Kişisel Verileri Koruma Kurumu

BÜLTEN

Ocak - Nisan 2026 Sayı:11

10. YILINDA KİŞİSEL VERİLERİN KORUNMASI KANUNU

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Kişisel Verileri Koruma Kurumu
KVKK Bülten
www.kvkk.gov.tr
Sayı:11
Kişisel Verileri Koruma Kurumu
Adına İmtiyaz Sahibi
Prof. Dr. Faruk BİLİR

Yönetim Yeri
Nasuh Akar Mahallesi 1407. Sokak
No:4 Balgat Çankaya/ANKARA
Tel: (312) 216 50 00

GİRİŞ

Kişisel verilerin korunması, bireylerin temel hak ve özgürlüklerinin güvence altına alınması bakımından hukukun güncel ve öncelikli alanlarından biri haline gelmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin işlenmesi sürecinde ilgili kişilerin verileri üzerindeki kontrolünü güçlendiren ve veri sorumlularının yükümlülüklerini belirleyen temel bir düzenleme niteliği taşımaktadır.

Kanun, özel hayatın gizliliğinin ve mahremiyetin korunmasına katkı sağlamakta; bireylerin dijital ortamda daha güvenli bir şekilde varlık gösterebilmelerine zemin hazırlamaktadır. Bu yönüyle, veri işleme faaliyetlerinin hukuka uygun şekilde yürütülmesinde önemli bir rol üstlenmektedir.

Kanun'un yürürlüğe girmesinin 10. yılında, kişisel verilerin korunması alanında önemli ilerlemeler kaydedilmiştir. Bu sayımızda, Kanunla ilgili genel hususlar ile on yıllık uygulama sürecine genel bir bakış sunulmaktadır.

Tüm ilgililer için faydalı olmasını dileriz.

Hüseyin Can AKSOY
Doçent Doktor
Bilkent Üniversitesi Hukuk Fakültesi
hcaksoy@bilkent.edu.tr

VERİ ÇAĞINDAN ALGORİTMA ÇAĞINA: MAHREMİYETİN DÖNÜŞÜMÜ

2016 yılında Kişisel Verilerin Korunması Kanunu yürürlüğe girdiğinde, mahremiyetin korunmasına ilişkin tartışmalar büyük ölçüde kişisel verilerin elde edilme yöntemlerine, hukuka uygun şekilde kullanılmasına ve üçüncü kişilerle paylaşılmasına odaklanıyordu. E-posta adresleri, telefon numaraları ve sosyal medya paylaşımları bu tartışmanın merkezindeydi. Bu nedenle, hukuki değerlendirmeler de esas olarak kişisel verilerin kim tarafından, nasıl elde edildiği ve hukuka uygun şekilde işlenip işlenmediği soruları etrafında şekilleniyordu.

Bugün ise bambaşka bir çağdayız.

Son on yıl içinde kişisel veri türleri ve bu verilerin elde edilme kaynakları dikkate değer ölçüde çeşitlendi. Akıllı telefonlarımız aralıksız şekilde konumumuzu, günlük rutinlerimizi ve hangi uygulamaları ne kadar süreyle kullandığımızı kaydediyor. Saatlerimiz biz uyurken dahi kalp ritmimizi ve uyku düzenimizi ölçüyor. Hatta artık evlerimiz bile akıllı! Bağlı cihazlar evlerimizi adeta birer veri üretim merkezlerine dönüştürmüş durumda.

Ancak asıl değişim, veri miktarının artması değil. Asıl değişim, verilerin işlenme biçiminde yatıyor. Nitekim çoğu zaman farkında olmasak da artık kişisel verilerimiz yapay zekâ sistemleri vasıtasıyla işleniyor. Örneğin, kredi başvurularımızın değerlendirilmesinden, iş başvurularına kadar birçok konuda yapay zekâ sistemleri karar verici olarak görev alıyor. Hatta internette karşımıza hangi reklamın üstelik hangi anda çıkacağına kadar birçok soruya yapay zekâ karar veriyor.

Bu nedenle son on yıl "veri çağı" idiyse, önümüzdeki on yıl büyük ihtimalle "algoritma çağı" olacak.

Günümüzde yapay zekâ sistemleri sayesinde veriden yeni bilgiler üretilebiliyor ve çok çeşitli çıkarımlar yapılabiliyor. Zira bu sistemler, onlarla paylaştığımız verilerden yola çıkarak, artık yalnızca "ne yaptığımızı" değil, "ne yapma ihtimalimizin yüksek olduğunu" da tahmin ediyor. Davranışlarımız yalnızca kayıt altına alınmıyor; aynı zamanda öngörülebilir ve yönlendirilebilir hale geliyor.

Mahremiyet anlayışımız da bu dönüşüm karşısında değişmek zorunda. Nitekim mesele artık yalnızca kimliğimizin ifşa edilmesi ya da sırlarımızın açığa çıkması değil. Mesele, algoritmaların bizim hakkımızda yaptığı çıkarımların kişilik hakkımız ve bireysel özerkliğimiz yönünden doğuracağı sakıncaların önlenmesi! Zira bireyler hakkında üretilen algoritmik çıkarımlar, çoğu zaman bireyin kendisinin dahi farkında olmadığı veya kontrol edemediği bir bilgi katmanı yaratıyor. Kaldı ki, algoritmaların karar alma süreçleri, şeffaflık ve hesap verebilirlik bakımından hâlâ gri alanlarla dolu.

Peki yapay zekâ sistemleri hayatımızda daha fazla karar vermeye başladığında, bireysel özerklik nasıl korunacak? Mesela, bir çocuğun dijital dünyadaki davranışları yıllar boyunca analiz edilip bir "dijital kişilik" oluşturulduğunda, o çocuk gerçekten özgür seçimler yapabilecek mi? Bir çalışanın performansı sürekli veriyle ölçülüp algoritmik olarak değerlendirildiğinde, o çalışanın üretimde kullanılan bir makineden farkı kalacak mı? Sağlık verilerinden hareketle sigorta primleri dinamik biçimde belirlendiğinde, riskli görülen kişilerin sağlık sisteminin dışına itilmesi nasıl engellenecek?

Şüphesiz bu sorular yalnızca bireysel düzeyde değil, kolektif düzeyde de tartışılmalı. Zira dijital çağda mahremiyet giderek kolektif bir meseleye dönüşüyor: algoritmalar yalnızca bireyleri değil, grupları da sınıflandırıyor. Örneğin, belirli bir semtte oturan herkes ya da belirli bir yaş grubundaki tüm kişiler belirli bir açıdan "riskli" olarak etiketlenebiliyor. Çoğu durumda bireylerin farkında dahi olmadığı bu "görünmez" etiketler, krediye erişimden sigorta primlerine, iş fırsatlarından kamusal hizmetlere erişime kadar pek çok alanda son derece ağır sonuçlar doğurabiliyor. Bu bağlamda, algoritmik sınıflandırmalar yalnızca bireysel hakları değil, toplumsal eşitlik ve adalet ilkelerini de doğrudan ilgilendiriyor.

Önümüzdeki on yılda veri üretiminin artmaya devam edeceğine kesin gözüyle bakabiliriz. Keza, yapay zekâ sistemleri ve bunların çıkarım becerileri daha da gelişecektir. Haliyle, bu sistemlerin karar alma süreçlerine daha fazla entegre olması da kaçınılmaz bir hal alacaktır. Şüphesiz, bu gelişmelerin tümü hayatı kolaylaştırma potansiyeli taşıyor. Ancak bu dönüşüm, insanlar hakkında bilgi üretme ve onlar hakkında karar verme gücünün giderek daha az sayıda aktörün elinde toplanması riskini de beraberinde getirecektir. Bu düzen, bireylerin zaaflarının ve gelecekteki davranışlarının öngörülebildiği, kolaylıkla manipüle edildiği ve kimilerinin ise sistemin dışına itilebildiği mekanizmalar yaratabilecektir.

Tam da bu nedenle, bireyin davranışlarının giderek daha öngörülebilir ve yönlendirilebilir hâle geldiği bu yeni çağda mahremiyeti, yalnızca kişisel verilerin toplanması ve paylaşılması meselesi olarak ele almak yanlış olur. Zira bu çağda başlıca ihtiyacımız, bireyin dijital dünyada sürekli analiz edilen, sınıflandırılan ve hakkında çıkarımlar üretilen bir veri nesnesine dönüşmemesi olacaktır. Veri koruma hukuku da önümüzdeki yıllarda, verilerden üretilen çıkarımların yarattığı güç ilişkileriyle giderek daha fazla ilgilenmek zorunda kalacaktır.

TÜRKİYE'DE VERİ KORUMANIN TARİHSEL GELİŞİMİ

Dijitalleşmenin hız kazandığı günümüzde, bireylerin kimliğini, mahremiyetini ve özgürlük alanını doğrudan ilgilendiren en önemli konulardan biri kişisel verilerin korunmasıdır. Teknolojik gelişmeler, bilgiye erişimi kolaylaştırırken aynı zamanda bireylerin özel hayatına müdahale riskini de artırmıştır. Bu durum, kişisel verilerin korunmasını yalnızca teknik bir mesele olmaktan çıkarıp hukuki, etik ve toplumsal bir gereklilik haline getirmiştir. Ülkemizde veri koruma anlayışının gelişimi de bu dönüşümün bir yansıması olarak şekillenmiştir.

Anayasal Güvence

Ülkemizde kişisel verilerin korunmasına ilişkin yolculuğun en güçlü dayanağı, anayasal güvence ile başlamaktadır. Anayasamızın ikinci kısmında düzenlenen kişinin hakları ve ödevleri arasında yer alan "özel hayatın gizliliği", bireyin dokunulmaz alanını koruma altına alan temel haklardan biridir. Bu hak, özellikle teknolojinin birey üzerindeki etkisinin artmasıyla birlikte daha da kritik bir hale gelmiştir.

2010 yılında 5982 sayılı Kanun ile yapılan Anayasa değişikliği, veri koruma alanında bir dönüm noktası olmuştur. Anayasa'nın 20. maddesine eklenen fıkra ile kişisel verilerin korunmasını isteme hakkı açıkça tanınmış ve anayasal güvence altına alınmıştır. Bu düzenleme ile herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu hükme bağlanmıştır.

Bu hak yalnızca genel bir koruma talebinden ibaret değildir; aynı zamanda bireylere önemli yetkiler tanımaktadır.

- Buna göre bireyler:
- Kendileriyle ilgili kişisel veriler hakkında bilgilendirilme,
- Bu verilere erişme,
- Verilerin düzeltilmesini veya silinmesini talep etme,
- Verilerin amacına uygun kullanılıp kullanılmadığını öğrenme haklarına sahiptir. Ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ifade edilmiştir. Bu yaklaşım, bireyi merkeze alan ve veri üzerinde kontrol sahibi olmasını sağlayan modern veri koruma anlayışının temelini oluşturmuştur.

Kanuni Çerçevenin Oluşumu

Ülkemizde kişisel verilerin korunmasına yönelik özel bir kanunun hazırlanması süreci oldukça uzun ve aşamalı olmuştur. İlk girişimler 1989 yılına kadar uzanmakta olup, bu tarihte oluşturulan komisyon çalışmalarını tamamlayamadan dağılmıştır. 2000 yılında kurulan yeni bir komisyon ise kapsamlı bir tasarı hazırlamış, ancak bu tasarı da yasama sürecinin tamamlanamaması nedeniyle kanunlaşamamıştır.

2008 ve 2014 yıllarında Adalet Bakanlığı öncülüğünde hazırlanan tasarıların Türkiye Büyük Millet Meclisine sunulmasına rağmen yasama döneminin sona ermesi nedeniyle bu girişimler de sonuçsuz kalmıştır.

Nihayetinde 26 Aralık 2014 tarihinde TBMM'ye sunulan "Kişisel Verilerin Korunması Kanunu Tasarısı", 24 Mart 2016 tarihinde kabul edilerek kanunlaşmış ve 7 Nisan 2016 tarihinde yürürlüğe girmiştir. Böylece ülkemizde veri koruma alanında kapsamlı bir yasal çerçeve oluşturulmuştur.

Veri Korumada Yeni Dönem: 6698 Sayılı Kişisel Verilerin Korunması Kanunu

6698 sayılı Kişisel Verilerin Korunması Kanunu, ülkemizde veri koruma alanında bir milat niteliği taşımaktadır. Bu Kanun ile birlikte kişisel verilerin işlenmesine ilişkin temel ilkeler belirlenmiş, veri sorumlularının yükümlülükleri tanımlanmış ve bireylerin hakları detaylandırılmıştır.

Kanun, kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesini, doğru ve gerektiğinde güncel tutulmasını, belirli, açık ve meşru amaçlarla işlenmesini ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmasını temel ilke olarak benimsemiştir. Ayrıca verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerektiği ifade edilmiştir.

Bu düzenleme ile birlikte veri işleme faaliyetleri belirli kurallara bağlanmış, keyfiliğin önüne geçilmiş ve bireylerin verileri üzerindeki kontrolü güçlendirilmiştir. Aynı zamanda Kanunda, özel hukuk tüzel kişileri ile kamu hukuku tüzel kişileri bakımından bir ayrım yapılmamış olup Kanunda öngörülen usul ve esasların hem özel kuruluşlar hem de kamu kuruluşları bakımından uygulanması öngörülmüştür.

Ceza Hukuku Boyutu

Kişisel verilerin korunması yalnızca idari düzenlemelerle sınırlı kalmamış, aynı zamanda ceza hukuku kapsamında da güvence altına alınmıştır. 5237 sayılı Türk Ceza Kanunu, kişisel verilerin korunmasına yönelik suç tiplerini düzenleyerek bu alanda caydırıcılığı artırmıştır.

TCK'nın:

135. maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi,
136. maddesinde verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi,
138. maddesinde ise verilerin yok edilmemesi suç olarak tanımlanmıştır. Ayrıca 140. maddede, bu suçlar kapsamında tüzel kişilere özgü güvenlik tedbirleri uygulanacağı hüküm altına alınmıştır.

Bu düzenlemeler, kişisel verilerin korunmasının yalnızca bir hak değil, aynı zamanda ihlali halinde ciddi yaptırımları olan bir yükümlülük olduğunu ortaya koymaktadır.

Günümüzde Veri Koruma: Süreklilik ve Gelişim

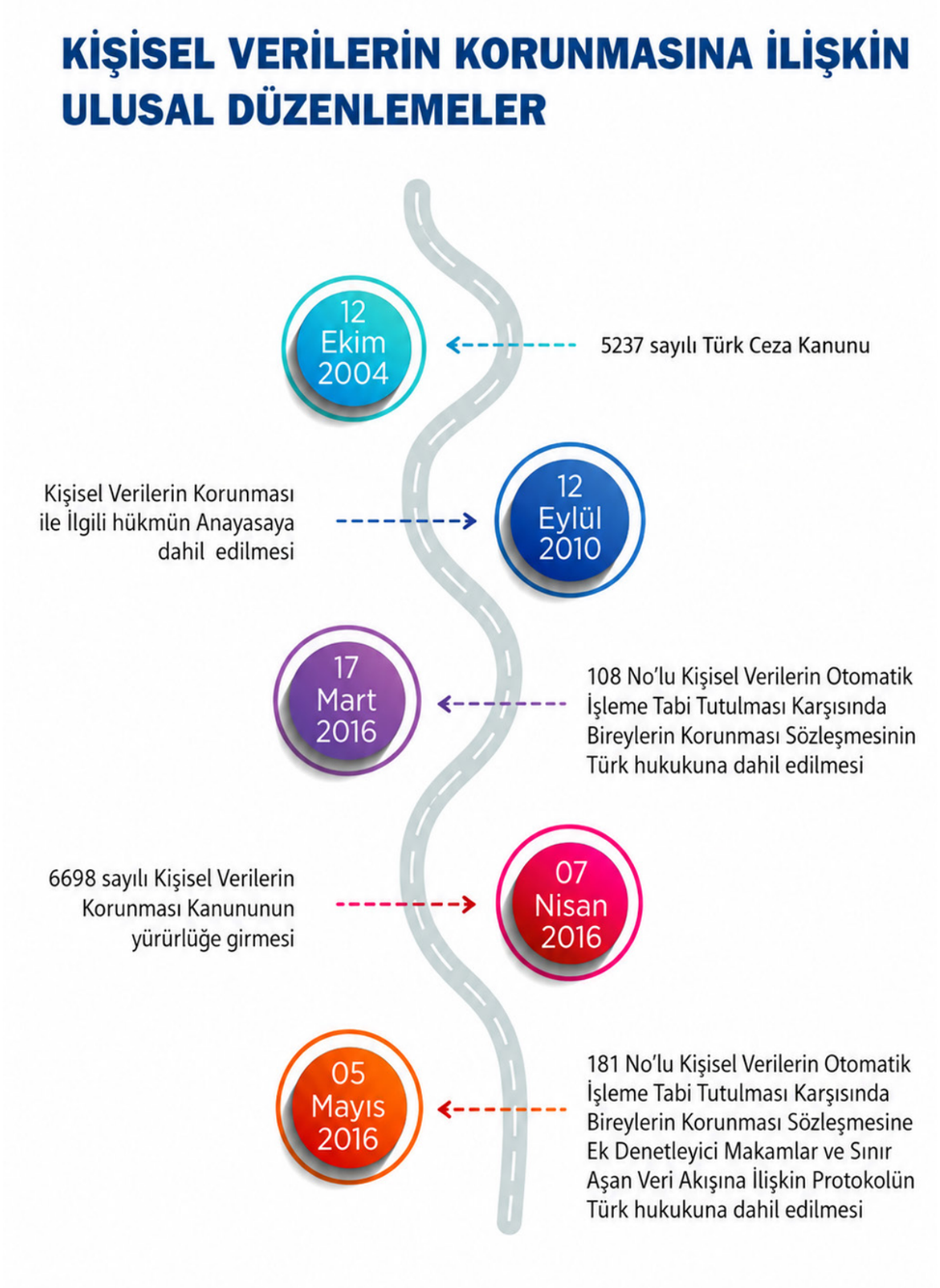
Ülkemizde veri koruma alanında atılan adımlar, sadece ulusal ihtiyaçların değil, aynı zamanda küresel gelişmelerin de bir sonucudur. Özellikle dijital ekonominin büyümesi, yapay zekâ uygulamalarının yaygınlaşması ve sınır ötesi veri akışlarının artması, veri koruma konusunu daha da önemli hale getirmiştir.

Bugün gelinen noktada, kişisel verilerin korunması yalnızca hukuki bir zorunluluk değil; aynı zamanda güven, şeffaflık ve kurumsal itibarın temel unsurlarından biri olarak görülmektedir. Bireylerin bilinçlenmesi, şirket, kurum ve kuruluşların sorumluluklarını yerine getirmesi ve teknolojinin etik ilkeler çerçevesinde kullanılması, bu sürecin hukuka uygun şekilde ilerlemesi açısından son derece önemlidir.

Ülkemizde veri korumanın yolculuğu, anayasal bir hak olarak tanınmasından başlayıp kapsamlı bir yasal çerçevenin oluşturulmasına kadar uzanan çok boyutlu bir süreçtir. Bu süreç, hem bireyin mahremiyetini koruma hem de dijital dünyanın sunduğu fırsatları güvenli bir şekilde değerlendirme çabasının bir yansımasıdır.

