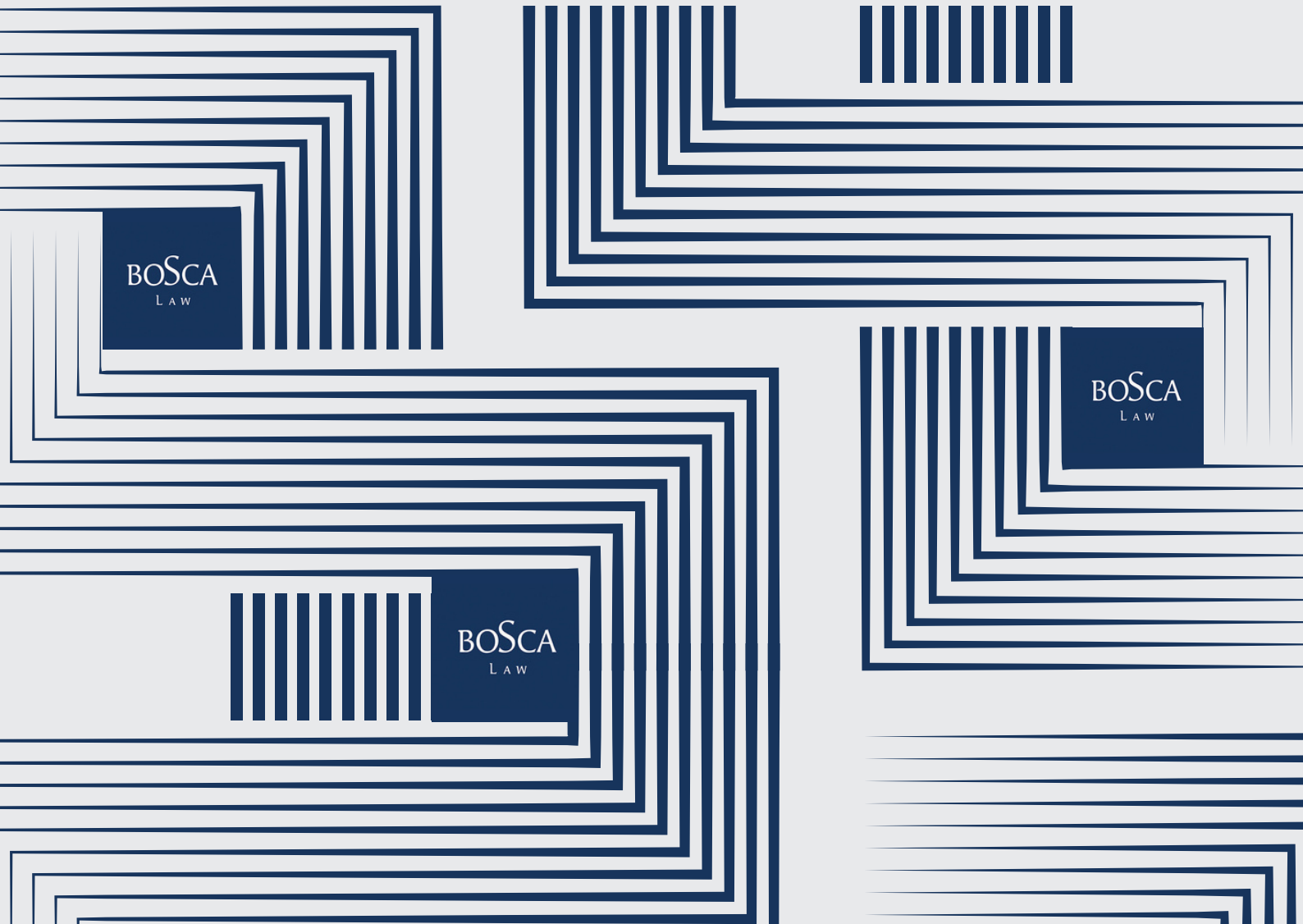
Kişisel Verileri Koruma Kurulu'nun 2026/266 Sayılı İlke Kararı ve Sadakat Kartı Programlarında Kişisel Veri İşleme Rejiminin Yeniden Tanımlanması



KVKK Kurulu’nun 2026/266 Sayılı İlke Kararı

Resmi Gazete

28.02.2026 - 33182

İçindekiler

I. Giriş

Perakende sektöründe sadakat kartı ve üyelik programları, uzun süredir müşteri bağlılığını artıran temel ticari araçlardan biri olarak kullanılmaktadır. Telefon numarası, sadakat kart numarası veya üyelik hesabı üzerinden yürütülen bu sistemler; indirim uygulanması, puan kazanımı, kampanya yönetimi ve müşteri davranışlarının analiz edilmesi gibi çok katmanlı veri işleme faaliyetlerini içermektedir.

Bununla birlikte söz konusu sistemler, uygulamada çoğu zaman veri koruma hukukunun temel varsayımlarından biri olan "ilgili kişi ile veri işleme faaliyetinin fiilî bağlantısı" yeterince sorgulanmaksızın işletilmiştir. Alışveriş sırasında yalnızca bir telefon numarasının paylaşılması yoluyla sadakat avantajlarının kullanılabilmesi, ticari açıdan pratik bir çözüm olarak kabul edilmiş; ancak kişisel veri hukuku bakımından doğurduğu sonuçlar ikincil planda kalmıştır.

Kişisel Verileri Koruma Kurulu'nun 11.02.2026 tarihli ve 2026/266 sayılı İlke Kararı, tam da bu noktada müdahale ederek sadakat programlarının hukuki niteliğini yeniden tartışmaya açmıştır. Karar, görünürde sınırlı bir uygulamayı konu almakla birlikte, gerçekte Türkiye'de kişisel veri uyum anlayışının yönünü değiştiren yapısal bir yaklaşım ortaya koymaktadır.

II. İlke Kararının Konusu

Kişisel Verileri Koruma Kurulu'nun söz konusu İlke Kararı incelendiğinde, kararın çıkış noktasını oluşturan hususun belirli bir şirkete özgü münferit bir uygulama olmadığı, aksine farklı sektörlerde faaliyet gösteren çok sayıda veri sorumlusunda benzer şekilde ortaya çıkan yaygın bir operasyonel model olduğu anlaşılmaktadır. Kurul, yaptığı değerlendirmede perakende, e-ticaret, hizmet ve müşteri sadakati temelli ticari faaliyet yürüten işletmelerde ortak bir uygulama pratiğinin bulunduğunu tespit etmiş ve bu pratiği kişisel veri koruma hukuku bakımından sistematik bir risk alanı olarak ele almıştır.

