Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber

NAZALI
Tax & Legal

Biyometrik veri işleme hususlarının açıklığa kavuşturulabilmesi için 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("**Kanun**") 6'ncı maddesinde özel nitelikli kişisel veri olarak sayılan biyometrik verilerin işlenmesinde göz önünde bulundurulması gereken hususlara ilişkin olarak hazırlanan Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber İlke Kararı (**"Rehber"**), Kişisel Verileri Koruma Kurumu (**"Kurum"**) tarafından 16 Eylül 2021 tarihinde kamuoyu ile paylaşılmıştır.

1- Biyometrik Verinin Tanımı

Kanun çerçevesinde özel nitelikli kişisel veriler arasında sayılan biyometrik verinin bugüne kadar yayımlanmış mevzuatta kapsamlı olarak tanımlanmamış olduğu Rehber'de belirtilmiş olup, Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ve Kanun'un kabulü öncesi bazı yargı kararlarında yer alan biyometrik veri tanımlarından hareketle 'biyometri' ile insana ait fiziksel veya davranışsal özelliklerin ifade edildiği ve biyometrik verilerin kişiye özgü, benzersiz ve tek olduğu açıklanmıştır. Bu doğrultuda biyometrik veriler, kişilerin unutmasının mümkün olmadığı, genelde ömür boyu değişmeyen ve herhangi bir müdahaleye gerek olmaksızın zahmetsiz şekilde sahip olunan veriler şeklinde tanımlanmış ve biyometrik verilerin kullanılması sayesinde kişilerin birbirlerinden ayırt edilmelerinin çok kolay hale geldiği ve birbirleriyle karıştırılma ihtimallerinin neredeyse ortadan kalktığı belirtilmiştir.

Biyometrik verilerin türleri bakımından ise fizyolojik nitelikli biyometrik veriler ve davranışsal nitelikli biyometrik veriler olmak üzere ikili bir ayrıma gidilmiştir. Bu kapsamda kişinin parmak izi, retinası, avuç içi, el şekli, irisi gibi biyometrik verilerinin fizyolojik nitelikli biyometrik verileri oluşturduğu ve kişinin yürüyüş biçimi, klavyeye basış biçimi, araba sürüş biçimi gibi biyometrik verileri ise davranışsal nitelikli biyometrik verileri oluşturduğu ortaya konmuştur.

2- Biyometrik Verinin İşlenmesi

Kanun'un 6'ncı maddesinin (3) numaralı fıkrası ile sağlık ve cinsel hayat dışındaki kişisel verilerin kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebileceği düzenlenmiş olduğundan, biyometrik verilerin ilgili kişinin açık rızası bulunmasa dahi kanunlarda öngörülen hallerde işlenebileceği Rehber'de ifade edilmiştir. Öte yandan, biyometrik verilerin işlenmesinde her zaman Kanun'un 4'üncü maddesinde düzenlenen genel ilkelere uyulması gerektiğinin altı çizilmiştir. Bu bakımdan, biyometrik verilerin hukuka uygun olarak işlenip işlenmediği hususunda Kanun'da öngörülen şartların mevcudiyetinin yanı sıra somut olay çerçevesinde yorum yapılmasının da önem arz ettiği Rehber kapsamında ifade edilmiştir.

3- Biyometrik Veri İşleme İlkeleri

Rehber uyarınca veri sorumluları tarafından biyometrik veriler Kanun'un 4'üncü maddesinde yer alan genel ilkelere ve 6'ncı maddesinde düzenlenen şartlara uygun bir şekilde, ancak aşağıda yer alan ilkeler doğrultusunda işlenebilecektir:

» **Temel hak ve özgürlüklerin özüne dokunmaması:** Biyometrik veri işleme faaliyetlerinin Türkiye Cumhuriyeti Anayasası'nda öngörülen temel hak ve özgürlükler bakımından temel güvencelere tabi olması gerektiği açıktır ve bu noktada ölçülülük hususu büyük önem arz etmektedir.