Gelecekte veri koruma alanında daha ileri adımların atılması muhtemeldir. Ancak bu yolculuğun en önemli unsuru, bireyin merkezde olduğu ve verinin insan onuruna saygı çerçevesinde işlendiği bir anlayışın sürdürülebilir kılınmasıdır. Çünkü kişisel veri, bir bilgi olmanın ötesinde, insanın kendisine dair izler taşımakta ve bireyin kimliğini yansıtmaktadır.

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ULUSAL DÜZENLEMELER



KİŞİSEL VERİLERİN KORUNMASI KANUNU'NUN GETİRDİKLERİ

Kişisel verilerin korunması, bireyin temel hak ve özgürlüklerinin etkin biçimde güvence altına alınmasını amaçlayan ve hukuk devleti ilkesinin somut görünümlerinden birini oluşturan normatif bir düzenleme alanıdır. Türkiye'de bu ihtiyaca yanıt olarak kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin işlenmesine ilişkin usul ve esasları düzenleyerek önemli bir hukuki çerçeve oluşturmuştur.

Kanunun en önemli getirilerinden biri; hukuka ve dürüstlük kurallarına uygunluk, belirli ve meşru amaçlarla işlenme ile ölçülülük gibi temel ilkelerin net bir şekilde ortaya konulmasıdır. Kanunun getirdiği bir diğer önemli yenilik, kişisel veri işleme faaliyetlerinin hukuki sebeplere bağlanmasıdır. Kişisel verilerin işlenebilmesi için ilgili kişinin açık rızasının varlığı bir dayanak olarak kabul edilmekle birlikte, Kanunda diğer hukuka uygunluk sebepleri de düzenlenmiştir. Böylece veri işleme faaliyetleri, yalnızca rızaya dayalı bir sistemden çıkarılarak daha geniş ve sistematik bir hukuki zemine oturtulmuştur. Bu yaklaşım, hem kamu hizmetlerinin sürekliliği hem de özel sektör faaliyetlerinin hukuka uygun şekilde yürütülmesi açısından önem taşımaktadır.

Açık rızanın kapsamı da Kanun ile birlikte daha net bir çerçeveye kavuşturulmuştur. Açık rızanın belirli bir konuya ilişkin olması, bilgilendirmeye dayanması ve özgür iradeyle açıklanması gerektiği hüküm altına alınarak, uygulamada ortaya çıkabilecek belirsizliklerin önüne geçilmesi amaçlanmıştır. Bu düzenleme, verisi işlenen kişilerin iradelerinin korunmasını ve bilinçli karar verme süreçlerinin güçlendirilmesini hedeflemektedir.

Kurumsal yapı açısından değerlendirildiğinde, Kişisel Verileri Koruma Kurumu'nun kurulması Kanun'un en önemli yapısal unsurlarından birini oluşturmaktadır. Bu çerçevede Kurumun hem idari yaptırım uygulama yetkisi hem de düzenleyici ve rehberlik rolü, veri koruma sisteminin etkinliğini artıran unsurlar olarak değerlendirilmektedir.

Kanunun önemli bir diğer boyutu, veri sorumlularına getirilen yükümlülüklerdir. Veri güvenliğinin sağlanması, teknik ve idari tedbirlerin alınması, ilgili kişilerin aydınlatılması, temel ilkelere ve veri işleme şartlarına uyum sağlanması gibi yükümlülükler, bu yükümlülüklerin bütüncül bir yaklaşımla ele alınması gerektiğini göstermektedir. Bu durum, kişisel veri koruma rejimini yalnızca bireysel haklara indirgememekte; aynı zamanda kurumsal yönetişim ve uyum mekanizmalarının da bir parçası haline getirmektedir.

Öte yandan Kanun, toplumsal farkındalığın artmasına da katkı sağlamıştır. Bireylerin dijital ortamlarda paylaştıkları veriler konusunda daha bilinçli hale gelmeleri, veri mahremiyetine ilişkin bireysel tedbirlerin öneminin gündeme gelmesi, bu dönüşümün somut göstergeleri arasında yer almaktadır.

Sonuç olarak Kişisel Verilerin Korunması Kanunu, Türkiye'de veri koruma hukukunun temelini oluşturan kapsamlı bir düzenleme niteliği taşımaktadır. Kanun, bireyin kişisel verileri üzerindeki kontrolünü güçlendiren, veri işleme faaliyetlerini hukuki ilkelere bağlayan ve kurumsal denetim mekanizmalarını tesis eden çok boyutlu bir yapı ortaya koymaktadır.

Bu yönüyle Kanun, yalnızca hukuki bir metin değil; aynı zamanda bireyin mahremiyetini güvence altına alması bakımından ülkemiz adına önemli bir hukuki kazanım teşkil etmektedir.

6698 sayılı Kanun ile Veri Sorumlularına Getirilen Yükümlülüklerden Bazıları

- Temel İlkelere ve Veri İşleme Şartlarına Uyum
- Aydınlatma Yükümlülüğü
- Veri Güvenliğine İlişkin Yükümlülükler
- Gerçekleşmesi Halinde Veri İhlalinin İlgilisine ve Kurula Bildirilmesi
- Veri Sorumluları Siciline Kayıt ve Bildirim Yükümlülüğü
- İşlenmesini Gerektiren Sebeplerin Ortadan Kalkması Halinde Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi
- İlgili Kişiler Tarafından Yapılan Başvuruların Cevaplanması ve Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü

6698 sayılı Kanun ile Bireylere Tanınan Haklar

Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- Kanun'un 7'nci maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- Düzeltme, silme ve yok etme işlemlerinin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.

6698 SAYILI KANUN KAPSAMINDA HAK ARAMA YÖNTEMLERİ

6698 sayılı Kişisel Verilerin Korunması Kanunu, ilgili kişilerin bu Kanunun uygulanmasına ilişkin taleplerini iletebilmeleri ve kişisel verilerine ilişkin haklarını korumaları için birtakım hak arama yöntemleri getirmiştir. Böylelikle kişiler, verilerinin korunmasına ilişkin haklarını kullanmak adına doğrudan yargı yoluna başvurmanın yanı sıra 6698 sayılı Kanunla getirilen diğer hak arama yöntemlerini de kullanabilmektedir. Kanun ile getirilen hak arama yöntemlerinden ilki Kanunun 13. Maddesinde düzenlenen veri sorumlusuna başvuru yöntemidir. İkincisi ise Kanunun 14. ve 15. maddelerinde düzenlenen Kurula şikâyettir.

Veri Sorumlusuna Başvuru

6698 sayılı Kanun, kişisel verilerin korunması kapsamındaki başvurular için kademeli bir başvuru usulü öngörmüştür. İlgili kişilerin, sahip oldukları hakları kullanabilmeleri için öncelikle veri sorumlusuna başvurmaları zorunludur. Bu yol tüketilmeden Kurula şikâyet yoluna gidilemez.

İlgili kişinin talebinin, talebin niteliğine göre en kısa sürede ve en geç 30 gün içerisinde veri sorumlusu tarafından cevaplandırılması gerekmektedir.

Başvurusu reddedilen veya verilen cevabı yetersiz bulan yahut süresinde başvurusuna cevap verilmeyen ilgili kişiler Kurul'a şikâyet hakkını kullanabilecektir.

Ayrıca 6698 sayılı Kanun'da, kişilik hakları ihlal edilen ilgili kişilerin genel hükümlere göre tazminat hakları saklı tutulmuştur. Başvuru yoluna gitmenin zorunlu, şikâyet yoluna gitmenin ise ihtiyari olması sebebiyle, başvurusu dolaylı olarak veya açıkça reddedilen ilgili kişinin bir yandan Kurul'a şikâyette bulunabilmesi, diğer yandan doğrudan yargı yoluna gidebilmesi mümkün olacaktır. Ancak bu noktada belirtmek gerekir ki; ilgili kişilerin hak ihlallerine yönelik olarak doğrudan yargı organlarına başvurmalarının önünde herhangi bir engel bulunmamaktadır.

Başka bir ifadeyle; konunun yargıya intikal ettirilmesinden önce, veri sorumlusuna başvuru zorunluluğu bulunmamaktadır. Veri sorumlusuna doğrudan başvurulması sadece konunun Kurul'a iletilmesinden önce uyulması gereken bir zorunluluktur.

Başvuru ve Cevap Yöntemine İlişkin Kurallar

Veri sorumlusuna yapılacak başvuruların şekli konusunda 6698 sayılı Kanun'da iki temel hüküm bulunmaktadır ve bunlardan ilki yazılı başvurudur. Yazılı başvuru, genel hükümler gereğince ıslak imza içeren belge ile yapılan başvuru anlamına gelmektedir. Buna ek olarak güvenli elektronik imza ile imzalanan belgeler de yazılı şekil şartını sağlayacaktır. Yazılı başvuru haricindeki diğer başvuru yöntemlerinin belirlenmesi konusunda 6698 sayılı Kanun, Kurul'u yetkilendirmektedir ve buna istinaden Kurul tarafından 10.03.2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ ile veri sorumlusuna yapılacak başvuruların yöntemleri belirlenmiştir.

Buna göre veri sorumluları, ilgili kişiler tarafından yazılı olarak veya bahse konu Tebliğ'de yer verilen kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla yapılan başvuruları, niteliklerine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmalıdır.

Veri sorumlusu, kural olarak kendisine yöneltilen talepleri en kısa sürede cevaplandırmak zorundadır ancak bu süre en fazla 30 gün ile sınırlandırılmıştır. Veri sorumlusu, kendisine yöneltilen talepleri kabul edebileceği gibi gerekçesini açıklayarak reddedebilir. Ret kararının gerekçeli olmasının mecburi tutulması suretiyle ilgili kişilerin haklarının daha etkili korunması hedeflenmektedir. Zira ret kararının gerekçeli olması zorunluluğu, veri sorumlularının ret kararlarına ilişkin mutlaka bir hukuki gerekçe göstermeleri gerekliliğini beraberinde getirmektedir.

Veri sorumlusu kendisine yöneltilen talebi kabul etmesi halinde, talebin gereklerini derhal yerine getirmek zorundadır. Talebin kabul edilmesine rağmen gereklerinin yerine getirilmemesi halinde, veri sorumlusunun talebi reddettiğini varsaymak gerekir. Zira 6698 sayılı Kanun, sadece veri sorumlusunun ilgili kişinin başvurusunu reddetmesi, verdiği cevabın yetersiz bulunması ya da süresinde cevap vermemesi hallerinde ilgili kişiye Kurul'a şikâyette bulunma hakkı vermektedir. Bu durum, ilgili kişinin Kurul'a şikâyette bulunmasına imkân vermek açısından önemli bir konudur.

6698 sayılı Kanun, veri sorumlusunun kendisine yapılan başvurulara dair kararını bildirmesine ilişkin izlenebilecek yöntem konusunda yazılı bildirim ya da elektronik ortamda bildirim hükümlerine yer vermiştir. Dolayısıyla ilgili kişi tarafından, veri sorumlusuna gerek yazılı olarak gerek Kurul'un belirleyeceği diğer yöntemlerle başvurulduğunda, veri sorumlusunun cevabı mutlaka ya yazılı olarak ya da elektronik ortamda gönderilmelidir. Kendisine başvuru yapılan veri sorumlusunun, kamu kurum ya da kuruluşu olması hali üzerinde özellikle durulması gerekmektedir. Zira kamu kurum ve kuruluşlarının yapacağı bildirimler 7201 sayılı Tebligat Kanunu ile düzenlenmektedir. Tebligat Kanunu'nun da elektronik tebligata imkân verdiği göz önüne alındığında, kamu kurum ve kuruluşu olan veri sorumlularının da ilgili mevzuata uyarak hem yazılı hem elektronik ortamda bildirimde bulunabilmeleri mümkün olacaktır.

Kurula Şikâyet

Veri sorumlusuna başvurusu reddedilen, verilen cevabı yetersiz bulan veya süresinde başvurusuna cevap verilmeyen ilgili kişiler Kurul'a şikâyet hakkını kullanabilecektir.

Kişisel Verileri Koruma Kurulu'nun İnceleme Yapması

6698 sayılı Kanun'un 15. maddesi gereğince ihlal halinde Kurul'un inceleme yapma yetkisi bulunmaktadır. Kurul bu yetkisini, şikâyet üzerine ya da resen kullanabilmektedir.

Resen İnceleme: Kurul'un inceleme başlatma konusunda resen yetkili olması, Kurul'un haberdar olduğu bir ihlal durumunda kendiliğinden harekete geçerek inceleme başlatabileceği anlamına gelmektedir. Diğer bir ifadeyle; Kurul'un inceleme başlatabilmesi için kendisine şikâyette bulunulmasına ihtiyaç yoktur. Bu durum, ilgili kişilerin şikâyette bulunmamasına ve hatta ilgili kişilerin ihlalden haberlerinin dahi olmamasına rağmen Kurul'un hak ihlallerini engelleyebilmesini sağlamaktadır. Dolayısıyla ilgili kişilerin hakları daha etkin bir şekilde korunabilmektedir. Kurul'un inceleme başlatmaya resen yetkili oluşunun bir diğer sonucu da kendisine gelen ihbarları değerlendirme ve gerekiyorsa inceleme başlatma yetkisine sahip olmasıdır.

Şikâyet Üzerine İnceleme: İlgili kişilerin haklarını kullanması için öncelikle veri sorumlularına başvurmaları zorunludur. Veri sorumlusunun bu başvuruyu reddetmesi, verdiği cevabın yetersiz olması veya süresinde cevap vermemesi halinde ilgili kişinin konu hakkında Kurul'a şikâyette bulunma hakkı doğmaktadır. Yapılacak şikâyet ile konu, Kurul'a taşınmakta ve Kurul'un incelemesi sonucunda karara bağlanmaktadır.

KİŞİSEL VERİLERİN KORUNMASI KANUNU'NDA 2024 YILINDA YAPILAN DEĞİŞİKLİKLERİN UYGULAMAYA YANSIMALARI

Bilindiği üzere, 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'la (8. Yargı Paketi) 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6'ncı, 9'uncu ve 18'inci maddeleri yeniden düzenlenmiştir. Bu kapsamda söz konusu değişikliklerin yürürlüğe girdiği 1 Haziran 2024 tarihinden bu yana Kanun uygulamasında görülen gelişmelere aşağıda yer verilmiştir.

Madde 6 - Özel Nitelikli Kişisel Verilerin İşlenme Şartları

Düzenlemenin önceki hâlinde sağlık ve cinsel hayata ilişkin veriler ile diğer özel nitelikli kişisel veri kategorileri bakımından farklı işleme şartları öngörülmekteydi. Kanunlarda öngörülen hâllerde diğer özel nitelikli kişisel verilerin işlenmesi mümkünken kişisel sağlık verileri bakımından böyle bir işleme şartı bulunmamaktaydı.

Bununla birlikte kişisel veriler, her geçen gün artan bir biçimde iş süreçlerine dahil edilmekte, kamu hizmetlerinin sunumu iyileştirilmektedir. Kişisel veri işleme faaliyetlerinin kapsamının genişlemesi, yeni teknolojilerin ortaya çıkardığı farklı uygulama alanları ve uluslararası veri koruma standartlarındaki gelişmeler, mevcut düzenlemelerin uygulamadaki karşılığının gözden geçirilmesini gerekli hale getirmiştir. Bu çerçevede, Kanun'un temel yaklaşımı ve koruma amacı korunarak, uygulamada ortaya çıkan ihtiyaçlara daha etkin yanıt verebilmek amacıyla bazı düzenlemelerin güncellenmesi gündeme gelmiştir.

Bu itibarla, yapılan değişiklikle işleme şartları bakımından özel nitelikli kişisel veri kategorileri arasındaki ayrım kaldırılmış ve Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GVKT) yer alan hükümler ile uygulamada karşılaşılan eksiklikler dikkate alınarak yeni işleme şartları getirilmiştir.

Madde 9 - Kişisel Verilerin Yurt Dışına Aktarılması

Değişiklik öncesinde Kişisel Verileri Koruma Kurulu (Kurul) tarafından verilmiş bir yeterlilik kararı yokluğunda, ilgili kişinin açık rızasının alınması haricinde yalnızca içeriği Kurul tarafından belirlenen taahhütnamelerin taraflarca imzalanması ve Kurul tarafından izin verilmesi suretiyle kişisel veriler yurt dışına aktarılabilmekteydi. Ayrıca, küreselleşmenin etkisiyle ortaya çıkan yeni iş modelleri ve bununla birlikte farklılaşan iş ilişkileri sonucunda daha karmaşık işleme faaliyetlerinin yaygın olarak yürütülmesi ile dijital ekonomi alanında yaşanan gelişmeler dikkate alındığında veri işleyenler tarafından da kişisel verilerin yurt dışına aktarılabilmesi mümkündür. Dolayısıyla, veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırabilmek adına kişisel verilerin yurt dışına aktarımı düzenlemelerinde birtakım iyileştirmeler yapılması ihtiyacı ortaya çıkmıştır. Yeni aktarım rejimi, GVKT ile uyumlu olacak şekilde üç aşamalı olarak tasarlanmıştır:

1. Yeterlilik kararının bulunması durumunda kişisel veriler yurt dışına aktarılabilecektir.
2. Yeterlilik kararının bulunmaması durumunda Kanun'da öngörülen uygun güvencelerden birinin sağlanması kaydıyla kişisel veriler yurt dışına aktarılabilecektir.
3. Hem yeterlilik kararının bulunmaması hem de uygun güvencelerin sağlanamaması durumunda ise Kanun'da sınırlı olarak düzenlenen istisnai hâllerden birinin varlığı ve arızi olmak kaydıyla kişisel veriler yurt dışına aktarılabilecektir.

Yapılan değişiklik neticesinde temel hak ve özgürlükleri güvence altına alan, alternatif, kolaylaştırılmış ve maliyetsiz yollar öngören bir hukuki çerçeve oluşturulmuştur. Bu bağlamda uygun güvence sağlama yolu olarak standart sözleşmeler, kişisel verilerin yurt dışına aktarılmasına yönelik pratik bir araç olarak ön plana çıkmıştır. Aktarım tarafları, içeriği Kurul tarafından belirlenen standart sözleşmeleri imzalamaları hâlinde kişisel veriler yurt dışına aktarılabilmektedir. Değişiklik öncesindeki taahhütname uygulamasından farklı olarak Kurul'un izni aranmamakta olup Kurum'a bildirim yapılması yeterli kılınmıştır. Bu çerçevede, veri sorumlularını ve veri işleyenleri uyuma teşvik edici bir veri aktarım sistemi yürürlüğe konulmuştur.

Madde 18 - Kabahatler

Değişiklik öncesinde, Kurul tarafından verilen idari para cezası kararlarına karşı sulh ceza hakimliklerine başvuru yapılmaktaydı. Yapılan değişiklik sonrasında ise bu kararlara karşı idari yargıya başvuru imkânı sağlanmıştır. Böylelikle Kurul kararları daha etkin bir yargısal denetime tabi olmuştur. Belirtmek gerekir ki söz konusu değişiklik, 2. İnsan Hakları Eylem Planı'nın hedefleri arasında da yer almaktadır.