Tespit edilen uygulama modelinde sadakat kartı veya müşteri üyeliği belirli bir gerçek kişiye ait olmakla birlikte, alışveriş işlemi sırasında ilgili kişinin fiilen işlemde bulunmasının aranmadığı görülmektedir. Uygulamada çoğu zaman kasada bulunan kişinin yalnızca ilgili kişiye ait cep telefonu numarasını veya sadakat kart numarasını paylaşması yeterli kabul edilmekte; sistem bu bilgi üzerinden üyelik hesabını otomatik olarak eşleştirerek indirim, kampanya veya puan avantajlarını devreye almaktadır. Bu süreçte veri sorumlusu tarafından herhangi bir kimlik doğrulama mekanizmasının işletilmediği veya doğrulamanın yalnızca sözlü beyana dayalı olduğu anlaşılmaktadır.

Kurul'un dikkat çektiği husus, bu uygulamanın çoğu zaman ticari kolaylık veya müşteri memnuniyetini artıran pratik bir yöntem olarak görülmesine rağmen, veri işleme faaliyetinin özüne ilişkin önemli sonuçlar doğurmasıdır. Çünkü sadakat sistemi üzerinden gerçekleştirilen her işlem, yalnızca anlık bir indirim uygulanmasından ibaret değildir; aynı zamanda veri sorumlusunun bilgi sistemlerinde ilgili kişi adına yeni bir veri kaydı oluşturulması anlamına gelmektedir. Başka bir ifadeyle, alışveriş işlemi tamamlandığı anda sistem, ilgili kişinin satın alma davranışına ilişkin yeni bir veri üretmekte ve bu veriyi müşteri profiline kalıcı olarak eklemektedir.

Bu modelin sonucu olarak, fiilen alışveriş yapmayan bir kişi adına alışveriş kayıtları oluşturulmakta, satın alma geçmişi gerçeğe aykırı şekilde şekillenmekte ve sadakat hesabı üzerinden puan veya avantaj hareketleri ilgili kişiye atfedilmektedir. Zaman içerisinde bu kayıtlar birikerek ilgili kişinin tüketim alışkanlıklarını yansıttığı varsayılan kapsamlı bir profil meydana getirmektedir. Oysa bu profil, ilgili kişinin gerçek ekonomik davranışlarını değil, üçüncü kişilerin gerçekleştirdiği işlemleri de içerebilmektedir. Bu durum özellikle veri analitiği, hedefli pazarlama, kampanya yönetimi ve müşteri segmentasyonu gibi süreçlerde veri doğruluğunu doğrudan etkileyen bir sonuç doğurmaktadır.

Kurul ayrıca bazı uygulamalarda sadakat hesabı ile fatura veya müşteri işlem bilgilerinin de ilişkilendirilebildiğine dikkat çekmektedir. Bu tür durumlarda yalnızca alışveriş geçmişi değil, mali işlem kayıtları da ilgili kişiyle bağlantılı hale gelmekte ve kişisel veri işleme faaliyetinin kapsamı genişlemektedir. Böylece veri sorumlusu, ilgili kişinin bilgisi veya fiilî katılımı olmaksızın o kişi adına ekonomik işlem verisi üretmiş olmaktadır. Kurul'a göre bu sonuç, kişisel veri işleme faaliyetinin temel varsayımı olan "verinin ilgili kişiyle bağlantılı olması" ilkesini zedeleyen bir nitelik taşımaktadır.

Kararda özellikle vurgulanan husus, söz konusu uygulamanın yalnızca sadakat programının kullanım biçimine ilişkin ticari bir tercih olarak değerlendirilemeyeceğidir. Kurul, bu uygulamanın doğrudan kişisel veri işleme faaliyetinin hukuka uygunluğu ile bağlantılı olduğunu açıkça ortaya koymaktadır. Çünkü veri sorumlusu tarafından işlenen veri, ilgili kişinin gerçek davranışını temsil etmiyorsa, veri işleme faaliyetinin hukuki dayanağı ve meşruiyeti tartışmalı hale gelmektedir. Bu noktada mesele artık bir pazarlama stratejisi veya müşteri deneyimi tercihi olmaktan çıkmakta; kişisel verilerin doğru, dürüst ve hukuka uygun şekilde işlenip işlenmediği sorusuna dönüşmektedir.

III. KVKK'nın Temel İlkeleri Açısından Değerlendirme

A. Genel İlkeler (KVKK m.4) Bakımından Sorun

Kişisel Verileri Koruma Kurulu'nun söz konusu İlke Kararı incelendiğinde, değerlendirmesinin merkezinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde düzenlenen genel ilkelerin yer aldığı görülmektedir. Kurul, sadakat kartı uygulamalarına ilişkin incelemesini yalnızca belirli bir işlem pratiğinin uygunluğu üzerinden değil, kişisel veri işleme faaliyetinin temelini oluşturan normatif ilkeler çerçevesinde ele almış ve özellikle "hukuka ve dürüstlük kurallarına uygun işleme" ile "doğru ve gerektiğinde güncel olma" ilkelerinin ihlal edilme riskine odaklanmıştır.

Genel ilkeler, kişisel veri koruma hukukunun çekirdeğini oluşturmakta ve veri işleme faaliyetinin hukuka uygunluğunun ilk değerlendirme aşamasını teşkil etmektedir. Bu ilkeler yalnızca veri işleme süreçlerine yön veren soyut prensipler değil, veri sorumlularının tüm operasyonel faaliyetlerine nüfuz eden bağlayıcı kurallardır. Kurul'un kararında özellikle veri doğruluğu ilkesine yaptığı vurgu, kişisel veri hukukunda uzun süredir teknik doğruluk ekseninde değerlendirilen bir kavramın daha geniş bir anlam çerçevesine oturtulduğunu göstermektedir.

Uygulamada sadakat sistemleri, müşterinin telefon numarası veya üyelik bilgisi üzerinden otomatik eşleştirme yaparak işlem gerçekleştirmektedir. Teknik açıdan bakıldığında sistem doğru çalışmakta; girilen telefon numarası doğru üyelik hesabını bulmakta ve işlem ilgili hesap üzerinde kayıt altına alınmaktadır.

Ancak Kurul'un yaklaşımı, veri doğruluğunun yalnızca sistemsel eşleşmenin doğru olmasına indirgenemeyeceğini ortaya koymaktadır. Çünkü veri doğruluğu, yalnızca bilginin doğru veri alanına yazılması değil, aynı zamanda o bilginin doğru kişiye ait olması anlamına gelmektedir.

Bir kişinin fiilen gerçekleştirmediği alışverişlerin o kişi adına veri sistemine kaydedilmesi, teknik olarak hatasız görünen fakat içerik bakımından gerçeği yansıtmayan bir veri üretimine yol açmaktadır. Bu durumda veri sorumlusu tarafından oluşturulan müşteri profili, ilgili kişinin gerçek tüketim alışkanlıklarını değil, üçüncü kişilerin davranışlarını içeren karma bir veri setine dönüşmektedir. Böyle bir veri seti ise yalnızca bireysel veri doğruluğunu zedelemekle kalmamakta; aynı zamanda veri analitiği, hedefli pazarlama, segmentasyon ve müşteri davranışı modelleme gibi süreçlerin de yanlış sonuçlar üretmesine neden olmaktadır.

