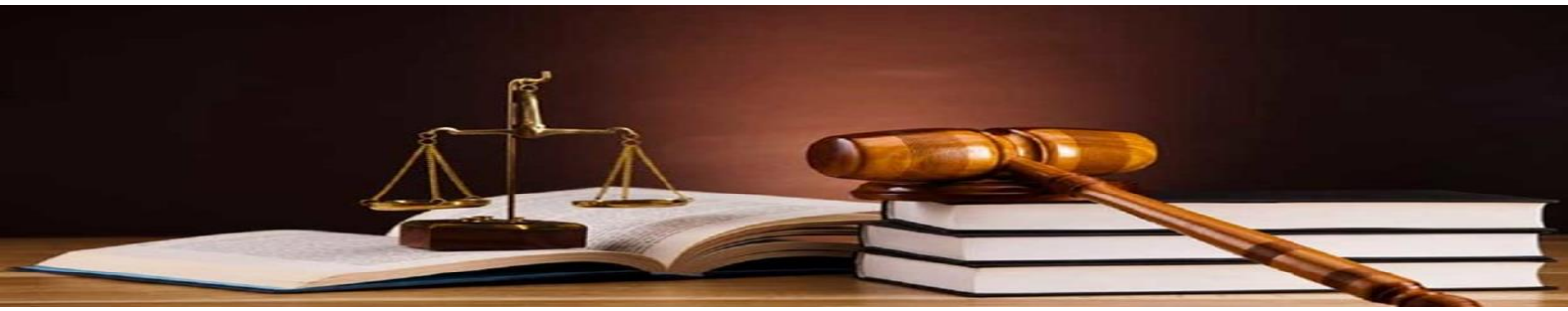
ÜREYHUKUK



PERSONEL DEVAM TAKİP SİSTEMLERİ VE KİŞİSEL VERİLERİN İŞLENMESİ

Tarih: 07.07.2023
Yazarlar: Sema Çelebi, Beyza Somuncu.

Kişisel Verileri Koruma Kurumu("***Kurum***") ve Yüksek Mahkemeler tarafından tesis edilen güncel tarihli kararlara istinaden, şirketlerimiz bünyesinde istihdam edilmiş olan personellerin, Personel Devam Kontrol Sistemleri aracılığı ile işe giriş çıkış, devamsızlık ve sair durumlarının takibinin yapılması noktasında özellikle kişisel verilerin alınması, işlenmesi, muhafaza ve imha edilmesi gibi çeşitli aşamalarda dikkat edilmesi gereken hususları ihtiva eden bilgi notumuzu bilgilerinize sunarız.

1. Personel Devam Kontrol Sistemleri

Bilindiği üzere işyerlerinde, istihdam edilen personellerin işe giriş çıkış saatleri, molaları, izinleri ve buna benzer çeşitli durumlarının takip edilmesi amacıyla Personel Devam Kontrol Sistemleri'nden ("***PDKS***") yararlanılmaktadır. Söz konusu PKDS kapsamında kartlı geçiş, yüz tanıma ya da parmak izi gibi biyometrik verilerin alınması suretiyle geçiş ve/veya mobil uygulamaların kullanılması suretiyle geçiş gibi birden çok sistem kullanılmaktadır. Bu noktada özellikle biyometrik verilerin alınması suretiyle geçiş sistemlerinin kullanıldığı işyerlerinde, hangi verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu("***KVKK***") uyarınca kişisel veri olarak kabul edildiğinin ve bu verilerin alınması, işlenmesi, paylaşılması, muhafaza ve imha edilmesi gibi çeşitli hususlarda nelere dikkat edilmesi gerektiğinin bilinmesi önem arz etmektedir. Nitekim aksi halde işverenler çeşitli yaptırımlarla karşı karşıya kalabilmektedir.