Diğer taraftan, yeni bir kabahat ihdas edilmiştir. Kişisel verilerin yurt dışına aktarımında standart sözleşme uygun güvence sağlama yoluna başvurulması hâlinde Kurum'a 5 iş günü içinde bildirim yapılması zorunlu tutulmuştur. Böylelikle, Kurum tarafından yurt dışına aktarılan kişisel verilere yönelik bir takip mekanizması oluşturularak ilgili kişilerin ülkemizde yararlandığı korumadan kişisel verilerinin yurt dışına aktarılması suretiyle mahrum kalmaması amaçlanmıştır.

DİJİTAL DÜNYADA ÇOCUKLARIN KİŞİSEL VERİLERİNİN KORUNMASI

Dijitalleşmenin hız kazandığı günümüzde çocukların internet kullanımı giderek artmaktadır. Türkiye İstatistik Kurumu verilerine göre, 6-15 yaş grubundaki çocukların internet kullanım oranı 2021 yılında %82,7 iken, bu oran 2024 yılında %91,3'e yükselmiştir. Özellikle çevrim içi oyun, sosyal medya, video izleme, mesajlaşma, eğitim vb. alanlardaki platform ve uygulamaların yaygınlaşmasıyla birlikte çocuklar çok erken yaşlardan itibaren dijital dünyada yer almaya başlamıştır.

Çocuklar için internet; bilgiye kolay erişim sağlanması, öğrenme süreçlerinin desteklenmesi ile eğlence, iletişim kurma ve sosyalleşme ihtiyaçlarının karşılanması gibi çok sayıda fayda sunmaktadır. Bununla birlikte, çocukların internet kullanımı çocuklara ait ad, soyad, fotoğraf, konum bilgisi, ilgi alanları, IP adresi ve çevrim içi davranışlarına ilişkin bilgiler gibi pek çok kişisel verinin çeşitli amaçlarla işlenmesi sonucunu doğurmaktadır. Dijital mecralarda gerçekleştirilen söz konusu kişisel veri işleme faaliyetleri, çocukların kişisel veri güvenliğini ve mahremiyetini tehlikeye atma riski taşımaktadır. Zira çocuklar, yetişkinlere kıyasla, kişisel veri işleme faaliyetlerinin kapsamını, kişisel verilerinin işlenmesine ilişkin haklarını ve bu işlemenin doğurabileceği sonuçları tam olarak kavrayacak olgunluğa sahip olmayabilirler. Bu nedenle, çocukların interneti bilinçli ve güvenli şekilde kullanmalarını sağlamak ve çevrim içi ortamda kişisel verilerini korumak amacıyla ebeveynler tarafından alınacak olan önlemler büyük önem taşımaktadır.

Bu doğrultuda, Kurumumuz tarafından çocukların kişisel verilerinin korunması konusunda farkındalığın artırılması ve ebeveynlerin bu hususta bilinçlendirilmesine katkı sağlanması amacıyla yetişkinler tarafından dikkat edilmesi gerekenlere yönelik dökümanlar hazırlanmıştır. Bahse konu dokümanlarda yetişkinlere yönelik;

- Çocukların, kişisel veri, çevrimiçi mahremiyet, istenmeyen (spam) ve önemsiz (junk) elektronik postalar gibi konular hakkında bilgilendirilmesi,
- Çocukların çevrim içi aktivitelerine dâhil olunması ve onların çevrim içi güvenlik hakkında bilgilendirilmesi,
- Çocukların, kişisel verilerinin istemedikleri kişilerce kullanılmaması için çevrim içi ortamlarda veri paylaşmamaları gerektiği konusunda bilgilendirilmesi,
- Çocukların, çevrim içi ortamlardaki kişilerin gerçek kimlikleri hakkında yalan söylüyor olabilecekleri konusunda bilgilendirilmesi ve yeni biriyle tanışma veya buluşma kararı almadan önce mutlaka yetişkinlerinden izin almaları gerektiğini bilmelerinin sağlanması,
- Kişisel veri işleyen ürün ve hizmetleri kullanmadan önce bilgilendirici metinlerin (aydınlatma metni, gizlilik politikası, kullanıcı şartları, çerez politikaları vb.) bulunup bulunmadığının kontrol edilmesi ve dikkatli şekilde okunması,
- Tarayıcının gizlilik ayarlarının kontrol edilmesi ve ön tanımlı olarak gelen ayarların değiştirilmesi,
- Yeni bir uygulama kurulduğunda, uygulamaya hangi izinlerin verildiğinin ve uygulamanın cihazdaki(akıllı telefon, tablet vb.) hangi bilgilere erişebildiğinin farkında olunması,
- Çocukların kişisel verilerinin ve özellikle fotoğraflarının çevrim içi ortamlarda herkese açık bir şekilde paylaşılmaması,
- Güvenli şifreler kullanılması ve çocuklara bu yönde tavsiyelerde bulunulması,
- Çocuğun kişisel verilerine sınırlı ve tanıdığı bir çevre tarafından ulaşılması için sosyal medya hesabının gizli/onaya tabi olmasının sağlanması,
- Sosyal medya kullanımı sırasında gerekli olmadıkça kamera kapağının ve mikrofonun kapalı olması,
- Çocuk adına sahte hesap/profil açılıp açılmadığı ve burada çocuğun kişisel verilerinin izinsiz paylaşılıp paylaşılmadığının kontrol edilmesi,
- Çocuğun, başkası adına hesap açma/profil oluşturma ve başkalarının verilerini izinleri olmadan paylaşma gibi konuların uygun olmadığı konusunda bilgilendirilmesi,
- Çevrim içi ortamlarda yer alan tehlikelerin gerçek dünyadaki tehlikelerden farklı olmadığının, hatta çevrim içi ortamların bazen daha ciddi tehlikeler arz edebileceğinin bilincinde olunması,
- Çocukların sosyal medya kullanmaları durumunda, uygun gizlilik ayarlarının kullanıldığından emin olunması,
- Çocukların kişisel verilerine internet bağlantılı oyuncaklar, oyun konsolları, akıllı televizyonlar, saatler vb. üzerinden de erişilebileceği, ayrıca ortak cihaz kullanımında tehlikenin yetişkinlere de yöneldiğinin farkında olunması,
- Çocukların sahip olduğu veya kullandığı bilgisayar, cep telefonu veya oyun konsolları için internet filtreleme ve izleme yazılımı kullanabileceği

hususlarında tavsiyelere yer verilmektedir.

KİŞİSEL VERİLERİN KORUNMASINDA VERİ KORUMA OTORİTELERİNİN ROLÜ: KVKK ÖRNEĞİ

Kişisel verilerin korunmasına ilişkin çağdaş hukuki düzenlemelerin neredeyse hepsinde uygulamada "*veri koruma otoritesi*" olarak adlandırılan denetleyici makamların kurulması öngörülmektedir. Veri koruma yasalarında yer alan ilkeler ile usul ve esaslara uyumu denetleme hususunda genellikle tek bir veri koruma otoritesi görevli kılınmaktadır. Bununla birlikte, ilgili ülkenin hukuk sistemine bağlı olarak Almanya Federal Cumhuriyeti'nde olduğu gibi farklı coğrafi alanlarda yetkili olacak şekilde birden çok veri koruma otoritesinin faaliyet gösterdiği örnekler de mevcuttur.

Kişisel verilerin korunmasını bir temel hak olarak tanıyan bazı hukuk düzenlerinde bu hakkın kullanımı ve korunmasıyla bağlantılı olarak bağımsız bir kamu otoritesinin kurulması da ayrıca anayasal düzeyde hükme bağlanmaktadır. Örneğin Avrupa Birliği Temel Haklar Şartı'nın "Kişisel verilerin korunması" başlıklı 8. maddesinde,

1. Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir.
2. Bu tür veriler, belirtilen amaçlar için ve ilgili kişinin rızasına veya yasada öngörülen başka bir meşru dayanak temelinde adil şekilde işlenmelidir. Herkes, kendisiyle ilgili toplanmış verilere erişme ve bunların düzeltilmesini isteme hakkına sahiptir.
3. Bu kurallara uyum, bağımsız bir makamın denetimine tabi olacaktır.

düzenlemesine yer verilmiştir. Böylelikle, kişisel verilerin korunmasına yönelik olarak bireylere sağlanan güvencelerin Üye Devletler nezdinde bağımsız bir makam tarafından kontrol edilmesi zorunlu tutulmuştur. Bu minvalde Avrupa Birliği (AB), kişisel verilerin aktarımı bağlamında bir ülkenin yeterli koruma düzeyine sahip olup olmadığına ilişkin yapacağı değerlendirmede etkin ve bağımsız bir veri koruma otoritesinin varlığını öncelikle ve özellikle dikkate almaktadır.

Diğer taraftan bilindiği üzere, Avrupa Konseyi bünyesinde hazırlanmış ve ülkemizin de taraf olduğu 108 sayılı Sözleşme[1] kişisel verilerin korunması alanında hukuken bağlayıcı ilk ve tek uluslararası düzenleme niteliğine sahiptir. Sözleşme'de taraf devletlerin veri koruma yasalarının ihtiva etmesi gereken asgari güvenceler belirlenmiş durumdadır. Bununla birlikte, Sözleşme'de öngörülen veri koruma ilkelerine uygun olarak yürürlüğe konulacak ulusal düzenlemelerin uygulanmasını sağlayacak ve bu düzenlemelere aykırılık hâlinde ilgili kişilerin zararını giderecek bir başvuru merciinin kurulması hususunda taraf devletlere bir yükümlülük getirilmemiştir. Sözleşme kapsamında kurulan Danışma Komitesi tarafından bu durum zaman içinde etkin ve yeknesak bir veri koruma hukuku uygulaması bakımından bir eksiklik olarak görülerek giderilmesi amacıyla bir ek protokol hazırlanmıştır. Ülkemiz tarafından da onaylanan Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol'ün yürürlüğe girmesiyle taraf devletlerce bir veya daha çok veri koruma otoritesinin kurulacağı hüküm altına alınmıştır. Bu itibarla, hem "*altın standart*" olarak kabul edilen AB veri koruma mevzuatında hem de bu alanda en etkili uluslararası düzenlemede veri koruma otoritelerinin kurulması "*sine qua non*"[2] bir koşul olarak kabul edilmektedir.

Günümüzde kişisel verileri işlenen ilgili kişilerle söz konusu işleme faaliyetini gerçekleştiren kişi, kurum ve kuruluşlar arasında büyük bir bilgi asimetrisi bulunmaktadır. Teknoloji devi çok uluslu şirketler ile kamu kurum ve kuruluşları gün geçtikçe daha fazla kişisel veri elde etmektedir. Öyle ki çoğu zaman ilgili kişiler, kişisel verilerinin toplandığından haberdar dahi olmamaktadır. Dolayısıyla her ne kadar veri koruma düzenlemeleri kapsamında birtakım haklar kabul edilmiş olsa da sahip oldukları teknik kapasite ve mali kaynaklar sayesinde çok daha güçlü konumda bulunan veri sorumluları ve ilgili kişiler arasında sağlıklı bir muhataplık ilişkisinin tesis edilebilmesi adına veri koruma otoritelerine ihtiyaç duyulmaktadır. Ayrıca, veri sorumlularına yönelik yükümlülüklerinin yerine getirilip getirilmediğinin sürekli biçimde izlenmesi ve bir ihlal durumunda bozulan kamu düzeninin etkili ve caydırıcı araçlarla yeniden tesis edilmesi gerekmektedir. Veri koruma otoriteleri, bu tür müdahaleleri hem ilgili kişinin şikâyeti üzerine hem de ihlalden doğrudan haberdar olduğu durumlarda resen gerçekleştirebilmektedir.

Kişisel Verileri Koruma Kurumu

Ülkemizde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesiyle birlikte Kişisel Verileri Koruma Kurumu (KVKK) kurulmuştur. KVKK, karar organı Kişisel Verileri Koruma Kurulu'nun (Kurul) teşekkül ettiği 2017 yılında faaliyetlerine başlamıştır. Bir insan hakları kurumu ve bağımsız idari otorite olarak nitelendirilebilecek KVKK, Türk idari teşkilatı içinde düzenleyici ve denetleyici kurum statüsünü haizdir.

Kişisel verilerin korunması alanında bir uzmanlık kuruluşu ve kamu kurumları dahil olmak üzere veri sorumluları üzerinde bağımsız bir denetim makamı olarak KVKK'nın faaliyetlerini gereği gibi yerine getirebilmesi amacıyla 6698 sayılı Kanun'da birtakım güvenceler bulunmaktadır. Öncelikle, KVKK'ya idari ve mali özerklik tanınmış ve kamu tüzel kişiliği verilerek kamu gücünden yararlanabilmesi mümkün kılınmıştır. Buna ilaveten Kurul, görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurul'a emir ve talimat veremez, tavsiye veya telkinde bulunamaz.

Kişisel Verileri Koruma Kurumu'nun Faaliyetleri

Veri koruma otoriteleri, hukuka aykırı uygulamaları tespit ederek veri sorumlularını ihlali giderme konusunda talimatlandırmak ve idari yaptırım uygulanmasına karar vermek suretiyle "*kanun uygulayıcı*" rolünü üstlenmiştir. Ancak modern veri koruma hukuku uygulamasında veri koruma otoritelerinin faaliyetleri bununla sınırlı değildir. Bennett ve Raab, veri koruma otoritelerinin yedi farklı işleve sahip olduğunu ifade etmişlerdir[3]: "*Ombudsman*", "*denetmen*", "*yönlendirici*", "*eğitmen*", "*müzakereci*", "*politika danışmanı*" ve "*kanun uygulayıcı*"[4]. Nitekim KVKK da faaliyette bulunduğu 9 yıl boyunca ülkemizde genellikle veri sorumluları hakkında yürütülen incelemeler ve bu incelemeler sonucunda uygulanan idari yaptırımlarla ilgili olarak gündeme gelmekle birlikte, 6698 sayılı Kanun'un doğru anlaşılması ve uygulanması hususunda faaliyetler gerçekleştirmektedir.

Bu çerçevede ilgili kişiler 6698 sayılı Kanun'un uygulanmasıyla ilgili şikâyetlerini Kurul'a intikal ettirebilmektedir. Kanun'da ilgili kişilerin öncelikle veri sorumlularına başvuru yapması zorunlu tutulmuştur. Böylelikle uyuşmazlığın daha erken bir aşamada ve tarafların doğrudan müzakeresi neticesinde çözülebilmesi amaçlanmıştır. Bununla birlikte, ilgili kişinin başvurusunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde, ilgili kişi Kanun'un 14'üncü maddesinde düzenlenen sürelere uygun olarak Kurula şikâyette bulunabilmektedir.

Kurul, inceleme safhasında veri sorumlusundan konuyla ilgili bilgi ve belge isteme yetkisine sahiptir. Ayrıca, gerekli görülen durumlarda veri sorumlusunun tesislerinde yerinde inceleme yapılabilecektir.

Kurul, yalnızca somut ve doğrudan şikâyet sahibini ilgilendiren iddialar hakkında inceleme yürütmemektedir. Aynı zamanda kendisine ulaşan ihbarlara veya medya başta olmak üzere diğer iletişim kanallarından edinilen bilgilere binaen resen inceleme başlatabilmektedir. Bu süreçte de veri sorumlusundan bilgi, belge ve açıklama talep edilmekte ve gerekli görülen durumlarda yerinde inceleme yapılmaktadır.

1 Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi.

2 Olmazsa olmaz.

3 Colin J. Bennett ve Charles Raab. (2003). Governance of Privacy (*Mahremiyetin Yönetişimi*). New York: Routledge.

4 Orijinal metin: "*Ombudsmen, auditors, consultants, educators, negotiators, policy advisers and enforcers.*"

Kişisel verilerin korunması için denetim ve telafi edici mekanizmalar tek başına yeterli olmayacaktır. Veri koruma düzenlemeleri, veri sorumluları tarafından kapsamlı bir uyum programının oluşturulmasını ve takip edilmesini gerekli kılmaktadır. Bu anlamda, veri sorumluları iş süreçlerini ve organizasyon yapılarını tasarlarken veri koruma düzenlemelerine uyumu göz önünde bulundurmalıdır.

Öte yandan, teknolojik gelişimden ve dönüşümden etkilenmeden bireylere yeterli düzeyde koruma sağlamaya devam edebilmesi adına 6698 sayılı Kanun'da ilke düzeyinde yükümlülüklere[5] yer verilmiştir. Dolayısıyla, çok çeşitli iş kollarında faaliyet gösteren veri sorumluları, Kanun'a uyum sağlama konusunda yol gösterilmesine ihtiyaç duyabilmektedir. Kurul gerek düzenleyici yetkileri kapsamında yürürlüğe koyduğu ikincil mevzuat gerek kişisel verilerin yurt dışına aktarımından üretken yapay zekâ teknolojileriyle gerçekleştirilen kişisel veri işleme faaliyetlerine kadar geniş bir çerçevede hazırladığı rehberlerle veri sorumlularına kılavuzluk etmektedir.

"*Kişisel verilerin korunmasına ilişkin kültürün oluşturulmasında öncü bir kurum olmak*", KVKK'nın vizyonunun temel bileşenlerinden biri olarak belirlenmiştir. 6698 sayılı Kanun'un etkili bir şekilde uygulanması, ancak toplumun her kesiminde veri koruma kültürünün yerleşmesiyle mümkün olabilecektir. İdari yaptırımlar, tek başına yeterli ölçüde caydırıcılık sağlamayacaktır. Bireylerin ve kişisel veri işleyen kuruluşların bilinçlendirilerek veri koruma kültürünün ve dolayısıyla sorumlu veri paylaşımının ve kullanımının içselleştirilmesi gerekmektedir.

KVKK faaliyete geçtiği günden bugüne seminer, konferans, zirve ve çalıştay formatında düzenlenen farkındalık sağlayıcı/artırıcı etkinliklere önem vermiştir. Bu kapsamda, meslek kuruluşları ile kamu kurum ve kuruluşlarından öğretmenlere ve öğrencilere uzanan çeşitli hedef kitlelere yönelik organizasyonlar düzenlemektedir. Diğer paydaşlar tarafından düzenlenen toplantılara ise mümkün olduğu ölçüde destek vermektedir.

KVKK tarafından yürütülen farkındalık ve bilinçlendirme çalışmalarında özellikle çocuklara hassasiyet gösterilmektedir. Dijital çağda kişisel verilerin işlenmesi bağlamında maruz kalabileceği tehlikeler göz önünde bulundurularak çocuklara özgü broşürler, karikatürler ve animasyonlar hazırlanmıştır. Bu materyaller kapsamında çocukların karşılaşabileceği riskler ve bunlardan korunma yöntemleri dikkat çekici ve eğitici bir üslupla aktarılmaya çalışılmıştır.