Kurul'un değerlendirmesinde dikkat çeken husus, veri doğruluğu ilkesinin maddi gerçeklik kavramı ile ilişkilendirilmesidir. Veri yalnızca teknik anlamda doğru olduğunda değil, gerçek dünyadaki davranışı doğru temsil ettiğinde hukuka uygun kabul edilmektedir. Bu yaklaşım, kişisel verinin statik bir bilgi olmadığı; bireyin kimliği, davranışı ve ekonomik faaliyetleriyle doğrudan bağlantılı dinamik bir unsur olduğu anlayışına dayanmaktadır.

Kurul ayrıca hukuka ve dürüstlük kurallarına uygun işleme ilkesini de veri doğruluğu değerlendirmesiyle birlikte ele almaktadır. Veri sorumlusunun sistem tasarımı, üçüncü kişilerin ilgili kişi adına işlem yapmasını kolaylaştırıyorsa ve bu durum veri üretim sürecinde öngörülebilir bir sonuç doğuruyorsa, veri işleme faaliyetinin dürüstlük kuralıyla bağdaşması güçleşmektedir. Çünkü veri sorumlusu, fiilen işlem yapmayan bir kişi hakkında davranış verisi üretildiğini bilmesine veya makul ölçüde öngörebilmesine rağmen bu durumu engelleyecek mekanizmaları kurmamış olmaktadır.

Bu noktada Kurul'un yaklaşımı, veri sorumlularına yalnızca pasif bir veri kayıt rolü yüklememekte; aksine veri üretim sürecinin doğruluğunu sağlama yönünde aktif bir sorumluluk yüklemektedir. Veri sorumlusu, sistemin teknik olarak çalıştığını ileri sürerek sorumluluktan kurtulamaz; çünkü Kanun'un 4. maddesi veri işleme faaliyetinin sonuçlarının da hukuka uygun olmasını gerektirmektedir. Başka bir ifadeyle, veri işleme sürecinin çıktısı gerçeği yansıtmıyorsa, süreç hukuka uygun kabul edilemez.

Artık veri doğruluğu yalnızca yanlış yazılmış isimlerin düzeltilmesi veya eksik bilgilerin güncellenmesi anlamına gelmemekte; işlemi gerçekleştiren kişi ile veri sahibinin örtüşmesini de içeren daha kapsamlı bir doğruluk anlayışını ifade etmektedir.

B. Veri İşleme Şartları (KVKK m.5) Açısından Değerlendirme

Kişisel Verileri Koruma Kurulu'nun kararında ortaya koyduğu ikinci temel hukuki değerlendirme alanı, 6698 sayılı Kanun'un 5. maddesinde düzenlenen kişisel veri işleme şartlarına ilişkindir. Kurul, sadakat kartı uygulamalarında veri işleme faaliyetinin çoğunlukla üyelik sözleşmesine dayandırıldığını kabul etmekle birlikte, sözleşmesel ilişkinin varlığının tek başına veri işleme faaliyetini otomatik olarak hukuka uygun hale getirmeyeceğini açık biçimde ortaya koymaktadır.

Uygulamada sadakat programları, müşteri ile veri sorumlusu arasında kurulan üyelik sözleşmesi kapsamında yürütülmektedir. Bu sözleşme aracılığıyla müşteri sadakat sistemine dahil olmakta, puan kazanma, kampanyalardan yararlanma ve kişiselleştirilmiş teklif alma gibi avantajlar elde ederken veri sorumlusu da müşterinin alışveriş davranışlarına ilişkin verileri işlemektedir. Bu nedenle veri sorumluları çoğu durumda veri işleme faaliyetlerini Kanun'un 5. maddesinin ikinci fıkrasında yer alan "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması" hukuki sebebine dayandırmaktadır.

Kurul'un değerlendirmesine göre, ilgili kişi adına üçüncü bir kişi tarafından gerçekleştirilen alışverişlerde veri işleme faaliyetinin hukuki zemini zayıflamaktadır. Öncelikle işlem anında ilgili kişinin iradesi mevcut değildir; yani veri işleme faaliyetinin gerçekleştiği anda veri sahibinin bilinçli bir katılımından söz edilemez. Sadakat programına önceden üye olunmuş olması, her somut işlem bakımından ilgili kişinin iradesinin varsayılmasını mümkün kılmamaktadır. Çünkü kişisel veri işleme faaliyetinin hukuka uygunluğu, yalnızca başlangıçtaki sözleşme ilişkisine değil, her bir veri işleme eyleminin kendi bağlamına göre değerlendirilmesine bağlıdır.

Bu noktada Kurul'un yaklaşımı, veri işleme şartlarının statik değil dinamik bir nitelik taşıdığını ortaya koymaktadır. İlgili kişinin fiilen taraf olmadığı bir alışveriş işlemi, sözleşmenin ifası kapsamında değerlendirilemeyeceğinden, veri işleme faaliyetinin Kanun'un 5. maddesinde öngörülen hukuki sebeplerden birine dayanıp dayanmadığı tartışmalı hale gelmektedir.

Kurul'un bu yorumu, kişisel veri işleme şartlarının yalnızca soyut hukukî ilişkilere dayanarak geniş yorumlanamayacağını göstermektedir. Veri sorumlusu, sisteminde kayıtlı bir üyelik ilişkisini ileri sürerek her veri işleme faaliyetini otomatik biçimde sözleşme kapsamında değerlendiremez. Aksine veri işleme faaliyetinin, işlem anında sözleşmenin tarafı olan kişiyle gerçek ve doğrudan bir bağlantı içinde olması gerekir.

C. Veri Güvenliği Yükümlülüğü (KVKK m.12) Perspektifi

Kurul kararında en güçlü ve uygulama bakımından en dönüştürücü değerlendirme alanı, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12. maddesinde düzenlenen veri güvenliği yükümlülüğüne ilişkindir. Kurul, sadakat kartı uygulamalarına ilişkin sorunu yalnızca veri doğruluğu veya veri işleme şartları bağlamında ele almakla yetinmemiş; veri sorumlularının veri güvenliğine ilişkin pozitif yükümlülüklerini geniş bir yorumla değerlendirmiştir. Bu yönüyle karar, veri güvenliği kavramının kapsamını yeniden tanımlayan ve veri sorumlularının sorumluluk alanını operasyonel süreçlere doğrudan bağlayan önemli bir yaklaşım ortaya koymaktadır.

