olayın koşullarına göre değerlendirilebileceği,

16. Söz konusu yükümlülüklerle uyulmadığının tespiti halinde, somut olayın özellikleri dikkate alınarak gerekli incelemenin yapılacağı ve 6698 sayılı Kanun'un 18'inci maddesi uyarınca ilgili veri sorumluları hakkında idari işlem tesis edileceği

hususlarında kamuoyunun bilgilendirilmesine ve bu kapsamda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 15'inci maddesinin altıncı fıkrası hükmü uyarınca İlke Kararı alınmasına ve bu İlke Kararı'nın Resmi Gazete'de ve Kurumun internet sitesinde yayımlanmasına oy çokluğu ile karar verilmiştir.