6698 sayılı Kanun, kişisel verilerin işlenmesine ilişkin usul ve esasların belirlenmesi bakımından genel düzenleme niteliğindedir. Gerçek kişiler, özel hukuk tüzel kişileri veya kamu kurum ve kuruluşları tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinin bütünü kural olarak Kanun hükümlerine tabidir. Herhangi bir sektöre yönelik özel bir düzenleme, Kanun'da bulunmamaktadır. Bununla birlikte, sağlık, turizm, elektronik ticaret, reklamcılık veya havacılık gibi sektörlerde hem mal ve hizmet sunumu için hem de teknolojik imkânlardan yararlanılarak katma değer elde etmek üzere yoğunlukla kişisel veri kullanılmaktadır. KVKK'nın yönlendirici faaliyetlerinde ilgili sektör temsilcilerinin, meslek kuruluşlarının ve diğer kamu kurumlarının görüşlerini dikkate alması gerekecektir. Ancak bu şekilde veri sorumlularının kendi yapılarıyla ve faaliyet alanlarına özgü diğer yasal gerekliliklerle bağdaşan bir uyum çerçevesi ortaya konabilecektir.

Bankacılık ile ödeme ve elektronik para sektöründe kişisel verilerin korunmasına ilişkin rehberler, KVKK'nın bu müzakereci işlevini gösteren örnekler olarak kabul edilebilir. Söz konusu rehberler, ilgili kuruluşların temsilcileriyle iş birliği içinde hazırlanmıştır. Sektör paydaşlarının tabi olduğu sektörel mevzuat hükümleri ve uygulamaya yönelik gerçekleştirilen istişareler neticesinde rehberlere nihai hali verilmiştir.

5 Bu yaklaşım, İngilizce olarak "*tech-neutral*" terimiyle kavramsallaştırılmaktadır.

Kişisel verilerin korunması, bir yatay politika alanı teşkil etmektedir. Şöyle ki kişisel verilerin günlük hayatı dönüştürücü etkisi ve doğru şekilde işlendiği durumda sağlayabileceği katma değer; insan hakları, uluslararası ilişkiler ve ticaret, ulaşım, demografik planlama ve istatistik başta olmak üzere birçok alanda mevzuat, strateji ve eylem planı çalışmasında kişisel verilere ilişkin düzenlemeye yer verilmesini tetiklemiştir. 6698 sayılı Kanun'da öngörülen güvence mekanizmalarının sürdürülebilirliğinin sağlanabilmesi ve yeknesak bir veri koruma hukukunun yerleşebilmesi için kişisel verilere temas eden mevzuat taslaklarının hazırlık çalışmalarına KVKK'nın bir paydaş olarak katılım sağlaması önem arz etmektedir. Nitekim 6698 sayılı Kanun'da "*diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş vermek*" ayrıca ve açıkça Kurul'un görev ve yetkileri arasında sayılmaktadır.

Kurul, yaptığı inceleme neticesinde veri sorumlusunun 6698 sayılı Kanun'da öngörülen yükümlülüklerini yerine getirmediği kanaatine varması hâlinde idari para cezası uygulanmasına karar verebilir. Kurul tarafından bir hukuka aykırılığın tespit edilmesi durumunda bu aykırılığın ortadan kaldırılması amacıyla iş süreçlerini gözden geçirerek belirli işlemlerin gerçekleştirilmesine son verilmesi, kişisel verilerin korunmasına yönelik güvence mekanizmalarının işlevsel kılınabilmesi amacıyla iç yapılarında değişikliklerin yapılması veya hâlihazırda elde etmiş olduğu belli başlı kişisel verilerin imha edilmesi gibi talimatların yerine getirilmesi veri sorumlusundan talep edilebilir. Ayrıca ivedi bir şekilde müdahale gereken açık hukuka aykırılık hâllerinde Kurul, kişisel verilerin işlenmesini veya yurt dışına aktarımını durdurabilir.

Her ne kadar veri koruma düzenlemelerinin uygulanmasını temin etmede en etkili araç olarak görülebilirse de Kurul tarafından ceza hukuku ilkelerine uygun şekilde son çare olarak yaptırım uygulanması tercih edilmektedir. Kurul'un önceliği, güvenli bir ekosistemin oluşturulabilmesini sağlamaktır. KVKK tarafından yukarıda açıklanan diğer roller kapsamında cezalandırıcı değil; uyuma teşvik edici bir anlayış benimsenmektedir.

KVKK, "*Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, ülkemizde kişisel verilerin korunmasını sağlamak ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmek, aynı zamanda veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak*" misyonunu üstlendiğini ilân etmiştir. Kişisel verilerin işlenmesi ile temel hak ve özgürlüklerin korunması arasındaki dengeyi gözetmeye çalışmaktadır. KVKK, faaliyetlerine başlamasının ardından öncelikle veri koruma bilincini ülkemize yayarak farkındalık oluşturmuştur. Ardından, iç yapılanmasını tamamlayarak uzmanlık birimlerini kurmuştur ve kişisel veri işleme faaliyetlerinin 6698 sayılı Kanun'a uygun şekilde disiplin altına alınmasını sağlamıştır. Bununla birlikte, ülkemizin dijital politikalarının hazırlanmasında insan odaklı yaklaşımıyla önemli bir paydaş olarak yer almaya başlamıştır. Bu çerçevede, KVKK'nın kişisel verilerin korunmasını isteme hakkını bireyler bakımından her yönüyle işlevsel kıldığı söylenebilecektir.

İLKE KARARLARI

Kişisel Verileri Koruma Kurulu (Kurul), şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen yürütülen incelemeler neticesinde aldığı kararların yanı sıra, Kanun'un 15'inci maddesinin (6) numaralı fıkrası hükmü uyarınca ihlalin yaygın olduğunu tespit etmesi hâlinde ilke kararları da alabilmektedir. Bu kapsamda, Kanun'un doğru ve etkin bir şekilde uygulanmasını sağlamak, veri sorumlularının kişisel verilerin işlenmesi süreçlerinde uyması gereken temel ilke ve yükümlülükleri açıklığa kavuşturmak amacıyla Kurul tarafından bugüne dek çeşitli konularda toplamda 13 adet ilke kararı alınmıştır. Söz konusu ilke kararları hem Resmî Gazete'de hem de Kurumun internet sitesinde yayımlanarak kamuoyunun bilgisine sunulmaktadır.

Söz konusu ilke kararlarının özetlerine aşağıda yer verilmektedir:

1-Banko, gişe ve masa gibi vatandaşa hizmet sunulan alanlarda yaşanan kişisel veri güvenliği ihlallerine ilişkin olarak Kuruma intikal eden ihbarlar kapsamında alınan Kurulun 21/12/2017 tarih ve 2017/62 sayılı ilke kararı ile, bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşlarının; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte Kanun'un 12'nci maddesi uyarınca gerekli teknik ve idari tedbirleri almasına, diğer taraftan söz konusu Karara uymayanlar hakkında Kanun'un 18'nci maddesi kapsamında işlem yapılmasına karar verilmiştir.

2- İlgili kişilerin açık rızalarını almaksızın isimden telefon numarası veya telefon numarasından isim sorgulanması şeklinde rehberlik hizmeti veren internet siteleri ve uygulamalara ilişkin olarak Kuruma intikal eden ihbar ve şikâyetler kapsamında alınan Kurulun 21/12/2017 tarih ve 2017/61 sayılı İlke Kararı'nda; çeşitli uygulamalar, internet siteleri veya sosyal medya hesapları üzerinden kişisel verileri toplayarak bu verilerin paylaşımını sağlayan, isim sorgulandığında telefon numarası bilgisine, telefon numarası sorgulandığında da isim bilgisine erişme ve başkalarının telefon rehberinde nasıl kayıtlı olunduğunu öğrenme gibi konularda hizmet veren birçok uygulamanın ve internet sitesinin bulunduğunun tespit edildiği, kişisel veri işleme faaliyetlerinin gerçekleştirilebilmesi için Kanun'un 5 ve 6'ncı maddelerinde sayılan işlenme şartlarından birinin bulunmasının, ayrıca Kanun ile öngörülen diğer yükümlülüklerin yerine getirilmesinin gerektiği değerlendirmelerine yer verilerek,

Kanun'da ve ilgili mevzuatta dayanağı bulunmaksızın ilgili kişilerin iletişim bilgilerinin paylaşımını yapan internet siteleri ve mobil uygulamalar tarafından gerçekleştirilen veri işleme faaliyetinin Kanun'un 15 inci maddesinin (7) numaralı fıkrası uyarınca derhal durdurulması gerektiği ve belirtilen şekilde faaliyetlerde bulunan internet sitelerinin/uygulamaların faaliyetlerine son vermediğine ilişkin bilgi edinilmesi halinde bu internet sitelerine/uygulamalara erişimin engellenmesi adına gereğinin yapılmasını teminen yetkili kurumlara başvuruda bulunulacağı, öte yandan kişisel verilerin hukuka aykırı olarak elde edilmiş olabileceği de dikkate alınarak, 5237 sayılı Türk Ceza Kanunu'nun ilgili hükümleri çerçevesinde ilgili internet siteleri/uygulamalar hakkında gerekli hukuki işlemlerin tesisi için konunun ihbaren Cumhuriyet Başsavcılığına bildirileceği hususunda kamuoyunun bilgilendirilmesine ve söz konusu Karara uymayanlar hakkında Kanun'un 18'nci maddesi kapsamında işlem yapılmasına karar verilmiştir.

3- Veri sorumlusu nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişim yetkisi olanlar tarafından, yetkilerini aşarak ve işleme amacı dışında söz konusu verilerin işlendiği hususunda Kuruma intikal eden ihbar ve şikâyetler kapsamında alınan Kurulun 31/05/2018 tarih ve 2018/63 sayılı ilke kararı ile, bir veri sorumlusu nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılmasının Kanun'un 12'nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceği değerlendirmesinde bulunularak, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine karar verilmiştir.

4- İlgili kişilerin açık rızaları alınmaksızın e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları gelmesi hususunda Kuruma intikal eden başvurular neticesinde alınan Kurulun 16/10/2018 tarih ve 2018/119 sayılı ilke kararı ile, ilgili kişilerin rızalarını almadan veya Kanun'un 5'inci maddesinde hüküm altına alınan işleme şartlarını sağlamadan telefon numaralarına SMS göndermek, arama yapmak veya e-posta adreslerine posta göndermek suretiyle reklam içerikli ileti yönlendiren veri sorumluları ile veri sorumluları adına reklam içerikli mesaj/e-posta göndermek veya arama yapmak amacıyla ilgili kişilerin açık rızaları bulunmaksızın bu verileri kullanan veri işleyenlerin söz konusu veri işleme faaliyetlerini Kanun'un 15'inci maddesinin (7) numaralı fıkrası uyarınca derhal durdurması gerektiği, Kanun'un 12'nci maddesi kapsamında veri sorumlusunun kişisel verilerin işlenmesinde uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak zorunda olduğu ve kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, anılan tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu olduğu, belirtilen şekilde söz konusu faaliyetlerde bulunan veri sorumluları hakkında Kanun'un 18 inci maddesi hükümleri çerçevesinde işlem tesis edileceği ve bahse konu şekilde işlenen kişisel verilerin hukuka aykırı olarak elde edilmiş olabileceği de göz önüne alınarak 5237 sayılı Türk Ceza Kanunu'nun ilgili hükmü çerçevesinde ilgili veri sorumluları hakkında gerekli hukuki işlemlerin tesisi için konunun ihbaren ilgili Cumhuriyet Başsavcılığına bildirileceği hususunda kamuoyunun bilgilendirilmesine karar verilmiştir.

5- Kuruma intikal eden ihbarlar kapsamında alınan Kurulun 18/10/2019 tarih ve 2019/308 sayılı ilke kararında, avukatlar/hukuk büroları ile finans, gayrimenkul danışmanlık, sigorta vb. sektörlerde faaliyet gösteren bazı kişi ve kuruluşlar tarafından muhtelif yollarla elde edilen veriler üzerinden vatandaşların kimlik ve iletişim bilgileri gibi kişisel verilerinin sorgulanmasına imkân tanıyan yazılım/program/uygulamaların kullanılmakta olduğunun tespit edildiğine ve söz konusu durumun, Kanun'un veri sorumlularının veri güvenliğine ilişkin yükümlülüklerini düzenleyen 12'nci maddesi hükümlerine aykırılık oluşturduğuna yer verilerek,

Bu mahiyetteki yazılımları/programları/uygulamaları kullandığı tespit edilenler hakkında Türk Ceza Kanunu kapsamında gerekli adli işlemlerin tesisi için konunun ihbaren ilgili Cumhuriyet Başsavcılıklarına bildirileceği ve veri sorumluları hakkında Kanun'un 18'inci maddesi hükmü çerçevesinde idari işlem tesis edileceği hususlarında kamuoyunun bilgilendirilmesine karar verilmiştir.

6- Kuruma intikal eden şikâyet ve ihbarlar kapsamında alınan Kurulun 22/12/2020 tarih ve 2020/966 sayılı ilke kararında, e-ticaret, telekomünikasyon, ulaşım, turizm gibi muhtelif sektörlerde faaliyet gösteren veri sorumlularınca, fatura, ekstre, rezervasyon belgesi gibi kişisel veri içeren dokümanların sms ve/veya e-posta vasıtasıyla gönderimini teminen ilgili kişilerden telefon numarası ve/veya e-posta adreslerini beyan etmelerinin istenildiği, bununla birlikte ilgili kişiler tarafından söz konusu bilgilerin beyanında yanlışlık olabildiği veya yine ilgili kişilerce üçüncü kişilere ait bilgilerin beyan edilmesi neticesinde ilgili kişilere ait verileri içeren bahse konu dokümanların üçüncü kişilere iletildiğinin görüldüğü, Kanun'un 4'üncü maddesinde düzenlenen genel ilkelerden "doğru ve gerektiğinde güncel olma" ilkesi gereğince kişisel verilerin doğru ve gerektiğinde güncel şekilde tutulmasının veri sorumlusunun çıkarına uygun olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin korunması bakımından da gerekli olduğu, kişisel verilere dayalı olarak ilgili kişiye dair sonuç oluşturması veya doğurması durumunda veri sorumlusunun kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması bakımından aktif özen yükümlülüğünün bulunduğu, bunun yanı sıra veri sorumlusunun her zaman ilgili kişinin bilgilerinin doğru ve gerektiğinde güncel olmasını temin edecek kanalları açık tutmasının önemli olduğu, aksi takdirde kişilerin, güncel olmayan veya yanlış tutulan kişisel verileri nedeniyle maddi ve manevi zarar görmesinin gündeme gelebileceği, bu anlamda kişisel verilerin doğru ve gerektiğinde güncel tutulabilmesini temin etmek amacıyla; kişisel verilerin elde edildiği kaynakların belirli olması ve kişisel verilerin toplandığı kaynağın doğruluğunun tespit edilmesi ile kişisel verilerin doğru olmamasından kaynaklı ilgili kişiler açısından olumsuz sonuçlar ortaya çıkmasının önlenmesi kapsamında ilgili kişilerce beyan edilen iletişim bilgilerinin doğrulanmasına yönelik (telefon numarası ve/veya e-posta adresine doğrulama kodu/linki gönderilmesi vb.) makul önlemler alınmasının gerekli görüldüğü değerlendirmelerine yer verilerek,

Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına, Kanun'a aykırılık oluşturacak şekilde üçüncü kişilerin kişisel verilerini içeren ekstre, fatura vb. belgelerin gönderilmesinin önlenmesini teminen; Kanun'un 12'nci maddesinin (1) numaralı fıkrası gereğince veri sorumluları tarafından kendilerine bildirilen iletişim bilgilerinin doğruluğunu teyit edecek mekanizmaların oluşturulması adına gerekli idari ve teknik tedbirlerin alınması hususunda Kanun'un 15'inci maddesinin 6 numaralı fıkrası uyarınca İlke Kararı alınmasına karar verilmiştir.

7- Araç kiralama sektöründe kara liste uygulanmasına ilişkin Kuruma intikal eden ihbarlar kapsamında alınan Kurulun 23/12/2021 tarih ve 2021/1304 sayılı ilke kararında; araç kiralama yazılımcısı ve satıcısı kişilerin araç kiralama firmalarına (veya araç kiralama işi yapan gerçek kişilere) "kara liste" özelliği de içeren araç kiralama yazılımları sundukları, araç kiralama firmaları tarafından söz konusu yazılımlara kendi müşterileri olan araç kiralayan gerçek kişilerin kişisel verilerinin işlendiği, işlenen bu veriler arasında araçların kullanım sürecinde meydana gelen olumsuzlukları veya araç kiralama firmasının yorumlarını da içeren "kara liste" bilgilerinin yer aldığı, söz konusu bilgilerin araç kiralama firmaları tarafından sonraki kiralamalar için karar verirken kullanılmak üzere işlendiği, öte yandan bahse konu yazılımların bir araç kiralama firmasının kendi girdiği verileri diğer araç kiralama firmalarına da açmasına olanak veren sistemler olarak tasarlandığı, dolayısıyla araç kiralama firmasından yazılıma, yazılımdan ise söz konusu yazılımı kullanan diğer araç kiralama firmalarına kara listeye ilişkin veri akışı/paylaşımı sağlayan bir sistem oluşturulduğu, araç kiralayan ilgili kişilerin kişisel verilerinin de böylece karşılıklı olarak paylaşılmakta olduğu, genel olarak yazılım şirketleri tarafından sunulan hizmetin, SaaS (Software as a Service) şeklinde olduğu, SaaS hizmetinin gereği olarak veri tabanı ve yazılımın yönetiminin yazılım şirketlerinde olup araç kiralama firmalarında ve gerektiğinde teknik destek ve geliştirme sağlayabilmesi için yazılım şirketlerinde admin yetkisine sahip kullanıcıların atandığı, sunulan hizmet türü hazır bir SaaS hizmeti olduğundan kaynak kod halinde sunulmadığı, araç kiralama firmalarının yazılım kodlarına müdahalesine izin verilmediği, bu sebeple araç kiralama firmalarının yetkilerinin içerik sağlamakla sınırlı olduğu, araç kiralayan bir gerçek kişinin, müşterisi olduğu araç kiralama firmasına kiralama sözleşmesi kapsamında gerekli olan kişisel verilerini sağlarken, bu süreçte firmaya sağladığı verilerin, firma ile yaşadığı olumlu/olumsuz ilişkinin, araca verdiği zarar, ödeme sürecinde yaşanan sorunlar gibi kişisel verilerinin kara liste özelliği içeren yazılımlar vasıtasıyla müşterisi olduğu araç kiralama firması haricinde bilinmeyen sayıda kullanıcı ile paylaşıldığına dair bilgi sahibi olmadığının anlaşıldığına yer verilerek,