2. Kişisel Verileri Koruma Kanunu ve Özel Nitelikli Kişisel Veriler

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini koruma ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenleme amacı taşıyan KVKK uyarınca; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, kişisel veri olarak isimlendirilmektedir ve bu veriler yalnızca Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilmektedir. Söz konusu verilerin işlenmesinde dikkat edilmesi gereken hususlara KVKK'da yer verilmiş olup bu kapsamda; **i)** Hukuka ve dürüstlük kurallarına uygun olma, **ii)** Doğru ve gerektiğinde güncel olma, **iii)** Belirli, açık ve meşru amaçlar için işlenme, **iv)**

İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, **v)** İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme koşullarının her olayda mevcut olması gerekmektedir. Bu noktada önemle vurgulamak isteriz ki, kişisel verilerin işlenmesi yalnızca ilgili kişinin bilgilendirilmesi/aydınlatılması ve neticede açık rızasının alınmış olması halinde mümkün olabilmektedir.

Belirtmek isteriz ki kanun koyucu, kişilerin biyometrik ve genetik verilerine özel bir önem atfetmekte ve bu kapsamda söz konusu verileri özel nitelikli kişisel veri olarak isimlendirmektedir. Adından da anlaşılacağı üzere özel nitelikli kişisel verilerin işlenmesinde birtakım özel ve ek tedbirler öngörülmüş olup bu kapsamda söz konusu verilerin işlenmesinde Kişisel Verileri Koruma Kurulu("***Kurul***") tarafından belirlenen yeterli önlemlerin de alınmış olması gerekmektedir.

Gelinen aşamada öncelikle hangi verilerin biyometrik ve genetik veri niteliği taşıdığına ilişkin bir açıklama yapılmasında fayda görüyoruz. Şöyle ki, Avrupa Birliği Resmi Gazetesi'nde yayımlanan Avrupa Birliği Genel Veri Koruma Tüzüğü'nün("***Tüzük***") 4. maddesi uyarınca genetik veri; bir gerçek kişinin fizyoloji veya sağlığı ile ilgili eşsiz bilgiler sağlayan ve özellikle söz konusu gerçek kişiden alınan bir biyolojik numunenin analizinden kaynaklanan ve söz konusu kişinin kalıtım yoluyla alınan veya kazanılan özelliklerine ilişkin kişisel verilerini ifade ederken; biyometrik veri ise yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerini ifade etmektedir. Bu noktada kişinin kan grubu ve tükürük numunesi genetik verilerine; parmak izi, el şekli, avuç içi, retinası ve irisi ise biyometrik verilerine örnek olarak gösterilebilmektedir.

3. İşyerlerinde Kişisel Verilerin Alınması Suretiyle Denetim Yapılması ve Bu Verilerin İşlenmesi Hususunda Dikkat Edilmesi Gerekenler

Öncelikle, işyerlerindeki PKDS'lerde sıklıkla kullanılan parmak izi ve yüz tanıma gibi biyometrik veri kullanılan kimlik doğrulama altyapılarının ilgili kurum ve kuruluşlar tarafından yapılan denetimlerde mercek altında tutulduğunun bilinmesi bir önem arz etmektedir. Nitekim bu tarz altyapıların kullanılması ile özel nitelikli kişisel veri olarak isimlendirilen veriler toplandığından işverenlere birtakım ek yükümlülükler de getirilmiş bulunmaktadır. Bu noktada çalışanların mesaiye devamlarını, izinlerini, mola sürelerini ve sair durumlarını kontrol etmek amacıyla işyerine girişlerinde parmak izi alınması, yüz tanıma sistemlerinin kullanılması gibi alt yapılardan yararlanılması halinde, özel hayatın gizliliği ilkesine uygun şekilde hareket edildiğinden emin olunması gerekmektedir. Ek olarak belirtmemiz gerekirse, söz konusu altyapıların kullanıldığı işyerleri kamusal alanda da olsa, bu işyerleri yine de özel hayatın gizliliği ilkesi kapsamında bulunmaktadır.