» **Başvurulan yöntemin işleme amacına ulaşılabilmesi bakımından elverişli olması, veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması:** Biyometrik veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması gerekmekte olup, aracın yardımıyla istenilen neticeye yaklaşılabiliyor ise o aracın elverişli olduğu kabul edilebilecektir.

» **Biyometrik veri işleme yönteminin ulaşılmak istenen amaç bakımından gerekli olması:** Daha az sınırlayıcı bir müdahale ile aynı veya daha iyi bir sonuç elde edilebilecek ise bu kapsamda kullanılan araç, gereklilik ilkesine aykırı olacaktır. Diğer bir deyişle, biyometrik veri işlemenin yerine herhangi bir alternatifin mevcut olması durumunda biyometrik verinin işlenmesi gerekli olmayacağından, söz konusu veriler işlenemeyecektir. Her somut olayda amaca bakarak yorum getirilmeli, veri sorumlusu tarafından biyometrik verinin neden işlendiği açıkça belirtilmeli ve işlenmek zorunda olduğu kanıtlanmalıdır.

» **Veri işlemeyle ulaşılmak istenilen amaç ve aracın arasında orantı bulunması:** Biyometrik veri işleme faaliyetinde müdahalenin ağırlığı ile müdahaleyi haklı kılacak sebepler arasında ölçülülüğün bulunması gerekmekte olup, kullanılan araç neticesinde ilgili kişilere orantısız müdahalelerde bulunulmamalıdır. Birden fazla aracın bulunduğu durumda en uygun olan aracın seçilmesi bu kapsamda orantılılığı ifade etmektedir.

» **Gerektiği süre kadar tutulması, gereklilik ortadan kalktıktan sonra söz konusu verilerin gecikmeksizin / derhal imha edilmesi**

» **İşleme amacı doğrultusunda sınırlı olmak üzere, veri sorumlularının Kanun'un 10'uncu maddesine uygun bir biçimde aydınlatma yükümlülüğünü yerine getirmesi:** Biyometrik veri işleme faaliyetlerinde, aydınlatma yükümlülüğünün yerine getirilmesine ilişkin Kanun'un 10'uncu maddesi ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümleri yanı sıra, biyometrik verile-

rin önemine binaen veri sorumluları tarafından hangi biyometrik verilerin hangi hukuki sebeple ve hangi amaçla alındığı, bu verilerin önemi ve veri ihlali durumunda ortaya çıkabilecek sonuçların neler olabileceği (biyometrik verilerin işlenmesine yönelik riskler) hususlarına ilişkin olarak ilgili kişiler ayrıca aydınlatılmalıdır.

» **Açık rızanın gerekmesi halinde ilgili kişilerin açık rızalarının Kanun'a uygun şekilde alınmış olması:** Rehber çerçevesinde veri sorumluları tarafından ayrıca (i) yukarıda sayılan bütün ilkelerin sağlandığı hususunun kayıt altına alınıp belgelendirilmesi, (ii) gerekmediği takdirde biyometrik veri alınırken genetik veri (örn. kan, tükürük) alınmaması, (iii) tercih edilen biyometrik veri türünün veya türlerinin (örn. iris, parmak izi, elin damar ağı) diğerleri yerine neden seçildiğine dair gerekçeler ve belgeler sunulması ve (iv) biyometrik özelliğin bütün çeşitlerinin (örn. ham ve türetilmiş kayıtlar) gereken süre boyunca işlenmesi ve söz konusu verilerin ne kadar süre boyunca tutulacağının nedenleri ile birlikte saklama ve imha politikasında açıklanması gerektiği ifade edilmiştir.