1774 sayılı Kimlik Bildirme Kanunu'nun ilgili maddeleri gereğince araç kiralama faaliyetinin kolluk kuvvetlerine bildirilme zorunluluğunun bulunduğu, dolayısıyla araç kiralama firmalarının Kiralık Araç Bildirim Sistemine (KABİS) veri girişi yapmaları bağlamında kişisel veri işlemelerinin Kanun'un 5'inci maddesi uyarınca *"Kanunlarda açıkça öngörülmesi"* ve *"veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması"* işleme şartları kapsamında değerlendirilebileceği, ayrıca araç kiralama işi taraflar arasında akdedilen bir sözleşme kapsamında gerçekleştirilmekte olduğundan Kanun'un 5'inci maddesi uyarınca *"bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* işleme şartı kapsamında ilgili kişilerin kişisel verilerinin araç kiralama firmalarınca işlenebileceği, kara liste benzeri veri kayıtları bakımından ise kişisel verilerin işletme faaliyetleri ile sınırlı olmak üzere işlenmesi ile yazılım firmaları aracılığıyla diğer veri sorumlularına açılmasının farklılık arz edeceği, Kanun'un 5'inci maddesinin 2 numaralı fıkrasının (f) bendinde *"ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* işleme şartı düzenlenmiş olup ilgili kişinin temel hak ve özgürlükleri ile veri sorumlusunun meşru menfaatleri arasında yapılacak denge testi sonucunda meşru menfaatin baskın gelmesi durumunda, işletme faaliyetleri ile sınırlı olmak kaydıyla, başka bir ifadeyle veri sorumlusu bünyesinde olmak üzere kara liste kaydı yapılmasının somut olaya göre ayrıca değerlendirilmek koşuluyla uygulanabilir olabileceği; ancak işlenen kişisel verilerin aynı yazılımı kullanan diğer veri sorumlularına (diğer araç kiralama firmalarına) açılması halinde ilgili kişinin temel hak ve özgürlüklerinin ihlal edilmeme şartının karşılanamayacağı, ayrıca bir araç kiralama firmasının işlediği kişisel verilen yazılım vasıtasıyla bilinmeyen sayıda araç kiralama firması ile paylaşmasının Kanun'un 4'üncü maddesinde düzenlenen genel ilkelerden *"hukuka ve dürüstlük kurallarına uygun olma", "belirli, açık ve meşru amaçlar için işlenme", "amaçla bağlantılı, sınırlı ve ölçülü olma"* ilkelerine aykırılık teşkil edeceği, ihbara konu kara liste uygulamalarında araç kiralama firmalarının gerçek kişi müşterilerden kişisel verileri ilk elden toplayan veri sorumluları oldukları, ancak, kara liste kaydına erişimin bir firma ile sınırlı kalmadığı, yazılıma aktarılan kişisel verilere yazılımı kullanan diğer araç kiralama firmalarının da erişim sağlayabildiği ve veri üzerinde hakimiyetleri olduğu dikkate alındığında, kara liste kaydını kendi menfaatleri doğrultusunda kullanan araç kiralama şirketleri ile yazılım şirketlerinin ortak veri sorumluluğunun ortaya çıkacağı, ortak veri sorumlularına ilişkin sorumluluk ve kusur miktarlarının belirlenmesi açısından her halükarda olay bazında veri işleme süreçlerinin incelenmesinin; kusurun ve söz konusu veri üzerindeki kontrolün kimde olduğunun tespitinin gerekeceği, ortak veri sorumluları arasında kusurluluk belirlenirken işlenen verinin ilk ve son kullanıcısının kim olduğu; veri girişini kimin yaptığı; hangi amaçla söz konusu yerinin girildiği; verinin değiştirilmesine veya silinmesine yahut aktarılmasına kimin karar verdiği; ; veriyi toplayan dışında kalan veri sorumlularının bu veri ile hangi faaliyetleri gerçekleştirdiği vb. etkenlere dikkat edileceği, araç kiralama sektöründe kara liste uygulamalarının ilgili kişinin hakları bakımından da değerlendirilmesinin gerektiği,

kara liste kapsamında kişisel veri işlenmesinin kişilerin Kanun'un 11'inci maddesinden kaynaklanan haklarını gereği gibi kullanabilmelerinin önünde engel teşkil edeceği, bu tür bir veri işlemenin kara liste uygulamalarının doğası gereği, kişi hakkında olumsuz bir sonuca ulaşılmasını, bu olumsuz sonucun kara listeye işlenmesini ve kişi hakkında bu olumsuz sonuca göre karar verilmesini içereceği için yapılan profilleme neticesinde ilgili kişi hakkında olumsuz bir sonuç ortaya çıkacağı; ancak araç kiralayan ilgili kişinin kişisel verilerinin paylaşıldığı diğer araç kiralama firmalarının kim olduğunu bilebilecek durumda olmaması nedeniyle Kanun'un 11'inci maddesinden kaynaklanan haklarını bu veri sorumluları nezdinde ileri sürebilmesinin güçleşeceği değerlendirmelerine yer verilerek,

Kanun'un 4'üncü maddesinde düzenlenen genel ilkelere, Kanun'un 5'inci maddesinde düzenlenen işleme şartlarına ve Kanun'un 8'inci maddesinde düzenlenen aktarıma ilişkin hükümlere aykırı olarak araç kiralama sektöründe kara liste uygulamaları kapsamında kişisel verilerin işlenmesi halinde, söz konusu veriler üzerinde hakimiyeti bulunan araç kiralama şirketlerinin yazılım şirketleri ile ortak veri sorumlusu olarak değerlendirileceklerine, hukuka aykırı bu gibi uygulamalara son verilerek araç kiralama sektöründe kişisel veri işleme süreçlerinin Kanun'a uygun olmasını teminen Kanun'un 12'nci maddesinde düzenlenen gerekli teknik ve idari tedbirlerin veri sorumlularınca alınması gerektiğine, söz konusu önlemleri almaksızın ve Kanun hükümlerine aykırı şekilde araç kiralama sektöründe kara liste uygulamasına başvuran veri sorumluları hakkında Kanun'un 18'inci maddesi hükümleri çerçevesinde işlem tesis edileceği hususunda kamuoyunun bilgilendirilmesine karar verilmiştir.

8- Belediyelerin çevrim içi sunmuş olduğu emlak vergisi ödeme/hızlı ödeme veya borç sorgulama sayfalarında yalnızca T.C. kimlik numarası girilerek vatandaşın emlak bilgilerine ulaşılmasına ilişkin Kuruma intikal eden ihbarlar kapsamında alınan Kurulun 21/04/2022 tarih ve 2022/388 sayılı ilke kararında, kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla Kurul tarafından hazırlanarak Kurum internet sayfasında yayımlanan Kişisel Veri Güvenliği Rehberinde (Teknik ve İdari Tedbirler) kişisel verilere gerekli durumlarda uzaktan erişilmesi halinde iki kademeli kimlik doğrulama kontrolünün uygulanmasının güvenliğin sağlanması adına alınması gereken tedbirler arasında sayıldığı, bu itibarla kişisel verilere uzaktan erişilmesi halinde 3. kişilerin kolayca ulaşamayacağı şekilde iki aşamalı sorgulama sistemi kullanılmasının gerekli olduğu, örneğin kişinin T.C. kimlik numarası ve doğum günü bilgisi sorgulanarak erişim imkânı veren sistemlerin tek kademeli doğrulama olduğu, kişinin T.C. kimlik numarasının yanı sıra kişiye özel oluşturulmuş şifre ya da kişinin daha önce bildirmiş olduğu telefon numarasına iletilen SMS kodu ile erişim sağlanan sistemlerin ise iki kademeli doğrulama olarak kabul edildiği, söz konusu rehberin "Teknik ve İdari Tedbirler Mevcut Risk ve Tehditlerin Belirlenmesi" başlıklı maddesi uyarınca, kişilerin bilgilerine kolayca erişilmesi riskini barındıran tek kademe doğrulama sistemlerinin yerine bu riski önemli ölçüde azaltacak ya da ortadan kaldıracak iki faktörlü doğrulama yöntemleriyle sorgulamaların uygulamaya konulmasının önemli olduğu, belediyeler tarafından emlak vergisi ödeme/hızlı ödeme veya borç sorgulama vb. sayfalar aracılığıyla çevrim içi olarak sunulan hizmetler kapsamında Kanun'un 12'nci maddesinde yer alan yükümlülüklerin yerine getirilmesi ve herhangi bir veri ihlalinin önlenmesi amacıyla; çift faktörlü doğrulama için ilk doğrulamanın T.C. kimlik no, ad soyad, vergi no, sicil no gibi verilerle yapılırken ikincil düzeydeki doğrulamanın kişiye özel oluşturulmuş SMS ya da e-postaya iletilen şifre gibi bir sistemle gerçekleştirilmesi, ikincil düzeyde kişiye ait başkalarının da erişebileceği telefon no, doğum tarihi, anne baba adı, sicil no gibi bilgiler yerine sadece kişiye özel olarak belirlenecek ve sadece ilgili kişinin erişebileceği verilerin istendiği sistemler ya da üyelik sistemi ile söz konusu hizmetlerin sunulmasının uygun olacağı değerlendirmelerine yer verilerek,

Belediyelerin emlak vergisi ödeme/hızlı ödeme ve borç sorgulama hizmetlerinde üyelik ve şifre ya da çift faktörlü doğrulama kullanmak sureti ile Kanun'un 12'nci maddesi kapsamında gerekli teknik ve idari tedbirleri alması gerektiğine, söz konusu önlemleri almayan belediyeler hakkında iletilecek şikâyet/ihbarlar doğrultusunda ilgili belediye hakkında Kanun'un 18'inci maddesi hükümleri çerçevesinde işlem tesis edileceği hususunda kamuoyunun bilgilendirilmesine karar verilmiştir.

9- Ürün ve hizmet sunumlarına ilişkin süreçlerde (ödeme yapma, kayıt açma, üyelik oluşturma, teklif oluşturma ve benzeri işlemler esnasında) ilgili kişilerin iletişim bilgilerinin talep edildiği, akabinde ilgili kişilere SMS ile doğrulama kodu gönderildiği ve ödemelerinin tamamlanması, fatura oluşturulması, faturanın iletişim adresine iletilmesi ya da bilgilerinin güncellenmesi için gerekli olduğu gerekçesi öne sürülerek söz konusu kodun görevliye bildirilmesinin/sisteme girilmesinin istenildiği ancak bahse konu işlemin akabinde ilgili kişilere söz konusu veri sorumlusunun faaliyetleri ile ilgili ticari elektronik ileti gönderildiğine yönelik Kuruma intikal eden ihbar ve şikâyetler kapsamında alınan Kurulun 10/06/2025 tarih ve 2025/1072 sayılı ilke kararında, ilgili kişilere ürün ve hizmet sunumlarına ilişkin süreçlerde (ödeme yapma, kayıt açma, üyelik oluşturma, teklif oluşturma ve benzeri işlemler esnasında) doğrulama kodu gönderilen SMS'lerin içeriklerinde ya da SMS gönderimi öncesinde veri sorumlusunca veya yetkilendirdiği kişilerce herhangi bir aydınlatma yapılmadığının ve/veya söz konusu kodun ödeme işlemlerinin tamamlanması ya da bilgilerinin güncellenmesi için gerekli olduğu gerekçesi ile istenilmesine rağmen veri sorumlusu tarafından bu yolla ticari elektronik ileti gönderimine ilişkin açık rıza alınması suretiyle ilgili kişilerin yanıltıldığının tespit edildiği, Kanun'un 3'üncü maddesi uyarınca açık rızanın *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* unsurlarını taşıması gerektiği, Kanun'un 10'uncu maddesi gereğince, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi tarafından aydınlatma yükümlülüğünün yerine getirilmesi gerektiği, aydınlatma yükümlülüğünün gerek açık rıza alınması gerekse de Kanun'daki diğer kişisel veri işleme şartlarının sağlanmasından bağımsız olarak yerine getirilmesi gereken bir yükümlülük olduğu, bununla birlikte, kişisel veri işleme faaliyetinin ilgili kişinin açık rızasına dayanarak gerçekleştirilmesi durumunda, veri sorumlusu tarafından aydınlatma yükümlülüğü ile açık rıza alınması işlemlerinin ayrı ayrı yerine getirilmesinin gerektiği ve veri sorumluları tarafından yapılacak aydınlatmanın Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine de uygun olması gerektiği değerlendirmelerine yer verilerek,

-Ürün ve hizmet sunumlarına ilişkin süreçlerde (ödeme yapma, kayıt açma, üyelik oluşturma, teklif oluşturma ve benzeri işlemler esnasında) ilgili kişilerin telefonuna gönderilecek olan SMS'in amacının ne olduğu ve bu SMS ile iletilen kodun verilmesi halinde ne gibi sonuçlar doğuracağı hususunun, katmanlı aydınlatmanın bir gereği olarak ilk aşamada veri sorumlusunun görevlileri tarafından ilgili kişilere açık ve anlaşılır bir biçimde aktarılması, ayrıca aydınlatma yükümlülüğünün yerine getirilebilmesi amacıyla söz konusu SMS içeriklerinde de gerekli bilgilendirme kanallarının sağlanması,

-İlgili kişilere SMS ile doğrulama kodu gönderilerek üyelik sözleşmesinin onaylanması, kişisel verileri işleme izni alınması, ticari elektronik ileti onayı alınması vb. birbirinden farklı işleme faaliyetlerinin tek bir eylemle gerçekleştirilmesine yönelik uygulamalara son verilmesi, açık rıza ile gerçekleştirilmesi gereken işleme faaliyetlerine yönelik seçenek sunulmak suretiyle ilgili kişilerden ayrı ayrı açık rıza alınması,

-Veri sorumlularınca açık rıza alınması ve aydınlatma yükümlülüğünün yerine getirilmesi işlemlerinin ayrı ayrı gerçekleştirilmesi,

-Ticari elektronik ileti gönderimi için açık rıza alınmasını teminen SMS doğrulama kodu gönderilmesine yönelik bir uygulamaya gidilmesi halinde ise söz konusu işlemde alınacak açık rızanın Kanun'da belirtilen tüm unsurları kapsaması,
-Ticari elektronik ileti gönderilmesi amacıyla kişisel verilerin işlenmesine açık rıza verilmesinin ürün ve hizmet sunumunun tamamlanabilmesi için zorunlu bir unsur şeklinde ilgili kişilere sunulmaması, aksi takdirde söz konusu uygulamanın açık rızanın unsurlarından olan "bilgilendirmeye dayanma ve özgür iradeyle açıklanma" unsurlarının zedelenmesine sebep olabileceği, bu nedenle tüm süreçlerin Kanun'a uygun şekilde gerçekleştirilmesi,
- Ticari elektronik ileti gönderilmesi amacıyla kişisel verilerin işlenmesine yönelik açık rızanın, ürün ve hizmet sunumunun tamamlanmasından sonra talep edilmesi veya gerek SMS içeriklerinde gerekse veri sorumlusu tarafından fiziksel ortamda veya dijital ortamda yapılan bilgilendirmelerde söz konusu kodun görevli ile paylaşılması suretiyle verilen rızanın ürün ve hizmet sunumunun tamamlanması için zorunlu olmadığı, kodun verilmemesi halinde de her zaman ürün ve hizmet sunulabileceği, kod ile verilen izinlerin ve tercihlerin istendiği zaman değiştirilebileceği bilgisine net bir şekilde yer verilmesi yöntemlerinin tercih edilmesi ile ticari elektronik ileti iznine yönelik açık rızanın ürün ve hizmet sunumunun zorunlu bir unsuru gibi algılanmasının önüne geçilmesi,
-Bahse konu işlemlerin hukuka uygunluğunun sağlanmasını teminen veri sorumluları tarafından bu süreçlerde yer alan personele yönelik gerekli eğitim ve farkındalık çalışmalarının periyodik olarak yürütülmesi

gerektiği kararlaştırılarak, belirtilen hususların Kanun'un 12'nci maddesinin birinci fıkrası uyarınca kişisel verilerin hukuka uygun işlenmesini teminen veri sorumluları tarafından alınması gereken idari ve teknik tedbirlerden olduğu ve belirtilen hususlara uygun hareket edilmediğinin tespiti halinde ilgili veri sorumluları hakkında Kanun'un 18'inci maddesi hükümleri çerçevesinde işlem tesis edileceği hususunda kamuoyunun bilgilendirilmesine karar verilmiştir.

10- Turizm ve otelcilik sektöründe konaklama hizmeti alan kişilerin T.C. kimlik belgesi fotokopisinin kaydedilmesi hakkında alınan Kurulun 06/11/2025 tarih ve 2025/2120 sayılı ilke kararı ile, Kanun'un 5'inci maddesinde kişisel verilerin işlenme şartlarına yer verildiği, Kanun'un 6'ncı maddesinde ise özel nitelikli kişisel verilerin işlenme şartlarına yer verildiği, 1774 sayılı Kimlik Bildirme Kanunu'nun 2'nci maddesinin; *"Otel, motel, han, pansiyon, bekar odaları, günübirlik kiralanan evler, kamp, kamping, tatil köyü ve benzeri her türlü, özel veya resmi konaklama yerleri ile özel sağlık müesseseleri, dinlenme ve huzur evleri, dini ve hayır kurumlarının sosyal tesislerinin sorumlu işleticileri, bu yerlerde ücretli veya ücretsiz, gündüz veya gece, yatacak yer gösterdikleri yerli veya yabancı herkesin kimlik ve geliş-ayrılış kayıtlarını, örneğine ve usulüne uygun şekilde günü gününe tutmak, genel koltuk örgütlerinin her an incelemelerine hazır bulundurmak, Devlet İstatistik Enstitüsüne, talebi halinde vermek zorundadırlar."* hükmünü haiz olduğu, Kimlik Bildirme Kanunu'nun Uygulanmasına Dair Yönetmeliğin *"Kayıtlama"* başlıklı 5'inci maddesinin; *"Bu Yönetmelik hükümlerine göre kimlik bildirme belgelerini en yakın yetkili genel kolluk örgütüne vermekle yükümlü tutulanlar, kimliğini nüfus hüviyet cüzdanı veya diğer resmi geçerli belgelerle ispat edemeyen kimseleri, tesislerinde barındıramaz, konut ve iş yerinde çalıştıramaz."* ve aynı yönetmeliğin *"Yükümlü"* başlıklı 23'üncü maddesinin; *"Yönetmeliğin 6.maddesinde sayılan yerlerin sorumlu işleticileri tarafından; buralarda ücretli veya ücretsiz, gündüz veya gece yatacak yer gösterilen yerli veya yabancı herkesin kimliği ile geliş ve ayrılış tarihleri, Konaklama Yeri Kayıt Defteri (Form: 7) ne günü gününe geçirilir. Bu yerlerde kalacak kişilerin, kendilerine verilecek kopyalı bir örnek Konaklama Belgesi (form:8) ni doldurarak imzalamaları ve sorumlu işleticiye vermeleri şarttır. Konaklama belgesindeki bilgiler, kişinin kimliğini belirten geçerli resmi belge ile karşılaştırıldıktan sonra, konaklama yeri kayıt defterine aktarılır."* hükümlerini haiz olduğu, bu kapsamda, anılan yerlerde konaklama hizmeti alan ilgili kişilerden isim, soy isim, T.C. kimlik numarasından oluşan kimlik bilgilerinin kaydedilmesi şeklinde gerçekleşen kişisel veri işleme faaliyetinin 1774 sayılı Kimlik Bildirme Kanunu ve Kimlik Bildirme Kanununun Uygulanmasına Dair Yönetmeliğin açık hükümleri doğrultusunda Kanun'un 5'inci maddesinin (a) bendi *"Kanunlarda açıkça öngörülmesi"* ve (ç) bendi *"Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması"* şartları çerçevesinde işlendiği ve dolayısıyla hukuka uygun bir işleme faaliyeti olduğu, bununla beraber ilgili yerlerde konaklayan kişilerden işlenen kişisel verilerin doğruluğunun resmi belge ile karşılaştırmak suretiyle teyidinin sağlanması ve bu amaçla T.C. kimlik belgesinin talep edilmesinin hukuki olduğu gibi aynı zamanda eşyanın tabiatı gereği olduğu, ancak teyit amacıyla olsa dahi T.C. kimlik belgesinin istenmesinin ardından fotokopisinin de alınarak kayda geçirilmesi şeklinde gerçekleşen kişisel veri işleme faaliyeti, gereğinden fazla veri işleme sonucunu doğurmakla beraber bu işleme faaliyetinin herhangi bir hukuki bir dayanağının da söz konusu olmadığı, dolayısıyla ilgili kişilere ait T.C. Kimlik Belgesi fotokopisinin kaydedilmesi işleminin Kanun uyarınca hukuka aykırı bir işleme faaliyeti olduğu, ek olarak ülkemizde 2 Ocak 2017 tarihinden itibaren eski nüfus cüzdanları değiştirilerek üzerinde çip bulunan kimlik kartına geçiş yapılmış olsa da hâlihazırda nüfus cüzdanı kullanımına da devam edilebildiği, dolayısıyla nüfus cüzdanı üzerinde kişilerin dini ve kan grubu gibi özel nitelikli kişisel verilerinin de yer aldığı dikkate alındığında; veri sorumlularının konaklama nedeniyle ilgili kişilerin nüfus cüzdanı fotokopilerini kayıt altına alması halinde Kanun'un 6'ncı maddesine de ayrıca aykırılık teşkil edecek bir işleme faaliyetinde bulunulacağı, diğer taraftan turizm ve otelcilik sektöründe genel olarak konaklamaya ilişkin bir hizmet satışı söz konusu olduğundan faturalandırma amacıyla ilgili kişilerin kişisel verilerinin işlenmesinin de mümkün olduğu, bu çerçevede; 213 sayılı Vergi Usul Kanunu'nun 230'uncu maddesinin; *"Faturada en az aşağıdaki bilgiler bulunur:*