Konuyla ilgili olarak Anayasamızın "*Özel hayatın gizliliği*" kenar başlıklı 20 inci maddesinde, herkesin **i)** Özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu ve **ii)** Özel hayatın ve aile hayatının gizliliğine dokunulamayacağı hüküm altına alınmış; hükmün devamında herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın; **i)** Kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, **ii)** Bu verilere erişme, **iii)** Bunların düzeltilmesini veya silinmesini talep etme ve **iv)** Amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı belirtilmiş ve kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği düzenlenmiştir. Açık rıza deyiminden ne anlaşılması gerektiği ise KVKK'nın "*Tanımlar*" kenar başlıklı 3 üncü maddesinde düzenlenmiştir. Anılan düzenlemeye göre açık rıza, belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade etmektedir.

Kurum tarafından yayımlanmış olan Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber("***Rehber***") uyarınca biyometrik veriler, KVKK'nun 4 üncü maddesinde yer alan genel ilkelere ve 6 ncı maddesinde düzenlenen şartlara uygun olarak yalnızca aşağıda yer alan ilkeler doğrultusunda işlenebilmektedir. Bu ilkeler ise şunlardır:

- **i)** Temel hak ve özgürlüklerin özüne dokunulmaması,
- **ii)** Başvurulan yöntemin işleme amacına ulaşılabilmesi bakımından elverişli olması ve veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması,
- **iii)** Biyometrik veri işleme yönteminin ulaşılmak istenen amaç bakımından gerekli olması
- **iv)** Veri işlemeyle ulaşılmak istenilen amaç ve aracın arasında orantı bulunması
- **v)** Verilerin gerektiği süre kadar tutulması, gereklilik ortadan kalktıktan gecikmeksizin imha edilmesi,
- **vi)** İşleme amacı ile sınırlı olmak üzere; veri sorumlularının Kanunun 10 uncu maddesine uygun bir biçimde aydınlatma yükümlülüğünü yerine getirmesi
- **vii)** Açık rızanın gerekmesi halinde ilgili kişilerin açık rızalarının Kanuna uygun şekilde alınmış olması

Tüm bu hususlara ek olarak;

- **i)** Yukarıda yer verilmiş olan ilkelerin tümünün gereklerinin yerine getirildiği hususu kayıt altına alınıp belgelendirilmeli,
- **ii)** Gerekmediği takdirde, biyometrik veri alınırken genetik veri (*kan, tükürük vb.)* alınmamalı,
- **iii)** Biyometri türünün veya türlerinin seçiminde (*iris, parmak izi, elin damar ağı, vb*.) tercih edilen biyometrik veri türünün veya türlerinin diğerleri yerine neden seçildiğine dair gerekçeler ve belgeler sunulmalı,
- **i)** Kişisel verilerin işlenmesinde azami süre belirlenmeli ve biyometrik özelliğin bütün çeşitleri (*ham ve türetilmiş vb. kayıtlar*) gereken süre boyunca işlenmeli; söz konusu verilerin ne kadar süre boyunca tutulacağı nedenleri ile birlikte açıklanmalıdır.

4. Alınması Gereken Teknik ve İdari Tedbirler

Verilerin niteliği ve veri işlemenin ilgili kişi açısından oluşturacağı muhtemel risklerle ilgili olarak, verilerin güvenliğini sağlamak amacıyla birtakım teknik ve idari tedbirlerin alınması gerekmektedir. Bu noktada teknik tedbirlere örnek olarak;