Kararda özellikle vurgulanan husus, sadakat programı üyelik sözleşmelerinde yer alan "kartın yalnızca ilgili kişi tarafından kullanılabileceği" veya "üçüncü kişilerle paylaşılmaması gerektiği" yönündeki hükümlerin tek başına veri sorumlusunu sorumluluktan kurtarmayacağıdır. Kurul'a göre veri sorumlusu, hukuka aykırı kullanım ihtimalini yalnızca sözleşmesel yasaklarla düzenlemekle yetinemez. Çünkü veri güvenliği yükümlülüğü, riskin kullanıcı davranışına bırakılmasını değil, veri işleme sisteminin bu riski azaltacak şekilde tasarlanmasını gerektirir.

Bu yaklaşım, veri güvenliği sorumluluğunu pasif bir yükümlülük olmaktan çıkararak aktif bir önleme yükümlülüğüne dönüştürmektedir. Kanun'un 12. maddesi veri sorumlularına kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek amacıyla uygun teknik ve idari tedbirleri alma yükümlülüğü yüklemektedir. Bu hüküm, veri işleme süreçlerinin kendi iç dinamiklerinden kaynaklanan hukuka aykırılık ihtimallerini de kapsamaktadır.

Sadakat kartı uygulamalarında üçüncü kişilerin ilgili kişi adına işlem yapabilmesi, Kurul tarafından öngörülebilir bir risk olarak değerlendirilmiştir. Bu durumda veri sorumlusu, sözleşmede yer alan kullanım yasaklarını ileri sürerek sorumluluktan kaçınamaz; çünkü veri güvenliği yükümlülüğü riskin ortaya çıkmasını önlemeye yönelik tedbirlerin fiilen uygulanmasını gerektirir.

Geleneksel olarak veri güvenliği çoğu zaman siber saldırılara karşı koruma, yetkisiz erişimin engellenmesi veya veri sızıntılarının önlenmesi şeklinde anlaşılmaktadır. Oysa bu kararda veri güvenliği, verinin yanlış kişi adına işlenmesini önleme yükümlülüğünü de kapsayacak şekilde yorumlanmaktadır. Böylece veri güvenliği yalnızca dış tehditlere karşı koruma değil, sistemin kendi işleyişinden kaynaklanan hatalı veri üretimini engelleme sorumluluğunu da içermektedir.

Veri güvenliği artık normatif bir uyum meselesi değil, operasyonel bir tasarım sorumluluğu olarak ele alınmaktadır. Başka bir ifadeyle veri sorumlusu yalnızca kuralları belirleyen değil, bu kuralların fiilen uygulanmasını sağlayan sistemleri kurmakla yükümlüdür. Bu yaklaşım, uluslararası veri koruma hukukunda giderek önem kazanan “privacy by design” ve “privacy by default” anlayışlarıyla paralellik göstermektedir.

IV. Sadakat Bilgisi Kimlik Doğrulama Aracı Değildir

Kişisel Verileri Koruma Kurulu'nun 2026/266 sayılı İlke Kararı'nın ortaya koyduğu en temel ve uygulamada en geniş etki doğuracak sonucu, sadakat kartı sistemlerinde kullanılan bilgilerin hukuki niteliğine ilişkin yaptığı değerlendirmedir. Kurul, açık bir biçimde telefon numarası, sadakat kart numarası veya üyelik bilgisi gibi verilerin tek başına kimlik doğrulama aracı olarak kabul edilemeyeceğini ortaya koymuştur. Bu tespit, ilk bakışta teknik bir ayrım gibi görünse de, gerçekte perakende ve müşteri yönetimi sistemlerinin veri işleme mantığını doğrudan etkileyen yapısal bir ilkeye işaret etmektedir.

Uygulamada sadakat sistemleri uzun süredir "bilgiye sahip olan kişinin yetkili kullanıcı olduğu" varsayımı üzerine kuruludur. Kasada telefon numarasının söylenmesi veya sadakat kart numarasının paylaşılması, sistem tarafından ilgili kişinin kimliğinin doğrulanması için yeterli kabul edilmekte ve işlem bu varsayım üzerine tamamlanmaktadır. Ancak Kurul'un değerlendirmesi, bu varsayımın kişisel veri koruma hukuku bakımından geçerli olmadığını ortaya koymaktadır. Çünkü telefon numarası veya kart numarası, ilgili kişiye ait bir veri olmakla birlikte, bu veriye erişen kişinin mutlaka veri sahibi olduğu anlamına gelmemektedir.

Kurul'un yaklaşımına göre sadakat bilgisi bir kimlik doğrulama unsuru değil, yalnızca bir hesap tanımlayıcısıdır. Başka bir ifadeyle bu bilgiler, sistemin hangi üyelik hesabı üzerinde işlem yapacağını belirler; ancak işlemi yapan kişinin gerçekten o hesabın sahibi olduğunu kanıtlamaz. Bu ayrım, veri işleme faaliyetinin hukuka uygunluğu bakımından kritik öneme sahiptir. Zira veri işleme faaliyetinin ilgili kişiye atfedilebilmesi için yalnızca doğru hesabın bulunması yeterli değildir; işlemin gerçekten ilgili kişi tarafından gerçekleştirildiğinin makul ölçüde doğrulanabilir olması gerekir.

Kurul bu nedenle veri sorumlularından, sadakat sistemi kapsamında gerçekleştirilen işlemlerin ilgili kişiyle ilişkilendirilebilir şekilde doğrulanmasını sağlayacak mekanizmalar kurmasını beklemektedir.

Kararda belirli bir teknoloji veya yöntem zorunlu tutulmamakta, bunun yerine doğrulanabilirlik ilkesine odaklanılmaktadır. Tek kullanımlık doğrulama kodları (OTP), mobil uygulama üzerinden doğrulama, fiziksel sadakat kartının okutulması, kullanıcıya özel şifre kullanımı veya hesap bazlı onay mekanizmaları gibi yöntemler örnek olarak sayılmıştır. Ancak Kurul'un vurgusu, bu yöntemlerin kendisinden ziyade, veri işleme faaliyetinin ilgili kişiyle güvenilir biçimde ilişkilendirilebilmesidir.

Kurul'un beklentisi, veri sorumlularının müşteri deneyimi ile veri güvenliği arasında yeni bir denge kurmasıdır. İşlemin hızlı gerçekleşmesi tek başına yeterli bir gerekçe olarak kabul edilmemekte; veri işleme faaliyetinin doğrulanabilir bir irade ve kimlik bağlantısına dayanması gerektiği kabul edilmektedir.