1. *Faturanın düzenlenme tarihi seri ve sıra numarası;*
2. *Faturayı düzenleyenin adı, varsa ticaret unvanı, iş adresi, bağlı olduğu vergi dairesi ve hesap numarası;*
3. *Müşterinin adı, ticaret unvanı, adresi, varsa vergi dairesi ve hesap numarası;*
4. *Malın veya işin nevi, miktara, fiyatı ve tutarı;*
5. *(Değişik: 4/12/1985-3239/19 md) Satılan malların teslim tarihi ve irsaliye numarası, (Malın alıcıya teslim edilmek üzere satıcı tarafından taşındığı veya taşıttırıldığı hallerde satıcının, teslim edilen malın alıcı tarafından taşınması veya taşıttırılması halinde alıcının taşınan veya taşıttırılan mallar için sevk irsaliyesi düzenlemesi ve taşıtta bulundurulması şarttır." hükümlerini haiz olduğu, aynı Kanun'un "Taşıma ve otel işletmelerine ait belgeler"* başlıklı 240'ıncı maddesinin: *"... C) Günlük müşteri listeleri: Otel, motel ve pansiyon gibi konaklama yerleri, odalar, bölmeler ve yatak planlarına uygun olarak müteselsil seri ve sıra numaralı günlük müşteri listeleri düzenlerler ve işletmede bulundururlar.*
Bu listelerde aşağıdaki bilgiler bulunur:

1. *Mükellefin adı, soyadı, varsa unvanı ve adresi,*
2. *Oda numaraları yazılmak suretiyle müşterinin adı, soyadı ve oda ücreti,*
3. *Düzenleme tarihi." hükmünü haiz olduğu,*

Bu kapsamda, 213 sayılı Vergi Usul Kanunu'nun bahse konu maddeleri çerçevesinde ilgili kişilerin anılan maddede yer verilen kişisel verilerinin işlenmesi faaliyetinin Kanun'un 5'inci maddesinin (a) bendinde yer alan "Kanunlarda açıkça öngörülmesi" şartı çerçevesinde hukuka uygun bir işleme faaliyeti olduğu değerlendirmelerine yer verilerek,

Turizm ve otelcilik alanında hizmet veren veri sorumluları tarafından, konaklama yerlerinde misafir edilen kişilerden T.C. kimlik belgesi fotokopisi alınması uygulamasına son verilmesi ve söz konusu ilke kararının yayımlanmasından önce konaklama amacıyla hizmet alan ilgili kişilere ait T.C. Kimlik Belgesi fotokopilerini kayıt altına alan veri sorumlularının bu nitelikteki belgeleri Kanun'un 7'nci maddesine uygun olarak imha etmesi gerektiği sonucuna varılarak,

Bahse konu hususların, Kanun'un 12'nci maddesinin birinci fıkrası uyarınca kişisel verilerin hukuka uygun işlenmesini teminen veri sorumluları tarafından alınması gereken idari ve teknik tedbirlerden olduğu ve belirtilen hususlara uygun hareket edilmediğinin tespiti halinde ilgili veri sorumluları hakkında Kanun'un 18'inci maddesi hükümleri çerçevesinde işlem tesis edileceği hususunda kamuoyunun ve sektör temsilcilerinin bilgilendirilmesine karar verilmiştir.

11- Muhtelif sektörlerde veri sorumluları tarafından yürütülmekte olan Sadakat Kart programları kapsamında; sadakat kart sahibi ilgili kişiye ait cep telefonu numarasının alışveriş sırasında üçüncü bir şahıs tarafından kasa görevlisi ile paylaşılması suretiyle alışveriş yapıldığı, sadakat kart üzerinden yapılan bu alışveriş işleminin kasa görevlisi tarafından herhangi bir işlem onay kodu sisteme girilmeksizin gerçekleştirildiği, ilgili kişinin alışveriş işlemi sırasında kasada olmamasına, bilgisinin ve rızasının bulunmamasına rağmen veri sorumlusu tarafından ilgili kişiye ait cep telefonu numarasının üçüncü şahıs tarafından paylaşılması suretiyle kişisel verileri kullanılarak sadakat kartı üzerinden alışveriş yapılmasına olanak sağlandığı, ayrıca yapılan alışverişe ilişkin fatura vb. belgenin ilgili kişi adına düzenlenerek hukuka aykırı veri işleme faaliyetinin gerçekleştirildiği ve kişisel veri güvenliğinin ihlal edildiği hususlarında Kuruma muhtelif kanallardan iletilen ihbar ve şikâyetler kapsamında alınan Kurulun 11/02/2026 tarih ve 2026/266 sayılı ilke kararında;

-Gıda, kozmetik, teknoloji, yapı market, giyim vb. muhtelif sektörlerde faaliyet gösteren veri sorumlularınca yürütülen sadakat kart üyelik programları kapsamında bahse konu uygulamanın yaygın olduğunun,

-Genel olarak sadakat kartın veri sorumluları tarafından üyelik sözleşmesi çerçevesinde ilgili kişilerin şahsi kullanımı için verildiğinin,

-Sadakat kart üyeliğinin, ilgili kişiye ait cep telefonu numarasına SMS yoluyla tek kullanımlık doğrulama kodu gönderilmesi, mobil uygulama/ internet sitesi üzerinden sağlanan barkod/ QR kod okutma vb. yöntemlerin kullanılması suretiyle gerçekleştirildiğinin,

-İlgili kişiye ait cep telefonu numarasının veya sadakat kart numarasının kasadaki görevliye bildirilmesi suretiyle sadakat kart üzerinden alışveriş yapılabildiğinin, indirim ve promosyondan faydalanılabildiğinin,

-Sadakat kartın alışveriş esnasında indirim, promosyon, puan kazanımı gibi amaçlarla kullanımı için; alışverişin bizzat ilgili kişi tarafından veya ilgili kişinin bilgisi ve onayı dahilinde yapılıp yapılmadığına dair veri sorumlularınca herhangi bir doğrulama mekanizması oluşturulmaksızın, kasadaki görevliye yalnızca ilgili kişiye ait cep telefonu numarası veya sadakat kart numarasının bildirilmesi suretiyle sadakat kart üzerinden alışveriş işleminin gerçekleştirilebilmesine ilişkin uygulamanın yaygın olduğunun,

-Sadakat kart kullanımı ile kazanılan puanların harcanmasına ilişkin işlemlerde ise ilgili kişiye ait cep telefonu numarasına SMS yoluyla gönderilen tek kullanımlık doğrulama kodunun kasa görevlisine bildirilmesi, mobil uygulama/ internet sitesi üzerinden sağlanan barkodun/ QR kodun kasada okutulması vb. yöntemlerin kullanılması suretiyle oluşturulan doğrulama mekanizmalarının yaygın olarak kullanıldığının,

-Sadakat kart üzerinden gerçekleştirilen alışveriş işlemi sonucunda düzenlenen fatura vb. belgenin sıklıkla sadakat kart sahibi ilgili kişi adına düzenlendiği ve yapılan alıverişe ilişkin müşteri işlem bilgilerinin (satın alınan ürün/hizmet, satın alma tarihi vb.) ilgili kişi ile ilgili kayıtlar arasına işlendiğinin; bu nedenle, sadakat kart sahibi ilgili kişinin bilgisi ve rızası olmaksızın cep telefonu numarasının veya sadakat kart numarasının üçüncü bir kişi tarafından alışverişte kullanımı halinde, ilgili kişiye ait kayıtlara/ üyelik hesabına hatalı müşteri işlem bilgisinin işlenmesi veya ilgili kişi adına yapmadığı, bilgisi ve rızasının olmadığı bir alışverişe ilişkin fatura düzenlenmesi suretiyle kişisel veri ihlallerinin yaşanabildiğinin tespit edildiğine yer verilerek,

-İlgili kişiye ait cep telefonu numarasının veya sadakat kart numarasının, bilgisi ve rızası olmaksızın üçüncü bir kişi tarafından alışveriş esnasında kasada görevli kişiye bildirilmesi suretiyle ilgili kişi adına alışveriş işlemi gerçekleştirilmesinin, Kanun'un 5'inci maddesinde yer alan herhangi bir veri işleme şartına dayandırılamayacağı ve hukuka aykırı kişisel veri işleme faaliyetine yol açacağı,

-İlgili kişiye ait cep telefonu numarası veya sadakat kart numarası kullanılarak ilgili kişinin bizzat kendisi tarafından yapılmayan, bilgisinin ve rızasının olmadığı bir alışveriş işlemine ilişkin olarak ilgili kişi adına fatura vb. belge düzenlenmesi ve/veya müşteri işlem bilgisinin (hangi mağazadan, hangi tarihte, hangi ürünün satın alındığı vb.) ilgili kişi ile ilgili kayıtlara/ üyelik hesabına işlenmesi suretiyle gerçekleşen kişisel veri işleme faaliyetinin Kanun'un 4'üncü maddesinde öngörülen "doğru ve gerektiğinde güncel olma" ilkesine aykırılık teşkil edeceği,

-Her ne kadar veri sorumluları tarafından Sadakat Kart Üyelik Sözleşmesi kapsamında ilgili kişilerin şahsi kullanımına yönelik olarak düzenlenen sadakat kartın üçüncü kişilere kullandırılmaması hususunda ilgili kişilere sorumluluk yüklenmiş olsa da bu durumun veri sorumluları tarafından yürütülen kişisel veri işleme faaliyetlerinde Kanun'un 12'nci maddesinde düzenlenen kişisel veri güvenliğini sağlama yükümlülüğünü ortadan kaldırmadığı değerlendirmelerinden hareketle,

-Kanun kapsamında hukuka aykırı olduğu değerlendirilen, ilgili kişiye ait cep telefonu numarasının veya sadakat kart numarasının ilgili kişinin bilgisi ve rızası dışında üçüncü bir kişi tarafından alışveriş esnasında kasadaki görevliye bildirilmesi suretiyle sadakat kart üzerinden alışveriş işlemi yapılabilmesine imkân sağlayan uygulamaya son verilmesine,

-Sadakat kart üzerinden gerçekleşen alışveriş işlemlerine ilişkin kişisel veri işleme süreçlerinin Kanun'a uygun olmasını teminen, Kanun'un 12'nci maddesinde düzenlenen gerekli teknik ve idari tedbirlerin veri sorumlularınca alınması gerektiğine,

-Sadakat kart sahibi ilgili kişinin cep telefonu numarasının veya sadakat kart numarasının kasa görevlisine bildirilmesi suretiyle gerçekleşen alışveriş işleminin ilgili kişinin bilgisi ve rızası dahilinde gerçekleştiğini doğrulamak amacıyla; sadakat kartların herhangi bir amaçla (üyelik oluşturma, alışverişte puan kazanımı, puan kullanımı, indirimden/ promosyondan faydalanma vb.) kullanımı için ilgili kişilerin cep telefonu numarasına SMS yoluyla gönderilen tek kullanımlık doğrulama kodunun kasa görevlisine bildirilmesi; mobil uygulama/ internet sitesi üzerinden sağlanan barkodun/ QR kodun kasada okutulması; fiziki sadakat kartın kasada ibrazı/okutulması; sadakat kart şifresinin kasada işlem cihazına girilmesi; sadakat kart programları kapsamında oluşturulan online üyelik hesabı üzerinden sadakat kart kullanımında yalnızca cep telefonu numarası bildirilmek suretiyle alışveriş esnasında hangi işlemlerin (alışverişte puan kazanma/indirim veya promosyondan faydalanma/puan harcama) yapılmasına onay verildiğine ilişkin "opt-in" olarak ilgili kişilere tercih imkânının sunulması vb. yöntemler kullanılmak suretiyle veri sorumluları tarafından doğrulama mekanizmalarının oluşturulması gerektiğine,

-Alışveriş esnasında sadakat kart üyeliği bulunan ilgili kişinin cep telefonu numarasının veya sadakat kart numarasının ilgili kişinin bilgisi ve rızası olmaksızın üçüncü bir kişi tarafından kullanılması suretiyle gerçekleştirilen kişisel veri işleme faaliyetlerinde yaşanabilecek kişisel veri ihlallerini önlemeyi amaçlayan en uygun doğrulama yöntemlerinin kullanılmasının

temel amaç olduğu dikkate alındığında; veri sorumluları tarafından bu amaca hizmet edecek doğrulama mekanizmalarının tercih edilmesi gerektiği; bu kapsamda, farklı ilgili kişi gruplarına yönelik alternatif doğrulama mekanizmalarının sunulabileceği; sadakat kart uygulamasında üyelik doğrulama, puan/indirim/promosyon kazanma, puan harcama gibi farklı işlem türlerine ve bu işlemlerin risk oranına göre farklı doğrulama mekanizmalarının kullanılabileceğine,
-Bahse konu doğrulama mekanizmalarının oluşturulabilmesi için veri sorumlularına söz konusu ilke Kararının yayınlanma tarihinden itibaren 6 aylık uyum süresi öngörülmesine,
-Bahse konu önlemleri almayarak, Kanun hükümlerine aykırı şekilde bu uygulamaya devam eden, bu ilke kararında belirtilen hususlara uygun hareket etmediği tespit edilen veri sorumluları hakkında Kanun'un 18'inci maddesi hükümleri çerçevesinde işlem tesis edileceği hususunda kamuoyunun ve sektör temsilcilerinin bilgilendirilmesine karar verilmiştir.

12- Veri sorumluları tarafından açık rıza ve aydınlatma metinlerinin ayrı ayrı düzenlenmesi gerektiğine ilişkin olarak Kurulun 18/02/2026 tarih ve 2026/347 sayılı ilke kararında; açık rıza metni ile aydınlatma metninin iç içe geçmiş şekilde ilgili kişilere sunulmasının Kuruma intikal eden ihbar ve şikâyetlerde en çok karşılaşılan hukuka aykırılıklardan biri olduğu, Kanun'un 10'uncu maddesinde düzenlenen aydınlatma yükümlülüğünün temelde kişisel verileri işlenen ilgili kişilerin bilgileındirilmesi anlamına geldiği, açık rızanın ise kişisel verilerin hukuka uygun olarak işlenebilmesi için Kanun'da öngörülen işleme şartlarından biri olduğu, bu doğrultuda, niteliği itibariyle farklı kavramlara karşılık gelen açık rıza ve aydınlatma metinlerinin ayrı ayrı metinlerde düzenlenmesi gerektiği, Anayasa'nın 20'nci maddesinin üçüncü fıkrasında, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin hüküm altına alındığı, Kanun'un 5'inci maddesinde kişisel verilerin, 6'ncı maddesinde ise özel nitelikli kişisel verilerin işlenmesi için açık rıza alınmasının kişisel veri işleme şartları arasında sayıldığı, Kanun'un 3'üncü maddesinde yer alan tanım kapsamında açık rızanın, ilgili kişinin kendisiyle ilgili kişisel verilerin işlenmesine izin verdiğini/işlenmesini onayladığını gösteren özgürce verilmiş, konuya özel, bilgilendirilmiş ve belirsizlik içermeyen rızası anlamına geldiği, açık rıza metinlerine ilgili kişiler tarafından kişisel verilerinin metinde yer alan amaç ve hukuki sebeplere dayalı olarak işlenmesine açık rıza verildiğinin beyan edilmesi gerektiği, bununla birlikte, Kanun'a uygurı bir şekilde açık rıza alındığına ilişkin ispat yükümlülüğünün veri sorumlusuna ait olduğu,
Aydınlatma yükümlülüğünün ise Kanun'un 10'uncu maddesinde *"(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi; ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür."* şeklinde açıklandığı, aydınlatma yükümlülüğünün amacının işlenen kişisel veriler ve işleme faaliyetlerine ilişkin olarak ilgili kişilerin bilgilendirilmesinden ibaret olup aydınlatma metinlerinin sözleşme niteliği taşımadığı, bu nedenle aydınlatma metinlerinde sıkça yapılan hatalardan olan "okudum ve kabul ediyorum", "okudum ve açık rıza veriyorum", "okudum ve onaylıyorum" şeklindeki metnin sonunda yer verilen ifadelerin yerine aydınlatma metninin ilgili kişi tarafından okunduğuna ve anlaşıldığına yönelik olarak "okudum ve anladım" şeklindeki beyanda bulunulmasının bu aşamada hukuka uygun bir kullanım teşkil edeceği, ayrıca, aydınlatma yükümlülüğünün yerine getirildiğinin ispatının da veri sorumlusuna ait olduğu,
Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5'inci maddesinin birinci fıkrasının (f) bendinin; *"Veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesi esnasında aşağıda sayılan usul ve esaslara uyulması gerekmektedir: Kişisel veri işleme faalivetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir."* hükmünü amir olduğu, bu kapsamda, ilgili kişinin talebine veya herhangi bir onaya bağlı olmayan aydınlatma yükümlülüğünün kişisel veri işleme faaliyetinin açık rıza da dahil olmak üzere Kanun'da sayılan işleme şartlanndan hangisine dayalı olarak gerçekleştirildiğinden bağımsız olarak her durumda (kişisel veri işlemeye başlamadan önce) veri sorumluları tarafından yerine getirilmesi gerektiği, kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde aydınlatma metni ile açık rıza metninin ayrı ayrı düzenlenerek ilgili kişilere sunulması gerektiği, söz konusu metinlerin tek bir sayfada yer alacak olsa dahi ilgili kişiler tarafından verilecek beyanların niteliği itibariyle farklı olması sebebiyle her iki metnin alt ve üst şeklinde ayrı ayrı yer alması ve her iki metin için ayrı beyanlarda bulunulması gerektiği, değerlendirmelerinde bulunulmaktadır.
Diğer taraftan, uygulamada;