- **i)** Biyometrik veriler bulut sistemlerinde ancak kriptografik yöntemler kullanılarak muhafaza edilmelidir.
- **ii)** Türetilmiş biyometrik veriler, orijinal biyometrik özelliğin yeniden elde edilmesine izin vermeyecek biçimde saklanmalıdır.
- **iii)** Biyometrik veriler ve şablonları güncel teknolojiye uygun olarak, yeterli güvenliği sağlayacak kriptografik yöntemlerle şifrelenmelidir. Şifreleme ve anahtar yönetimi politikası açıkça tanımlanmalıdır.
- **iv)** Veri sorumlusu sistemi kurmadan önce ve herhangi bir değişiklikten sonra, oluşturulacak test ortamlarında sentetik veriler(*gerçek olmayan*) aracılığıyla sistemi test etmelidir.
- **v)** Veri sorumlusu, test amaçlı olarak yapacağı çalışmalarda biyometrik verilerin kullanımını gerekli olanla sınırlamalıdır. Tüm veriler en geç testlerin sonunda silinmelidir.
- **vi)** Veri sorumlusu, sisteme yetkisiz erişilmesi durumunda sistem yöneticisini ikaz eden ve/veya biyometrik verileri silen ve rapor veren önlemler uygulamalıdır.
- **vii)** Veri sorumlusu sistemde sertifikalı teçhizat, lisanslı ve güncel yazılımlar kullanmalı, öncelikli olarak açık kaynak kodlu yazılımları tercih etmeli ve sistemdeki gerekli güncellemeleri zamanında yapmalıdır.
- **viii)** Biyometrik veriyi işleyen cihazların kullanım ömrü izlenebilir olmalıdır.

ix) Veri sorumlusu biyometrik veriyi işleyen yazılım üzerindeki kullanıcı işlemlerini izleyebilmeli ve sınırlayabilmelidir.

x) Biyometrik veri sisteminin donanımsal ve yazılımsal testleri periyodik olarak yapılmalıdır.

İdari Tedbirlere örnek olarak;

i) Biyometrik çözümü kullanamayan(*biyometrik verilerin kaydedilmesi veya okunması imkansız, kullanımı zorlaştıran engel durumu vb*.) veya kullanmaya açık rızası olmayan ilgili kişiler için herhangi bir kısıtlama veya ek maliyet olmaksızın alternatif bir sistem sağlanmalıdır.

ii) Biyometrik yöntemlerle kimlik doğrulamanın yapılamaması ya da başarısızlığı durumunda gerçekleştirilecek bir eylem planı oluşturulmalıdır (*bir kimliği doğrulayamama, güvenli bir alana girme yetkisi eksikliği, vb.*)

iii) Yetkili kişilerin biyometrik veri sistemlerine erişim mekanizması kurulmalı, yönetilmeli ve sorumluları belirlenerek belgelendirilmelidir.

iv) Biyometrik veri işleme sürecinde yer alan personel biyometrik verilerin işlenmesi hususunda özel eğitimler almalı ve söz konusu eğitimler belgelendirilmelidir.

v) Çalışanların sistem ve servislerdeki muhtemel güvenlik zafiyetleri ve söz konusu zafiyetler sonucu oluşabilecek tehditleri bildirebilmesi için resmi bir raporlama prosedürü oluşturulmalıdır.

vi) Veri sorumlusu bir veri ihlali durumunda uygulanmak üzere acil durum prosedürü oluşturmalı ve ilgili herkese duyurmalıdır.

5. Yaptırımlar

Son olarak, mevzuattaki düzenlemelere aykırı hareket edilmesi halinde çeşitli yaptırımların öngörülmüş olduğuna dikkat çekmekte fayda görüyoruz. Şöyle ki;

5237 sayılı Türk Ceza Kanunu'nun 135 ile 140. maddeleri arasında yer alan düzenlemeler uyarınca kişisel verilerin hukuka aykırı olarak kaydedilmesi, bir başkasına verilmesi, yayılması, ele geçirilmesi, kanunların belirlediği süreler geçmiş olmasına rağmen verilerin imha edilmemesi ve sair hallerde suçu işleyen gerçek kişiler hapis cezası yaptırımına tabi tutulmakta ve tüzel kişiler hakkında da güvenlik tedbirleri uygulanmaktadır.