Kararın ortaya koyduğu bu ilke, kişisel veri hukukunda kimlik doğrulama kavramının kapsamını da dolaylı biçimde genişletmektedir. Artık kimlik doğrulama yalnızca finansal işlemler veya yüksek güvenlik gerektiren dijital hizmetler bakımından değil, davranış verisi üreten ticari sistemler bakımından da gerekli bir unsur olarak değerlendirilmektedir. Çünkü sadakat sistemleri yalnızca indirim uygulayan araçlar değil; bireyin tüketim alışkanlıklarını kayıt altına alan ve bu veriler üzerinden profil oluşturan sistemlerdir. Dolayısıyla bu sistemlerde yapılan her işlem, kişisel veri üretimi anlamına gelmektedir.

V. Etkilenen Veri Sorumluları ve Sektörel Yansımalar

Kişisel Verileri Koruma Kurulu'nun 2026/266 sayılı İlke Kararı'nın etkisi, ilk bakışta yalnızca sadakat kartı uygulaması kullanan perakende işletmeleriyle sınırlı gibi görünse de, kararın ortaya koyduğu hukuki yaklaşım dikkate alındığında çok daha geniş bir ekosistemi kapsadığı anlaşılmaktadır. Zira Kurul'un değerlendirmesi belirli bir sektöre özgü teknik bir düzenleme niteliği taşımamakta; sadakat sistemleri aracılığıyla yürütülen kişisel veri işleme faaliyetlerinin tamamına uygulanabilecek genel bir ilke ortaya koymaktadır. Bu nedenle karar, yalnızca fiziksel mağazacılık faaliyetlerini değil, müşteri verisi işleyen tüm dijital ve hibrit ticari modelleri doğrudan etkileme potansiyeline sahiptir.

Öncelikle zincir mağazalar ve büyük ölçekli perakende organizasyonları kararın en doğrudan muhataplarıdır. Bu işletmelerde sadakat programları genellikle merkezi veri tabanları üzerinden yürütülmekte, müşteri bilgileri tüm mağazalarda ortak şekilde kullanılmaktadır. Dolayısıyla herhangi bir mağazada gerçekleştirilen doğrulamasız işlem, yalnızca yerel bir operasyon hatası olarak değil, merkezi veri işleme sistemine yansıyan bir veri güvenliği sorunu olarak değerlendirilmelidir. Kurul'un yaklaşımı, mağaza bazlı uygulamaların merkez veri sorumluluğunu ortadan kaldırmadığını açıkça ortaya koymaktadır. Bu durum, büyük perakende zincirlerinin sadakat süreçlerini yalnızca operasyonel kolaylık açısından değil, veri koruma hukuku perspektifinden yeniden tasarlamalarını zorunlu hale getirmektedir.

Kararın önemli etkilerinden biri franchise modeliyle faaliyet gösteren organizasyonlarda ortaya çıkmaktadır. Franchise yapılarında günlük operasyonlar çoğu zaman bağımsız işletmeciler tarafından yürütülse de, sadakat sistemleri genellikle marka sahibi veya merkez şirket tarafından kurulmakta ve yönetilmektedir. Kurul'un veri sorumluluğuna ilişkin yaklaşımı dikkate alındığında, sahadaki uygulamaların üçüncü kişiler tarafından gerçekleştirilmesi veri sorumluluğunu ortadan kaldırmamaktadır.

Başka bir ifadeyle, franchise işletmecisinin kasada gerçekleştirdiği doğrulamasız bir işlem, merkezi organizasyon bakımından veri güvenliği yükümlülüğünün ihlali sonucunu doğurabilir. Bu nedenle franchise sistemlerinde yalnızca sözleşmesel yükümlülüklerin belirlenmesi yeterli olmayacak; operasyonel uygulamaların merkezi uyum politikalarıyla uyumlu şekilde standartlaştırılması gerekecektir.

E-ticaret platformları bakımından kararın etkisi daha da geniş bir boyut taşımaktadır. Online alışveriş sistemlerinde kullanıcı hesaplarının telefon numarası veya e-posta üzerinden eşleştirilmesi yaygın bir uygulamadır. Sadakat puanlarının otomatik tanımlanması, hızlı ödeme süreçleri ve hesap bazlı kampanyalar, veri işleme faaliyetinin büyük ölçüde otomatik sistemler aracılığıyla gerçekleşmesine yol açmaktadır. Kurul'un ortaya koyduğu doğrulanabilirlik yaklaşımı, bu platformların hesap erişimi ve işlem onayı süreçlerini yeniden değerlendirmesini gerektirebilir. Özellikle kullanıcı hesabı ile işlem yapan kişinin aynı olup olmadığının makul ölçüde doğrulanmadığı sistemler bakımından uyum riskleri ortaya çıkabilecektir.

Kararın etkilediği bir diğer önemli aktör grubu müşteri ilişkileri yönetimi (CRM) hizmeti sunan teknoloji sağlayıcılarıdır. Günümüzde birçok şirket sadakat programı altyapısını dış hizmet sağlayıcılardan temin etmekte ve müşteri verisi bu platformlar üzerinden işlenmektedir.

Kurul'un veri güvenliği ve doğrulama mekanizmalarına ilişkin yaklaşımı, CRM sistemlerinin yalnızca veri depolama veya analiz aracı olarak değil, veri işleme sürecinin aktif bir parçası olarak değerlendirilmesine yol açmaktadır. Bu durum, yazılım sağlayıcılarının ürün tasarımlarında veri koruma ilkelerini dikkate almasını ve müşterilerine KVKK uyumunu destekleyen teknik çözümler sunmasını gerekli kılmaktadır.

Benzer şekilde sadakat programı yazılımı geliştiren şirketler ile POS ve ödeme altyapısı sağlayıcıları da kararın dolaylı fakat önemli muhatapları arasında yer almaktadır. Çünkü sadakat doğrulama süreçleri çoğu zaman doğrudan kasa sistemleri veya ödeme altyapıları üzerinden yürütülmektedir. Eğer sistem tasarımı, yalnızca telefon numarası girilmesiyle işlem yapılmasına izin veriyorsa, veri sorumlusu kadar sistemi tasarlayan teknoloji altyapısı da uyum tartışmasının parçası haline gelmektedir. Bu durum, veri koruma hukukunun artık yalnızca hukuk departmanlarını değil, yazılım geliştirme ve ürün tasarım ekiplerini de doğrudan ilgilendirdiğini göstermektedir.

Veri sorumluluğu yalnızca veri tabanını yöneten tüzel kişiye ait soyut bir statü olmaktan çıkmakta; veri işleme sürecine katkı sağlayan tüm organizasyonel yapıların uyum zinciri içinde değerlendirilmesini gerektirmektedir.