- Açık rıza ve aydınlatma metinlerinin iç içe geçmiş şekilde tek bir metin halinde sunulması,
- Aydınlatma yapıldığına dair ilgili kişilerden onay/rıza talep edilmesi,
- Başka bir veri sorumlusu tarafından düzenlenen metinlerin veri sorumluları tarafından kendi faaliyetlerine uyarlanmadan birebir aynısının kullanılması,
- Aydınlatma metinlerinde açık, anlaşılır ve sade bir dil kullanılmaması, genel nitelikte, farklı anlaşılmaya müsait, eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmesi (örneğin; yurt dışına aktarım yapılmıyorken yurt dışına aktarım yapıldığı izlenimi uyandıran ifadeler kullanılması, *"kişisel verileriniz Kanun'un 5 ve 6'ncı maddesinde belirtilen işleme şartları kapsamında işlenmektedir"* gibi muğlak ifadelere yer verilmesi)
- Çok detaylı, karmaşık ve uzun metinlerin kullanılması,

gibi hukuka aykırılıkların sıkça tespit edildiğine yer verilerek,

- İlgili kişinin talebine veya herhangi bir onaya bağlı olmayan aydınlatma yükümlülüğünün kişisel veri işleme faaliyetinin açık rıza da dahil olmak üzere Kanun'da sayılan işleme şartlarından hangisine dayalı olarak gerçekleştirildiğinden bağımsız olarak her durumda (kişisel veri işlemeye başlamadan önce) veri sorumluları tarafından yerine getirilmesi,
- Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde aydınlatma metni ve açık rıza metinlerinin farklı başlıklar altında ayrı ayrı metinler olarak düzenlenmesi,
- Aydınlatma metni ve açık rıza metinlerinin aynı sayfada bulunması halinde farklı başlıklar altında (alt alta gelecek şekilde) ve iki metin için ayrı beyanlarda bulunulacak şekilde düzenlenmesi,
- Kişisel veri işleme faaliyetinin açık rıza şartı haricindeki Kanun'da sayılan diger işleme şartlarından herhangi birine dayalı olarak gerçekleştirilmesi durumunda sadece aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişilere ayrıca açık rıza metni sunulmaması,
- İlgili kişilerden sadece, aydınlatma metninin okunduğuna ve bilgi edinildiğine ilişkin geri bildirim alınması, aydınlatma metninde yer alan ifadeler için onay/rıza verilmesinin talep edilmemesi,
- Başka bir veri sorumlusu tarafından düzenlenen metinlerin birebir aynısının kullanılmaması, metinlerin her veri sorumlusu tarafından kendi organizasyonuna ve faaliyetlerine uygun şekilde düzenlenmesi,
- Metinlerde açık, anlaşılır ve sade bir dil kullanılması; genel nitelikte, farklı anlaşılmaya müsait, eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemesi,

- Çok detaylı, karmaşık ve uzun metinlerin kullanılmaması (örneğin; Kanun'un 11'inci maddesinin tamamına yer verilmesi metnin uzamasına sebep olacağından, *"Kanun'un 11'nci maddesi kapsamındaki haklarınız"* şeklinde ifade edilmesi),
- Aydınlatma metinlerinde işlenen kişisel veriler ve kategorileri ile birlikte kişisel veri işleme faaliyetinin amaç ve hukuki sebebinin açık ve net bir biçimde ifade edilmesi

gerektiği,

Belirtilen hususların, Kanun'un 12'nci maddesinin birinci fıkrası uyarınca kişisel verilerin hukuka uygun işlenmesini teminen veri sorumluları tarafından alınması gereken idari ve teknik tedbirlerden olduğu ve belirtilen hususlara uygun hareket edilmediğinin tespiti halinde ilgili veri sorumluları hakkında Kanun'un 18'inci maddesi hükümleri gereği işlem tesis edileceğine dair kamuoyunun bilgilendirilmesi ve bu kapsamda veri sorumluları tarafından açık rıza ve aydınlatma metinlerinin ayrı ayrı düzenlenmesi gerektiği hususunda Kanun'un l5'inci maddesinin altıncı fıkrası uyarınca İlke Kararı alınmasına karar verilmiştir. Diğer taraftan, söz konusu ilke kararının ekinde aydınlatma ve açık rıza metinlerine ilişkin iyi ve kötü uygulama şablonu örneklerine de yer verilmektedir.

13- Toplu yapılarda apartman/site sakinlerine ait borç bilgilerinin ortak yerlere asılmasına ilişkin Kurulun 18/02/2026 tarih ve 2026/348 ilke kararında, apaıtman/site yönetimi süreçlerinde çeşitli kişisel veri işleme faaliyetlerinin gerçekleştirildiği, bu kapsamda bilhassa apartman sakinlerinin aidat/avans/demirbaş gideri ve benzeri borçlarına yönelik duyuru yapılması ve diğer apartman sakinlerinin bilgilendirilmesi amaçlarıyla bu kişilere ait ad, soyadı, daire numarası bilgisi, borcun miktarı, ödeme gecikme süresi, ödeme gecikme dönem sayısı, daire sahiplik/kiracılık bilgisi gibi kişisel veri niteliğini haiz bilgilerin yer aldığı listelerin/dokümanların asansörler, bina girişleri, bina koridorları gibi ortak yerlere asıldığının bilindiği,

Kanun'un *"Genel ilkeler"* başlıklı 4'üncü maddesinde kişisel verilerin işlenmesinde uyulması zorunlu ilkelerin düzenlendiği, söz konusu madde hükmü gereğince kişisel verilerin işlenmesinde her hal ve şartta Kanun'un 4'üncü maddesinde sayılan genel ilkelere uyulmasının hukuki bir gereklilik olduğu, bu kapsamda, kişisel verilerin *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması"* ilkesine göre; işlenen kişisel verilerin belirlenen amaçların gerçekleştirilmesi için elverişli olması gerektiği ve kişisel veri işleme amacının gerçekleştirilmesiyle ilgili olmayan kişisel verilerin işlenmemesi gerektiği, ölçülülük ilkesinin ise; kişisel veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması yani kişisel veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği,

Kanun'un 5'inci maddesinde kişisel verilerin işlenme şartlarının düzenlendiği,

Kanun'un 12'nci maddesinin birinci fıkrasından kaynaklanan; *"...kişisel verilerin hukuka aykırı olarak işlenmesini önlemek... "* yükümlülüğünün, işlenen kişisel verilerin türüne göre Kanun'da düzenlenen hukuki sebeplerden herhangi birine dayanılması suretiyle geçerli bir kişisel veri işleme şartına istinaden kişisel verilerin işlenmesini gerektirdiği, yine aynı fıkradan kaynaklanan *"...kişisel verilere hukuka aykırı olarak erişilmesini önlemek..."* yükümlülüğü uyarınca veri sorumlularının işledikleri kişisel verilerin yetkisiz üçüncü kişilerle paylaşılmasını engellemeye yönelik gerekli teknik ve idari tedbirleri almaları gerektiği, *"Kişisel verilerin muhafazasını sağlamak..."* yükümlülüğünün ise kişisel verilerin işlenmesine ilişkin tüm süreçlerde Kanun'a uygunluğun sağlanması ve herhangi bir şekilde Kanun hükümlerine aykırılık teşkil edecek paylaşımların ve erişimlerin önlenmesi anlamına geldiği,

634 sayılı Kat Mülkiyeti Kanunu'nun (634 sayılı Kanun);

"Kat maliklerinin borçları" başlıklı 18'inci maddesinin; *"Kat malikleri gerek bağımsız bölümlerini gerek eklentileri ve ortak yerleri kullanırken doğruluk kaidelerine uymak, özellikle birbirini rahatsız etmemek, birbirinin haklarını çiğnememek ve yönetim planı hükümlerine uymakla, karşılıklı olarak yükümlüdürler.*

Bu kanunda kat maliklerinin borçlarına dair olan hükümler, bağımsız bölümlerdeki kiracılara ve oturma (sükna) hakkı sahiplerine veya bu bölümlerden herhangi bir surette devamlı olarak faydalananlara da uygulanır; bu borçları yerine getirmeyenler kat malikleriyle birlikte, müteselsil olarak sorumlu olur." hükmünü;

"Anagayrimenkulün genel giderlerine katılma" başlıklı 20'nci maddesinin; *"Kat maliklerinden her biri aralarında başka türlü anlaşma olmadıkça: a)Kapıcı, kaloriferci, bahçıvan ve bekçi giderlerine ve bunlar için toplanacak avansa eşit olarak; b) Anagayrimenkulün sigorta primlerin ve bütün ortak yerlerin bakım, koruma, güçlendirme ve onarım giderleri ile yönetici aylığı gibi diğer giderlere ve ortak tesislerin işletme giderlerine ve giderler için toplanacak avansa kendi arsa payı oranında;*

Katılmakla yükümlüdür. c) Kat malikleri ortak yer veya tesisler üzerindeki kullanma hakkından vazgeçmek veya kendi bağımsız bölümünün durumu dolayısıyla bunlardan faydalanmaya lüzum ve ihtiyaç bulunmadığını ileri sürmek suretiyle bu gider ve avans payını ödemekten kaçınamaz.

Gider veya avans payını ödemeyen kat maliki hakkında, diğer kat maliklerinden her biri veya yönetici tarafından, yönetim planına, bu Kanuna ve genel hükümlere göre dava açılabilir, icra takibi yapılabilir. Gider ve avans payının tamamını ödemeyen kat maliki ödemede geciktiği günler için aylık yüzde beş hesabıyla gecikme tazminatı ödemekle yükümlüdür.

Birinci fıkradaki giderlere, kat maliklerinden birinin veya onun bağımsız bölümünden herhangi bir surette faydalanan kişinin kusurlu bir hareketi sebep olmuşsa, gidere katılanların yaptıkları ödemeler için o kat malikine veya gidere sebep olanlara rücu hakları vardır," hükmünü;

"Ortak giderlerin teminatı" başlıklı 22'nci maddesinin; *"Kat malikinin, 20'nci madde uyarınca payına düşecek gider ve avans borcundan ve gecikme tazminatından, bağımsız bölümlerin birinde kira akdine, oturma (sükna) hakkına veya başka bir sebebe dayanarak devamlı bir şekilde faydalananlar da müştereken ve müteselsilen sorumludur. Ancak, kiracının sorumluluğu ödemekle yükümlü olduğu kira miktarı ile sınırlı olup, yaptığı ödeme kira horcundan düşülür.*

Kat malikinin borcu bu yolla da alınamazsa, mahkemece tesbit edilen borcunu ödemiyen kat malikinin bağımsız bölümü üzerine, varsa yöneticinin yoksa kat maliklerinden birinin yazılı istemiyle bu borç tutarı için, diğer kat malikleri lehine kanuni ipotek hakkı tescil edilir. 4721 sayılı Türk Medeni Kanununun 893'üncü maddesinin son fıkrası hükmü burada da uygulanır. Kat maliklerinin, gider borcunu ödemeyen kat maliki veya diğer sorumlulardan olan alacakları önceliklidir. " hükmünü;

"Genel kurul" başlıklı 27'nci maddesinin; *"Anagayrimenkul, kat malikleri kurulunca yönetilir ve yönetim tarzı, kanunların emredici hükümleri saklı kalmak şartiyle, bu kurul tarafından kararlaştırılır."* hükmünü;

"Yönetici" başlıklı (D) kısmının *"Atanması"* başlıklı 34'üncü maddesinin birinci fıkrasının; *"Kat malikleri, anagayrimenkulün yönetimini kendi aralarından veya dışardan seçecekleri bir kimseye veya üç kişilik bir kurula verebilirler; bu kimseye (Yönetici), kurula da (Yönetim kurulu) denir."* hükmünü, aynı maddenin beşinci fıkrasının ise; *"Yönetici her yıl kat malikleri kurulunun kanuni yıllık toplantısında yeniden atanır; eski yönetici tekrar atanabilir."* hükmünü amir olduğu,

634 sayılı Kanun'un 38'inci maddesinde yöneticinin sorumluluğunun düzenlendiği ve bu maddenin birinci fıkrasının; *"Yönetici, kat maliklerine karşı aynen bir vekil gibi sorumludur,"* hükmünü amir olduğu,

Aynı Kanun'un 39'uncu maddesinde yöneticinin hesap verme yükümlülüğünün düzenleme altına alındığı, anılan maddenin; *"Yönetici, yönetim planında yazılı zamanlarda eğer böyle bir zaman yazılmamışsa her takvim yılının birinci ayı, içinde kat malikleri kuruluna,*

anagayrimenkul dolayısiyle o tarihe kadar elde edilen gelirlerin ve yapılmış olan giderlerin hesabına vermekle yükümlüdür.
Kat maliklerinin yarısı isterse, bunların arsa payları ne olursa, olsun yönetim planında yazdı zamanlar dışında da hesabın gösterilmesi yöneticiden istenebilir." şeklinde olduğu, "*Yönetimin denetlenmesi*" başlıklı 41'inci maddenin birinci fıkrasında; "*Kat malikleri kurulu, yöneticinin bu görevdeki tutumunu devamlı olarak denetler ve haklı bir sebebin çıkması halinde onu her zaman değiştirebilir.*" hükmünün düzenlendiği, değerlendirmelerine yer verilerek,
Bahse konu mevzuat hükümleri çerçevesinde bir bütün olarak değerlendirme yapıldığında; apartman/site ve benzeri toplu yapılarda ortak giderlerin karşılanmasının tüm kat maliklerinin sorumluluğunda olduğu, bu tür borçların ifa edilmemesi durumunda diğer kat maliklerinin bu borcun ifasının sağlanması adına doğrudan 634 sayılı Kanun'dan kaynaklanan birtakım haklarının ve imkânlarının bulunduğu, ayrıca bu tür toplu yapılar bakımından uygulamada da sıklıkla görüldüğü üzere aidat/avans/demirbaş gideri ve benzeri ödemelerin yöneticiler tarafından toplandığı, yöneticilerin ise kat maliklerine karşı bir vekil gibi sorumlu olduğu ve belirli aralıklarla kat maliklerine gelir ve giderlere ilişkin hesap verme yükümlülüğünün bulunduğu, ayrıca kat maliklerinin de devamlı suretle yöneticiyi denetleme hak ve yetkisini haiz olduğu, dolayısıyla, apartman sakinlerinin aidat/avans/demirbaş gideri ve benzeri borçlarına yönelik olarak gerekli bilgilendirmenin yapılması amacıyla, bu kişilere ait ad, soyadı, daire numarası bilgisi, borcun miktarı, ödeme gecikme süresi, ödeme gecikme dönem sayısı, daire sahiplik/kiracılık bilgisi gibi kişisel veri niteliğini haiz bilgilerin diğer kat malikleriyle paylaşılmasının gerektiği ve bu yolla gerçekleştirilen kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinin ikinci fıkrasının (a) bendinde yer alan; "*Kanunlarda açıkça öngörülmesi*" ve kat maliklerinin alacak hakkının temini bakımından (e) bendinde bulunan; "*Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması*" şartları kapsamında gerçekleştirildiğinin anlaşıldığı, buna karşın, bilhassa bu bilgilendirmeler yapılırken tercih edilecek usul ve yöntemlerin 6698 sayılı Kanun açısından önem arz ettiği, zira kanunlardan kaynaklanan bir bilgilendirme yükümlülüğü yerine getirilirken dahi bilgilendirmenin gereğinden fazla kişisel veriyi içermemesinin ve bu doğrultuda Kanun'un 4'üncü maddesinde düzenlenen genel ilkelere uygun olmasının sağlanmasının ve söz konusu kişisel verilere konuyla alakası bulunmayan/yetkisiz üçüncü kişiler tarafından erişilmesinin engellenmesinin gerektiği,
Uygulamada sıklıkla kat maliklerinin aidat/avans/demirbaş gideri ve benzeri borçlarına yönelik listelerin/dokümanların toplu yapıların asansörleri, bina girişleri, bina koridorları gibi ortak yerlerine asıldığının görüldüğü, bu tür listelerde sadece borcu bulunanların değil, toplu yapıların bağımsız bölümlerinin maliklerinin/kiracılarının/oturma(sükna) hakkı sahiplerinin tamamının bilgilerinin bulunduğu,
Toplu yapıların asansörleri, bina girişleri, bina koridorları gibi ortak yerlerinin o toplu yapıda ikamet etmeyen/yaşamayan misafirlerin, kargo personellerinin, kuryelerin ve dahi apartman sakinleri tarafından hiç tanınmayan kişilerin sıklıkla bulunabildiği alanlar olduğu, bu bölümlerde yer alan duyuruların/dokümanların/listelerin bu kişilerce de görülebileceği, söz konusu listelerde, bağımsız bölümlerin maliklerinin/kiracılarının/oturma(sükna) hakkı sahiplerinin ad ve soyadı bilgileri bulunmasa dahi listelerde yer alan bilgilerin kişisel veri niteliğini haiz olduğu, zira söz konusu listelerde daire nuınaralarıyla ilişkilendirilıniş bir şekilde borç bilgilerinin yer almasından ve "kişisel veri" kavramının Kanun'da "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" " şeklinde tanımlanmasından hareketle, kişilerin ad ve soyadları bulunmasa dahi ilgili daire numaralarından bu kişilerin belirlenebilmesinin mümkün olduğu, dolayısıyla, bu tür ortak yerlere asılan dokümanlarda/listelerde bulunan kişisel veriler bakımından, Kanun'un 12'nci maddesinden kaynaklanan uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırılığa sebebiyet verileceği, zira, toplu yapıların ortak yerlerine asılan ve kişisel veri içeren listelerin muhatabı belirli olmayan bir kesime ifşa edilmiş ve bu suretle Kanun'a aykırı kişisel veri işlenmesine, bu verilere konuyla alakası bulunmayan/üçüncü kişilerin erişmesine ve dolayısıyla kişisel verilerin Kanun'a uygun bir şekilde muhafaza edilmemesine sebebiyet verilmiş olunacağı, değerlendirmelerine yer verilerek;
Kurul tarafından yapılan değerlendirme neticesinde;

- Apartman sakinlerinin aidat/avans/demirbaş gideri ve benzeri borçlarına yönelik duyuru yapılması ve diğer apartman sakinlerinin bilgilendirilmesi amaçlarıyla bu kişilere ait ad, soyadı, daire numarası bilgisi, borcun miktarı, ödeme gecikme süresi, ödeme gecikme dönem sayısı, daire sahiplik/kiracılık bilgisi gibi kişisel veri niteliğini haiz bilgilerin yer aldığı listelerin/dokümanların asansörler, bina girişleri, bina koridorları gibi ortak yerlere asılması suretiyle gerçekleştirilen kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmadığı,
- Toplu yapıların ortak yerlerine asılan ve kişisel veri içeren listelerin muhatabı belirli olmayan bir kesime ifşa edilmiş ve bu suretle Kanun'a aykırı kişisel veri işlenmesine sebebiyet verilmiş olunmasından hareketle bu durumun Kanun'un 12'nci maddesinde düzenlenen veri güvenliğinin sağlanmasına yönelik gerekli teknik ve idari tedbirlerin alınması yükümlülüğüne aykırılık teşkil ettiği,
- Bu kapsamda, söz konusu bilgilendirmelerin Kanun'un 12'nci maddesine uygun bir şekilde yerine getirilebilmesi için, kapalı e-posta yahut mesajlaşma grupları veya bu hizmete özgülenmiş uygulamalar gibi üçüncü kişi konumunda bulunan kişilerin erişiminin söz konusu olmayacağı usullerin/yöntemlerin kullanılmasının gerektiği

kanaatine varıldığından

- Bu tür uygulamalara ivedilikle son verilmesinin,
- Bu tür duyuruların/listelerin/dokümanların toplu yapıların ortak yerlerinden ivedilikle kaldırılmasının,
- Bu konulara ilişkin kat maliklerine yönelik yapılacak duyurular/bilgilendirmeler için Kanun'un 12'nci maddesine uygun ve sadece ilgililerin erişebileceği başkaca bir usulün/yöntemin uygulanmasının

gerektiği sonucuna varıldığı,
Bu çerçevede, belirtilen hususların, Kanun'un 12'nci maddesinin birinci fikrası uyarınca kişisel verilerin hukuka uygun işlenmesini ve güvenliğinin sağlanmasını teıninen veri sorumluları tarafından alınması gereken teknik ve idari tedbirlerden olduğuna ve belirtilen hususlara uygun hareket edilmediğinin tespiti halinde ilgili veri sorumluları hakkında Kanun'un 18'inci maddesi gereğince işlem tesis edileceğine ilişkin olarak kamuoyunun bilgilendirilmesine ve bu kapsamda Kanun'un 15'inci maddesinin altıncı fıkrası uyarınca İlke Kararı alınmasına karar verilmiştir.