KVKK'nın "*Kabahatler*" kenar başlıklı 18 inci maddesinde ise**;** ilgililerin **i)** Aydınlatma yükümlülüğünün gereklerini yerine getirmemeleri halinde 5.000,00-TL'den 100.000,00-TL'ye kadar, **ii)** Veri güvenliğine ilişkin yükümlülüklerin gereğini yerine getirmemeleri halinde 15.000,00-TL'den 1.000.000,00-TL'ye kadar, **iii)** Kurul tarafından verilen kararları yerine getirmemeleri halinde ise 25.000,00-TL'den 1.000.000,00-TL'ye kadar idari para cezası yaptırımına tabi tutulacağı düzenlenmiş ve bahsi geçen idari para cezasının hem gerçek kişiler hem de özel hukuk tüzel kişileri bakımından uygulanacağı hüküm altına alınmıştır.

SONUÇ OLARAK;

PKDS altyapılarının kullanılması ile personellerin işe giriş çıkış, devamsızlık ve sair durumlarının takibinde, özellikle parmak izi tarama, yüz tanıma ve sair nitelikli sistemlerin kullanılması halinde niteliği itibari ile özel nitelikli kişisel veri olan veriler toplandığından özel hayatın gizliliği ilkesinin gereklerine ve işbu bilgi notumuzda detaylı olarak yer vermiş olduğumuz kanuni düzenlemelere son derece dikkat edilmesi gerekmektedir. Bu noktada Şirketlerimizdeki mesai takiplerinde parmak izi ve yüz tanıma gibi sair verileri işlemekten olabildiğince kaçınılması ve personelin biyometrik verilerini işlemeyen kart okuma suretiyle giriş sistemi gibi alternatif altyapılardan faydalanılması önerilmektedir.

Kişisel verilerin kullanıldığı PKDS sistemlerinden yararlanılması halinde ise; olabildiğince temel hak ve özgürlüklerin özüne dokunulmamalı, veri işleme faaliyetinin ulaşılmak istenen amaca uygun ve elverişli olması ve amaçla orantılı olması sağlanmalı, aynı amacın gerçekleşmesine imkân tanıyan birden fazla aracın olması halinde bunlardan en az müdahaleci olan seçilmeli, elde edilen veriler belirlenmiş olan süre boyunca muhafaza edilmeli ve süre sonunda gecikmeksizin imha edilmeli, veri sahipleri mevzuatta öngörüldüğü şekilde aydınlatılmalı, açık rızanın arandığı hallerde verinin işlenmesinden önce ilgili kişilerin belirli bir konuya ve sonuçlarına ilişkin ve o konu ve sonuçları ile sınırlı olarak açık rızaları alınmış olmalı ve bu koşulların tümü yerine getirildiğinde bu husus kayıt altına alınarak belgelendirilmelidir. Kanaatimizce tüm bu hususlara gerekli ve yeterli dikkat ve özenin gösterilmesi halinde şirketlerimizin muhatap gösterileceği muhtemel şikayet ve yaptırımların önüne geçilebilecektir.

ÜREYHUKUK

İsmail Paşa Sok. No: 77
34718 Koşuyolu, Kadıköy/İstanbul
Tel : +90 0216 327 27 00 pbx
Faks : +90 0216 327 27 44
https://www.urey.av.tr

Bu bilgi notu ve varsa ekleri, sadece bilgilendirme amacıyla tarafınızla paylaşılmıştır. Bu bilgi notu, uygun yasal tavsiye olmaksızın herhangi bir özel durumda veya somut olayda uygulanmamalıdır. Bu bilgi notu, diğer internet adreslerinin linklerini içerebilir, ÜreyhukuK kendisine ait olmayan web sitelerinden hiçbir şekilde sorumlu değildir ve herhangi bir web sitesi ile ilgili bilgileri, içeriği, sunumu veya doğruluğu onaylamaz, açık veya zımni herhangi bir garanti vermez. Bu bilgi notunun telif hakları ÜreyhukuK'a ait olup işbu bilgi notu ÜreyhukuK'un önceden yazılı izni olmaksızın çoğaltılamaz, çevrilemez ve değiştirilemez.