VI. Uyum Perspektifi

Kişisel Verileri Koruma Kurulu'nun 2026/266 sayılı İlke Kararı'nın en dikkat çekici ve uzun vadede en önemli etkilerinden biri, veri koruma uyumuna ilişkin yerleşik anlayışı dönüştürmesidir. Türkiye'de KVKK uygulamasının yürürlüğe girdiği ilk yıllardan itibaren uyum süreçleri büyük ölçüde belge merkezli bir yaklaşım üzerinden şekillenmiştir. Veri sorumluları bakımından uyum çoğu zaman aydınlatma metinlerinin hazırlanması, açık rıza süreçlerinin oluşturulması, veri işleme envanterlerinin hazırlanması ve kurum içi politika dokümanlarının yayımlanması gibi normatif yükümlülüklerin yerine getirilmesiyle eşdeğer kabul edilmiştir. Bu yaklaşım, hukuki gerekliliklerin formel düzeyde karşılanmasını sağlamış olmakla birlikte, veri işleme faaliyetlerinin fiilî işleyişine çoğu zaman sınırlı ölçüde nüfuz edebilmiştir.

Kurul'un söz konusu İlke Kararı ise bu anlayışın artık yeterli görülmediğini açık biçimde ortaya koymaktadır. Kararın satır aralarında yer alan temel mesaj, veri koruma uyumunun yalnızca hukuki belgeler üretmekten ibaret olmadığıdır. Veri sorumlularının aydınlatma metni hazırlamış olması, açık rıza mekanizması kurması veya veri koruma politikalarını yayımlaması tek başına hukuka uygun veri işleme sonucunu garanti etmemektedir. Eğer veri işleme sistemi yapısal olarak hukuka aykırı kullanım ihtimalini mümkün kılıyorsa, belge düzeyindeki uyum faaliyetleri fiilî uyum eksikliğini ortadan kaldırmamaktadır.

Kurul'un yaklaşımı bu noktada örtük fakat son derece güçlü bir soruya indirgenebilir. Veri işleme sisteminiz, hukuka aykırı veri kullanımını teknik olarak engelliyor mu? Bu soru, veri koruma hukukunun odağını normatif düzenlemelerden operasyonel gerçekliğe kaydırmaktadır. Artık mesele yalnızca veri sorumlusunun hangi kuralları yazdığı değil, bu kuralların sistem tasarımına yansıyıp yansımadığıdır. Başka bir ifadeyle, veri koruma yükümlülüğü teorik bir taahhüt olmaktan çıkmakta, sistem mimarisinin ayrılmaz bir unsuru haline gelmektedir.

Sadakat kartı uygulaması üzerinden yapılan değerlendirme, bu dönüşümün somut bir örneğini sunmaktadır.

Veri sorumlusu sözleşmelerinde kartın üçüncü kişiler tarafından kullanılmasını yasaklamış olsa dahi, sistem telefon numarası girildiğinde otomatik işlem yapılmasına izin veriyorsa, hukuka aykırı kullanım ihtimali ortadan kaldırılmış sayılmamaktadır. Bu durumda veri sorumlusu, hukuki düzenleme yapmış olsa bile teknik önlem almamış kabul edilmektedir. Kurul'un yaklaşımı, veri koruma yükümlülüğünü davranış kurallarından sistem tasarımına taşıyan bir yorum niteliği taşımaktadır.

Bu gelişme, uluslararası veri koruma hukukunda uzun süredir kabul gören "privacy by design" ilkesine paralel bir yönelimi ifade etmektedir. Privacy by design anlayışı, veri korumanın sonradan eklenen bir uyum katmanı değil, sistemin tasarım aşamasından itibaren gözetilmesi gereken bir mühendislik ve yönetişim prensibi olduğunu kabul eder. Bu ilkeye göre veri koruma, politika belgeleri veya kullanıcı bildirimleriyle değil; erişim kontrolleri, doğrulama mekanizmaları, veri minimizasyonu ve risk azaltıcı teknik çözümler aracılığıyla sağlanmalıdır.

Kurul'un İlke Kararı, Türk veri koruma uygulamasında bu anlayışın fiilen benimsenmeye başladığını göstermektedir.

Veri sorumlularının sorumluluğu artık yalnızca hukuki metinlerin hazırlanmasıyla sınırlı değildir; bilgi sistemlerinin nasıl çalıştığı, kullanıcı akışlarının nasıl tasarlandığı ve veri işleme süreçlerinin hangi riskleri barındırdığı da uyum değerlendirmesinin parçası haline gelmiştir. Bu durum, veri koruma uyumunun yalnızca hukuk departmanlarının değil, bilgi teknolojileri, operasyon, ürün geliştirme ve müşteri deneyimi ekiplerinin ortak sorumluluğu haline geldiğini göstermektedir.

Dolayısıyla İlke Kararı, KVKK uyumunun ikinci evresine geçildiğinin güçlü bir göstergesi olarak değerlendirilebilir. İlk evre, hukuki farkındalık ve belge üretimi aşaması olarak tanımlanabilirken, yeni evre sistem mimarisi ve operasyonel tasarımın hukuka uygunluğu üzerine kurulmaktadır. Veri sorumluları açısından bu değişim, uyum çalışmalarının yalnızca mevzuat analizi değil, süreç analizi ve risk tasarımı perspektifiyle ele alınmasını zorunlu kılmaktadır.

VII. Risk Bazlı Doğrulama Modeli ve Orantılılık İlkesi

Kişisel Verileri Koruma Kurulu'nun söz konusu İlke Kararı'nda dikkat çeken önemli unsurlardan biri, doğrulama mekanizmalarına ilişkin yaklaşımın katı ve tek tip bir güvenlik modeli öngörmemesi, aksine işlem riskine göre farklılaştırılabilen bir doğrulama anlayışını benimsemesidir. Kurul, sadakat sistemlerinde kimlik doğrulamasının zorunluluğunu ortaya koyarken, her veri işleme faaliyetinin aynı yoğunlukta güvenlik tedbiri gerektirmediğini de dolaylı biçimde kabul etmektedir. Bu yaklaşım, kişisel veri koruma hukukunun temel prensiplerinden biri olan orantılılık ilkesinin veri güvenliği uygulamalarına yansıması olarak değerlendirilebilir.

Orantılılık ilkesi, veri koruma hukukunda alınacak tedbirlerin işlenen verinin niteliği, işlem faaliyetinin kapsamı ve ortaya çıkabilecek riskin ağırlığı ile uyumlu olması gerektiğini ifade eder. Başka bir ifadeyle veri sorumlusu, her durumda en ağır güvenlik tedbirlerini uygulamak zorunda değildir; ancak mevcut risk seviyesiyle uyumlu ve yeterli koruma sağlayan önlemleri almakla yükümlüdür. Kurul'un kararında doğrulama yöntemlerinin belirli bir teknolojiyle sınırlandırılmaması ve farklı doğrulama seviyelerine imkân tanınması, bu ilkenin açık bir yansımasıdır.