4- Biyometrik Veri Güvenliği

Veri sorumluları tarafından verilerin niteliği ve veri işlemenin ilgili kişi açısından oluşturacağı muhtemel risklerle ilgili olarak, verilerin güvenliğini sağlamak amacıyla gerekli teknik ve tedbirler alınmalıdır. Bu çerçevede, Kurum tarafından veri sorumlularına yol göstermek amacıyla hazırlanan rehber dokümanlarda tavsiye edilen tedbirlerden uygun olanlar dikkate alınmalı ve Kişisel Verileri Koruma Kurulu'nun özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemlere ilişkin 31 Ocak 2018 tarihli ve 2018/10 sayılı kararında belirtilen tedbirler yerine getirilmelidir. Bahse konu mevzuat ve rehberlerdeki veri güvenliği tedbirlerine ilaveten, Rehber kapsamında, biyometrik veri işleme hususunda aşağıdaki tedbirlerin de alınması gerektiği ifade edilmiştir:

Teknik Tedbirler:

» Biyometrik verilerin bulut sistemlerinde ancak kriptografik yöntemler kullanılarak muhafaza edilmesi,

» Türetilmiş biyometrik verilerin orijinal biyometrik özelliklerinin yeniden elde edilmesine izin vermeyecek şekilde saklanması,
» Biyometrik verilerin ve şablonlarının güncel teknolojiye uygun olarak, yeterli güvenliği sağlayacak kriptografik yöntemlerle şifrelenmesi ve şifreleme ile anahtar yönetimi politikasının açıkça tanımlanması,
» Sistemler kurulmadan önce ve herhangi bir değişiklikten sonra, oluşturulacak test ortamlarında sentetik veriler (gerçek olmayan) aracılığıyla sistemin test edilmesi,
» Test amaçlı olarak yapılacak çalışmalarda biyometrik verilerin kullanımının gerekli olanlar ile sınırlandırılması ve tüm verilerin en geç testlerin sonunda silinmesi,
» Sistemlere yetkisiz erişilmesi durumunda sistem yöneticisini ikaz eden ve/veya biyometrik verileri silen ve rapor veren önlemler uygulanması,
» Sistemlerde sertifikalı teçhizat, lisanslı ve güncel yazılımlar kullanılması, öncelikli olarak açık kaynak kodlu yazılımların tercih edilmesi ve sistemlerdeki gerekli güncellemelerin zamanında yapılması,
» Biyometrik veri işleyen cihazların kullanım ömürlerinin izlenebilir olması,
» Biyometrik veri işleyen yazılımlar üzerindeki kullanıcı işlemlerinin izlenebilmesi ve sınırlandırılabilmesi ve
» Biyometrik veri sistemlerinin donanımsal ve yazılımsal testlerinin periyodik olarak yapılması.

İdari Tedbirler:

» Biyometrik çözümü kullanamayan (örn. biyometrik verilerin kaydedilmesi veya okunması imkansız, kullanımı zorlaştıran handikap durumu) veya kullanmaya açık rızası olmayan ilgili kişiler için herhangi bir kısıtlama veya ek maliyet olmaksızın alternatif bir sistem sağlanması,
» Biyometrik yöntemlerle kimlik doğrulamanın yapılamaması ya da başarısızlığı durumunda uygulanacak bir eylem planı oluşturulması (örn. bir kimliği doğrulayamama, güvenli bir alana girme yetkisi eksikliği),
» Yetkili kişilerin biyometrik veri sistemlerine erişim mekanizmaları kurulması, yönetilmesi ve sorumluların belirlenerek belgelendirilmesi,
» Biyometrik veri işleme sürecinde yer alan personellere biyometrik verilerin işlenmesi hususunda özel eğitimler verilmesi ve söz konusu eğitimlerin belgelendirilmesi,
» Çalışanların sistem ve servislerdeki muhtemel güvenlik zafiyetleri ve söz konusu zafiyetler sonucu oluşabilecek tehditleri bildirebilmesi için resmi bir raporlama prosedürünün oluşturulması ve
» Veri ihlali durumunda uygulanmak üzere acil durum prosedürü oluşturulması ve ilgili herkese duyurulması.