Sadakat sistemleri bakımından tüm işlemler aynı hukuki ve operasyonel riski doğurmamaktadır. Örneğin yalnızca puan kazanımına yol açan düşük etkili bir işlem ile puan harcama, hesap bilgisi değiştirme veya fatura düzenlenmesi gibi sonuç doğuran işlemler arasında veri koruma riski bakımından önemli farklar bulunmaktadır. Düşük riskli işlemlerde yanlış kişi tarafından işlem yapılması çoğu zaman sınırlı bir etki yaratırken, yüksek riskli işlemlerde hem ilgili kişinin ekonomik menfaatleri hem de veri doğruluğu ciddi şekilde zarar görebilmektedir. Kurul'un yaklaşımı, doğrulama yükümlülüğünün bu risk farklılıkları dikkate alınarak tasarlanabileceğini ortaya koymaktadır.

Bu çerçevede düşük riskli işlemler bakımından daha hafif doğrulama yöntemlerinin uygulanması mümkün olabilecekken, yüksek risk içeren işlemlerde daha güçlü kimlik doğrulama mekanizmalarının devreye alınması gerekebilecektir. Önemli olan husus, doğrulama seviyesinin işlemden doğabilecek hukuki ve teknik riskle makul bir ilişki içinde olmasıdır. Veri sorumlusu, gerçekleştirdiği veri işleme faaliyetlerinin risk analizini yapmalı ve doğrulama mekanizmalarını bu analiz doğrultusunda kurgulamalıdır. Böylece doğrulama süreci, yalnızca formal bir gereklilik olmaktan çıkarak risk yönetiminin bir parçası haline gelmektedir.

Kurul'un bu yaklaşımı aynı zamanda veri koruma ile müşteri deneyimi arasındaki hassas dengeyi de gözetmektedir. Sadakat programları ticari açıdan hız, kolaylık ve kullanıcı dostu deneyim üzerine kuruludur. Her işlem için ağır doğrulama mekanizmalarının zorunlu tutulması, sistemlerin işlevselliğini ve müşteri memnuniyetini olumsuz etkileyebilir. Bu nedenle risk bazlı doğrulama modeli, veri güvenliği gereklilikleri ile ticari gerçeklik arasında makul bir denge kurulmasına imkân tanımaktadır. Kurul, veri sorumlularından mutlak güvenlik değil, riskle orantılı güvenlik beklemektedir.

VIII. Uyum Süresi ve Olası Hukuki Sonuçlar

Kişisel Verileri Koruma Kurulu'nun 2026/266 sayılı İlke Kararı'nda dikkat çeken önemli hususlardan biri, kararın yalnızca ilkesel bir değerlendirme niteliği taşımakla kalmayıp veri sorumlularına belirli bir uyum takvimi de öngörmesidir. Kurul, İlke Kararı'nın yayımlanmasından itibaren veri sorumlularına altı aylık bir uyum süresi tanımış ve bu süreyi, mevcut sadakat sistemlerinin kişisel veri koruma hukukuna uygun hale getirilmesi için bir geçiş dönemi olarak değerlendirmiştir. Bu yaklaşım, Kurul'un kararın sektörel ölçekte yaygın etkiler doğuracağını öngördüğünü ve veri sorumlularına teknik ve operasyonel dönüşüm için makul bir hazırlık süresi tanımayı amaçladığını göstermektedir.

Altı aylık süre, veri sorumlularının yalnızca hukuki belgelerini güncellemesi için tanınmış bir süre olarak yorumlanmamalıdır. Kararın içeriği dikkate alındığında, uyum yükümlülüğünün esasen sistem tasarımı, doğrulama mekanizmaları, operasyonel süreçler ve çalışan uygulamalarını kapsayan yapısal değişiklikler gerektirdiği açıktır. Bu nedenle uyum süreci; mevcut sadakat programlarının risk analizi yapılmasını, veri işleme akışlarının yeniden değerlendirilmesini, teknik doğrulama yöntemlerinin belirlenmesini ve organizasyonel süreçlerin yeniden yapılandırılmasını içeren kapsamlı bir dönüşüm süreci olarak ele alınmalıdır.

Kurul'un belirlediği uyum süresinin sona ermesiyle birlikte, gerekli önlemleri almayan veri sorumluları bakımından çeşitli hukuki sonuçların gündeme gelmesi muhtemeldir. Öncelikle, Kanun'un 18. maddesi kapsamında idari para cezalarının uygulanması söz konusu olabilecektir. Veri güvenliği yükümlülüğünün ihlali veya kişisel verilerin hukuka aykırı işlenmesi durumunda uygulanabilecek idari yaptırımlar, özellikle büyük ölçekli veri işleyen organizasyonlar açısından önemli finansal riskler doğurabilir. Kurul'un İlke Kararı ile ortaya koyduğu açık standartlar dikkate alındığında, uyum eksikliği artık yorum farklılığına dayalı bir savunma alanı olmaktan büyük ölçüde çıkmaktadır.

Bunun yanında Kurul'un resen veya şikâyet üzerine inceleme süreçlerini başlatması da kuvvetle muhtemeldir. Sadakat sistemleri doğası gereği çok sayıda kullanıcıyı etkileyen ve sürekli veri üretimi gerçekleştiren yapılar olduğundan, bireysel bir şikâyet dahi geniş kapsamlı bir incelemeye dönüşebilecektir. Özellikle ilgili kişilerin bilgisi dışında yapılan işlemler, yanlış alışveriş kayıtları veya hatalı müşteri profillemesi gibi durumlar, Kurul nezdinde veri işleme faaliyetinin bütününün incelenmesine yol açabilir.

Özellikle yüksek hacimli müşteri verisi işleyen perakende organizasyonları bakımından risk katsayısı önemli ölçüde artmaktadır. Çünkü sadakat programları milyonlarca işlem kaydı üretebilmekte ve sistematik bir doğrulama eksikliği, münferit bir hatadan ziyade sürekli tekrarlanan bir veri işleme sorunu anlamına gelebilmektedir. Bu durum, hem idari yaptırımların ağırlığını artırabilecek hem de şirketlerin itibar yönetimi açısından ciddi sonuçlar doğurabilecek niteliktedir.

Ayrıca uyum eksikliği yalnızca düzenleyici yaptırımlarla sınırlı kalmayabilir. Yanlış veri işleme nedeniyle ilgili kişilerin maddi veya manevi zarar iddiasıyla hukuki yollara başvurması ihtimali de göz ardı edilmemelidir. Özellikle tüketici bilincinin ve veri koruma farkındalığının artmasıyla birlikte, sadakat sistemleri üzerinden oluşan hatalı kayıtlar bireysel uyuşmazlıklara konu olabilecek potansiyele sahiptir.

IX. Sonuç

Kişisel Verileri Koruma Kurulu'nun 2026/266 sayılı İlke Kararı, ilk bakışta sadakat kartı uygulamalarına ilişkin sınırlı bir düzenleyici değerlendirme gibi görünse de, içerdiği hukuki yaklaşım itibarıyla kişisel veri koruma hukukunun uygulama paradigmasında önemli bir dönüşüme işaret etmektedir. Karar, belirli bir sektörel uygulamayı düzeltmeye yönelik teknik bir müdahalenin ötesinde, veri işleme faaliyetlerinin nasıl anlaşılması ve değerlendirilmesi gerektiğine ilişkin daha geniş bir normatif çerçeve ortaya koymaktadır.

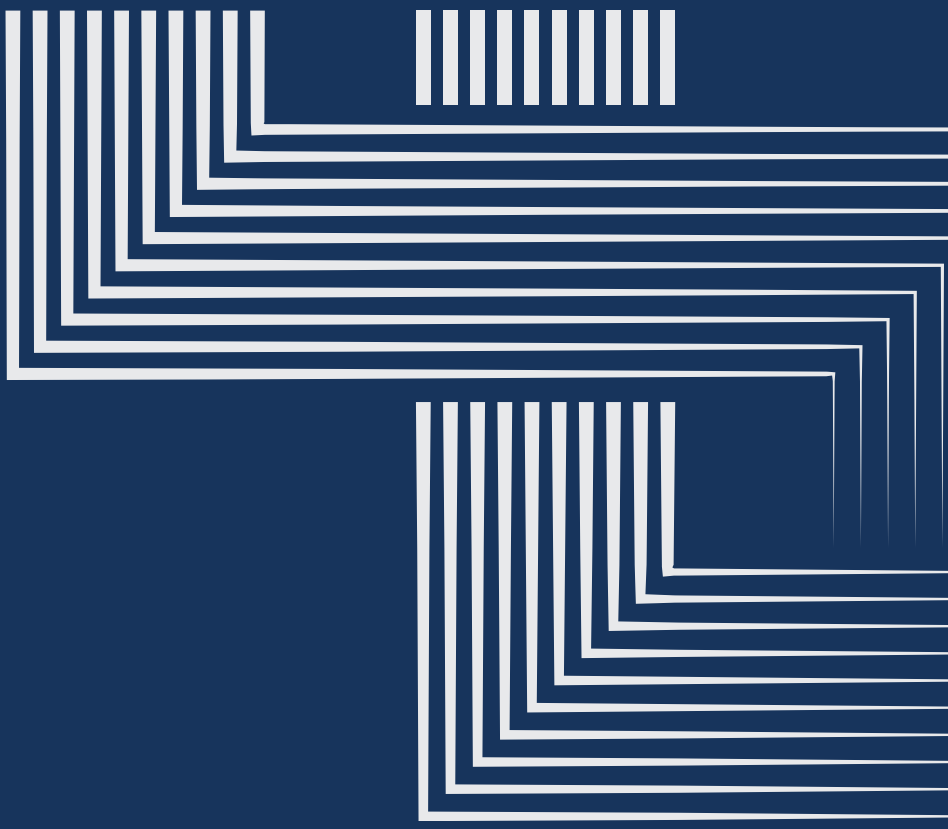
Kararın ortaya koyduğu temel yaklaşım, kişisel veri işleme faaliyetinin hukuka uygunluğunun artık yalnızca hukuki metinlerin varlığıyla ölçülemeyeceğidir. Aydınlatma metinlerinin hazırlanmış olması, açık rıza süreçlerinin oluşturulması veya politika dokümanlarının yayımlanması tek başına yeterli görülmemekte; veri işleme sisteminin yapısal olarak hukuka aykırı kullanım ihtimalini önleyip önlemediği esas değerlendirme kriteri haline gelmektedir. Başka bir ifadeyle hukuka uygunluk, normatif beyanlardan ziyade sistemin işleyişi üzerinden ölçülmektedir. Bu yaklaşım, veri koruma yükümlülüğünü teorik uyum anlayışından çıkararak operasyonel gerçekliğe dayalı bir sorumluluk alanına taşımaktadır.

Sadakat programları özelinde yapılan değerlendirme, modern ticari faaliyetlerin veri üretim kapasitesinin ulaştığı boyutu da görünür kılmaktadır. Sadakat sistemleri artık yalnızca müşteri bağlılığını artıran pazarlama araçları olarak değerlendirilemez; bu sistemler aynı zamanda bireylerin davranışsal verilerini üreten, analiz eden ve ticari karar mekanizmalarına yön veren veri işleme altyapılarıdır. Bu nedenle sadakat programları, veri doğruluğu, kimlik doğrulama ve veri güvenliği rejiminin ayrılmaz bir parçası olarak ele alınmak zorundadır.

Bu çerçevede veri sorumluları bakımından uyum sürecinin niteliği de değişmektedir. İlke Kararı, uyum çalışmalarının yalnızca politika güncellemesi veya hukuki dokümantasyon revizyonu olarak ele alınamayacağını göstermektedir. Veri sorumlularının sadakat sistemlerini, kullanıcı akışlarını, doğrulama mekanizmalarını ve veri işleme süreçlerini bütüncül biçimde yeniden değerlendirmesi gerekmektedir. Başka bir ifadeyle uyum, artık hukuk departmanının yürüttüğü sınırlı bir faaliyet değil; bilgi teknolojileri, operasyon, pazarlama ve ürün geliştirme süreçlerini kapsayan kurumsal bir yeniden tasarım sürecidir.

Veri işleme faaliyetlerinin hukuka uygunluğu artık yalnızca “neyin işlendiği” sorusuyla değil, “nasıl işlendiği” sorusuyla değerlendirilmektedir. Bu dönüşüm, veri sorumlularını reaktif uyum anlayışından proaktif tasarım anlayışına yönlendirmekte ve veri koruma hukukunu işletmelerin teknolojik ve operasyonel karar süreçlerinin merkezine yerleştirmektedir. Dolayısıyla veri sorumluları açısından asıl mesele, mevcut sistemlerin mevzuata uyup uymadığını kontrol etmekten ziyade, veri işleme süreçlerini baştan itibaren hukuka uygun şekilde kurgulayabilmektir. Bu yaklaşımın benimsenmesi, yalnızca düzenleyici risklerin azaltılması bakımından değil, veri güvenine dayalı sürdürülebilir ticari ilişkilerin kurulması açısından da kaçınılmaz görünmektedir.

BOSCA
LAW



Telefon

03124739570 (pbx)

Email

info@bosca.av.tr

Web

www.bosca.av.tr

Adres

Tekstilciler cad. Sabri Mermutlu İş Merkezi Kat: 2
Balgat Çankaya/ANKARA