KİŞİSEL VERİLERİN KORUNMASI İLE İLGİLİ BAZI KARAR ÖZETLERİ

Ülkemizde 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun), gerçek kişilerin kişisel verilerinin işlenmesine ilişkin haklarını güvence altına almakta ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uymaları gereken usul ve esasları düzenleyerek kişisel verilerin korunmasına ilişkin hukuki çerçeveyi ortaya koymaktadır. Bunun yanı sıra, Kurumun karar organı olan Kişisel Verileri Koruma Kurulu (Kurul) tarafından alınan kararlar da Kanun'un somut olaylara uygulanmasını sağlayarak uygulamaya yön vermektedir. Bu doğrultuda, Kanun'da öngörülen görev ve yetkiler çerçevesinde Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen gerçekleştirdiği incelemeler sonucunda ihlal tespit etmesi halinde, tespit edilen hukuka aykırılıkların giderilmesi ve idari para cezası uygulanması gibi idari yaptırımlara karar verebilmektedir. Nitekim, Kanun'un yürürlüğe girmesinden bu yana geçen on yıllık süreçte gerek şikâyet üzerine gerek resen gerçekleştirilen incelemeler neticesinde alınan Kurul Kararları, kişisel verilerin korunmasına ilişkin mevzuatın uygulanmasına katkı sağlamaktadır. İlgililerine tebliğ edilen söz konusu Kurul kararlarından, Kurul tarafından gerekli görülenler Kişisel Verileri Koruma Kurumunun (Kurum) web sitesinde kamuoyunun da erişimine sunulmaktadır.

Bu kapsamda, Kurumumuz internet sitesinde yayımlanan bazı Kurul Kararlarına aşağıda yer verilmektedir:

1- Spor salonu hizmeti sunan veri sorumlusu şirketin, üyelerinin giriş-çıkış kontrolü için biyometrik veri işlemesi ve söz konusu verilerin güvenli şekilde muhafaza edildiği konusunda şüphe oluşması üzerine ilgili kişilerce Kuruma intikal ettirilen şikâyetin incelenmesi neticesinde alınan Kurulun 27/02/2020 tarih ve 2020/167 sayılı Kararı ile, veri sorumlusunca spor tesisine giriş esnasında el ve parmak izinin taranması suretiyle kişilerin kimliklerinin doğrulanması faaliyetinin özel nitelikli kişisel veri niteliğindeki biyometrik veri işleme faaliyeti olduğu, diğer taraftan Kanun'un 4'üncü maddesinde düzenlenen genel ilkelerden *"ölçülülük"* ilkesinin kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması ve/veya işlenmemesi gerektiği anlamına geldiği, bu kapsamda veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi gerektiği değerlendirmelerine yer verilerek,

Somut olayda spor salonuna girişte uygulanan el ve parmak izi taraması sisteminin, üyelerin açık rızası bulunsa dahi, hizmetten faydalanmak için üyelere sunulmasının, Kanun'un 4'üncü maddesinde düzenlenen ölçülülük ilkesi gereğince ilgili kişilerden minimum düzeyde veri talep etme ilkesi ile uyumlu olmadığı kanaatine varılarak veri sorumlusu hakkında idari yaptırım uygulanmıştır.

2- Akaryakıt dağıtım firması olarak faaliyet gösteren bir veri sorumlusunun, hâlihazırda Petrol Piyasası mevzuatı gereği işlediği kişisel verileri, taraflarınca yanlış akaryakıt alımının otomatik olarak engellenmesi amacıyla geliştirilen "Araç Tanıma Projesi" uygulaması kapsamında meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvurunun incelenmesi neticesinde alınan 25/03/2019 tarih ve 2019/78 sayılı Kurul Kararı ile, veri sorumlusu tarafından Petrol Piyasası Kanunu ve ilgili mevzuatlarda düzenlenen denetim sistemi kurma zorunluluğu çerçevesinde araç sahiplerinin kişisel verilerini işlemesinin Kanun'un 5'inci maddesinin ikinci fıkrasının (ç) bendinde düzenlenen *"veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması"* hali sayıldığı; bu kapsamda kişisel veri işlenmesi halinde ilgili kişinin açık rızasının aranmadığı, diğer yandan Kanun'un 5'inci maddesinin ikinci fıkrasının (f) bendinde düzenlenen *"ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* hali tespit edilirken veri sorumluları tarafından söz konusu Kurul Kararında yer verilen hususların değerlendirilmesi gerektiği, kişisel verilerin ilk kez işlenmesi için gereken amaçtan farklı olarak başka bir amaca yönelik gerçekleştirilecek yeni bir veri işleme faaliyetinin Kanun'un 5'inci maddesinde sayılan veri işleme şartlarından en az birine dayanması ve ilk amaçtan bağımsız olarak Kanun'un 4'üncü maddesinde düzenlenen ilkelerin tümüne uyumlu olması gerektiği, somut olayda veri sorumlusu tarafından hâlihazırda kayıtlarında bulunan kişisel verilerin otomatik olarak "Araç Tanıma Projesi" sistemine entegre edilmesinin de yeni bir kişisel veri işleme faaliyeti sayıldığı değerlendirmelerine yer verilerek,

Meşru menfaatin ortaya konulmasına ilişkin olarak söz konusu Kurul Kararında yer verilen kriterler esas alınarak yapılan değerlendirme sonucunda, Kanun'un 5'inci maddesinin ikinci fıkrasının (f) bendine göre veri sorumlusunun, tüketicilere ait plaka ve ürün tipi bilgilerini kullanmasının *"İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* kapsamında olduğuna ve veri sorumlusunun erişilebilir ve görünür bir şekilde aydınlatma yükümlülüğünü yerine getirmek ve başka bir amaçla kullanmamak kaydıyla ilgili kişilerin açık rızasını almaksızın bahse konu sistemi kullanmasında Kanun yönünden hukuken bir engel bulunmadığına karar verilmiştir.

3- Kuruma intikal ettirilen bir şikâyette özetle; veri sorumlusu bir banka tarafından, müşteri temsilcisi ile ilgili kişi arasında gerçekleştirilen görüşmeye ilişkin ses kaydı dökümünün ilgili kişiye sağlanması yönündeki talebin yerine getirilmediği ifade edilmektedir. Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan alınan cevabi yazıda özetle; söz konusu görüşmeye ilişkin ses kaydı ve bu kayda ilişkin dökümün 5411 sayılı Bankacılık Kanunu'nun "Sırların Saklanması" başlıklı 73'üncü maddesi ile anılan Kanun'un ilgili maddesi kapsamında Bankacılık Düzenleme ve Denetleme Kurumunca çıkartılan "Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik" kapsamında düzenlenen sır saklama yükümlülüğü uyarınca ilgili kişi ile paylaşılamadığı ifade edilmektedir.

Konuya ilişkin yapılan inceleme neticesinde alınan Kurulun 15/06/2023 tarih ve 2023/1050 sayılı Kararı ile, 5411 sayılı Bankacılık Kanunu ve ilgili mevzuatta düzenlenen sır saklama yükümlülüğünün, kanuni düzenlemelerin öngördüğü hukuka uygunluk hâlleri dışında, müşteri ile ilgili ticari bağlantı nedeniyle elde edilmiş olan bilgi ve olaylar hakkında üçüncü kişilere bilgi verilmemesini gerektirdiği, diğer yandan Kanun'un 11'inci maddesi kapsamında düzenlenen, ilgili kişilerin kendileriyle ilgili kişisel verilerin işlenmesine ilişkin bilgi talep etme haklarının söz konusu veriye erişim hakkını da kapsadığı değerlendirmelerinde bulunularak,

Tarafların görüşme sırasındaki doğrudan ifadelerini içeren söz konusu dökümün, ilgili kişi dışında başkalarının kişisel verileri varsa bunların çıkarılması/maskelenmesi gibi önlemler alınarak ilgili kişiye gönderilmesi ve buna ilişkin tesis edilen işlemler hakkında Kurula bilgi verilmesi yönünde veri sorumlusunun talimatlandırılmasına karar verilmiştir.

4- İlgili kişinin, veri sorumlusu banka bünyesinde müdür yardımcısı pozisyonunda çalışmakta olan eşi ile boşanma davasının mevcut olduğu, bu süreçte banka aracılığıyla ilgili kişiye ait kişisel veri niteliğindeki bilgilerin sorgulandığı ve bu bilgilerin boşanma davası dosyasına sunulduğuna ilişkin Kuruma intikal eden şikâyetin incelenmesi neticesinde alınan Kurulun 12/01/2021 tarih ve 2021/32 sayılı kararında, Kanun'un 4'ncü maddesinde kişisel verilerin işlenmesinde uyulması gereken genel ilkelerin düzenlendiği, Kanun'un 5'nci maddesinde kişisel verilerin işlenme şartlarına yer verildiği, Kanun'un 12'nci maddesinin (1) numaralı fıkrasında veri sorumlularının kişisel verilerin işlenmesinde uygun güvenlik düzeyini temin etmeye yönelik her türlü teknik ve idari tedbiri alması gerektiği; (5) numaralı fıkrasında ise işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kurula bildireceği ve Kurulun gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceğinin düzenlendiği, Kurulun 31/05/2018 tarih ve 2018/63 sayılı Kararı ile bir veri sorumlusu nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması Kanun'un 12'nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine karar verildiği, ayrıca Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile Kanun'un 12'nci maddesinin (5) numaralı fıkrasında yer alan "en kısa sürede" ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun "işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi" durumunu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına karar verildiği, somut olayda veri sorumlusu Banka tarafından ilgili kişinin kişisel verilerinin hukuka uygun olarak işlendiği ve Kanun'un 12'nci maddesi uyarınca gerekli teknik ve idari tedbirlerin alındığı belirtilmekle birlikte Kişisel Verilerin Korunması Uygulama Esas ve Usulleri başlıklı idari ve teknik tedbirlerin listelendiği bir bölüme yer verilmesi dışında isimleri geçen düzenlemelerin, personele verilen eğitimlerin ve veri sorumlusu nezdinde uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü idari ve teknik tedbirin alındığına ilişkin herhangi bir tevsik edici belgenin Kuruma sunulmadığı ve veri sorumlusu Banka tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi kapsamındaki ihlalin varlığından haberdar olunmasına rağmen Kanun'un 12'nci maddesinin (5) numaralı fıkrası uyarınca ve Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı kapsamında ilgilisine ve Kurula herhangi bir veri ihlal bildirimi yapılmadığı değerlendirmelerine yer verilerek,

İlgili kişinin kişisel verisi niteliğindeki kimlik, müşteri işlem ve finansal bilgilerinin (geçmiş yıllara ilişkin karşılıksız çek ve tedbir kararı bilgileri) veri sorumlusu bünyesinde çalışan kişi tarafından sorgulanıp mahkemeye sunulması nedeniyle söz konusu kişisel verilere kanuni olmayan yollarla başkaları tarafından erişim sağlandığı, Kurulun 31.05.2018 tarih ve 2018/63 sayılı "Veri Sorumlusu Nezdindeki Kişisel Verilere Erişim Yetkisi Bulunan Personelin Yetkisi ve Amacı Dışında Söz Konusu Verileri İşlemesi Hususunun Değerlendirilmesine İlişkin İlke Kararı"nda da düzenlenen bu hususun Kanun'un 12'nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirlerin alınmadığının bir göstergesi olduğu dikkate alındığında, veri sorumlusu Banka hakkında idari yaptırım uygulanmasına karar verilmiştir.

5- 18 yaşını doldurmamış ilgili kişiye ait sağlık raporunun imha edilmesine yönelik ilgili kişinin babası tarafından veri sorumlusuna başvurulması ve cevap alınamaması üzerine ilgili kişinin kendisi tarafından Kurumumuza şikâyette bulunulması neticesinde alınan Kurulun 11/08/2020 tarih ve 2020/622 sayılı Kararında; Türk Medeni Kanunu'nun (TMK) 13'üncü maddesinde yaşının küçüklüğü yüzünden veya akıl hastalığı, akıl zayıflığı, sarhoşluk ya da bunlara benzer sebeplerden biriyle akla uygun davranma yeteneğinden yoksun olmayan herkesin TMK'ya göre ayırt etme gücüne sahip olduğunun düzenlendiği, anılan Kanun'un *"Ayırt etme gücüne sahip küçükler ve kısıtlılar"* başlıklı 16'ncı maddesinde ise ayırt etme gücüne sahip küçükler ve kısıtlıların, yasal temsilcilerinin rızası olmadıkça kendi işlemleriyle borç altına giremeyeceği düzenlenmekle birlikte karşılıksız kazanma ve kişiye sıkı sıkıya bağlı hakları kullanmada bu rızanın gerekli olmadığının hüküm altına alındığı; bu çerçevede, kural olarak sınırlı ehliyetsizlerin kişiye sıkı sıkıya bağlı haklarını kullanmada yasal temsilcinin rızasını almak zorunda olmadıkları, bununla birlikte ergin kılınma, nişanlanma, evlenme, evlatlığa alınma gibi bazı kişiye sıkı sıkıya bağlı hakların

TMK uyarınca istisnai olarak yasal temsilcinin rızasına tabi tutulduğu, öğretide kişiye sıkı sıkıya bağlı hakların nispi ve mutlak olarak ayrıldığı, nispi kişiye sıkı sıkıya bağlı hakların bizzat küçük tarafından kullanılabileceği gibi veli tarafından da küçük adına ve hesabına kullanılabildiği, bu kapsamda TMK'nın 16'ncı maddesinin veli için yasaklayıcı bir durum oluşturmadığı, kişisel verilerin korunması hakkının somut olayda nispi kişiye sıkı biçimde bağlı hak olarak ele alınmasının yerinde olacağı, Kişisel Sağlık Verileri Hakkında Yönetmelik uyarınca ayırtım gücüne sahip sınırlı ehliyetsizlerin Kanun'un 11'inci maddesinde belirtilen hakları bizzat kullanabilmesi ile küçük tarafından aksi öngörülmedikçe hem küçüğün hem velisinin e-Nabız verilerine erişim hususunda yetkili kılınmasının somut olayda kişisel verilerin korunması hakkının nispi kişiye sıkı biçimde bağlı hak olduğu yönündeki değerlendirme ile uyumlu olduğu değerlendirmelerine yer verilerek,

Ayırt etme gücü bulunan küçüğün ve velisinin başvuru konusundaki iradelerinin örtüştüğü de dikkate alınarak gerek veri sorumlusuna yapılan başvuru gerek Kurula intikal eden şikâyet bakımından her iki tarafın da hakkı kullanmada yetkili kabul edilebileceğine, somut olayda ilgili kişi ve babasının söz konusu şikâyet hakkını kullanmada yetkili olduğuna karar verilmiştir.

6- İlgili kişiye ait telefon numarasına ilgili kişiye ait olmayan içeriğin gönderilmesi ile ilgili olarak Kuruma intikal ettirilen şikâyetin incelenmesi neticesinde alınan Kurulun 31/05/2019 tarih ve 2019/166 sayılı Kararı ile, gerek ilgili kişiye ait cep telefonu numarasına ilgili kişinin yeğeni olduğu anlaşılan şahsın kişisel verilerinin iletilmesi gerekse ilgili kişiye ait telefon numarasının Kanun'da düzenlenen işleme şartlarından herhangi birine dayanmaksızın işlenmesi şeklindeki tek bir harekete bağlı iki farklı veri işleme faaliyeti gerçekleştirildiği değerlendirmesinde bulunularak veri sorumlusu hakkında idari yaptırım uygulanmasına karar verilmiştir.

7- Satıcı konumundaki kullanıcıların ürünlerini satabildikleri bir e-ticaret platformu tarafından Kurula intikal ettirilen veri ihlal bildiriminin incelenmesi neticesinde alınan Kurulun 08/08/2024 tarih ve 2024/1385 sayılı Kararında, siber saldırgan/saldırganların veri sorumlusu sistemlerinde yer alan bir zafiyeti kullandığı ve bu sayede hedefli bir şekilde saldırıda bulunabildiği, satıcı portalına girişlerde "Bot" trafiğinin önlenmesi adına kullanılan uygulamanın siber saldırgan/saldırganlar tarafından aşılabildiği, dolayısıyla bahse konu uygulamanın bu konuda yetersiz kaldığı, satıcıların ihlale konu portala ilk defa giriş yapmaları ya da son IP'lerinden farklı bir IP adresinden giriş denemeleri yapmaları durumunda tetiklenen tek seferlik parola sisteminin ancak ihlalden sonra uygulamaya konulduğu, dolayısıyla veri sorumlusunca ihlal öncesinde alınması gereken tedbirin ihlalden sonra alındığı, veri sorumlusunun veri ihlalini ancak müşteriler ve satıcılardan gelen şikâyetlerden sonra tespit edebilmesinin ihlalin tespiti noktasında geç kalındığının göstergesi olduğu, satıcıların (kullanıcı hesaplarına giriş yapmasının ardından) bilgi değişikliği ve giriş yapma süreçlerine çift faktörlü kimlik doğrulama aşaması eklenmesi önleminin veri sorumlusu tarafından ihlalden sonra hayata geçirildiği, dolayısıyla ihlalin olumsuz etkilerini azaltabilecek bir tedbirin ihlalin gerçekleşmesinden önce alınmadığı değerlendirmelerinde bulunularak, Kanun'un 12'nci maddesinin (1) numaralı fıkrası hükmü çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında idari yaptırım uygulanmasına karar verilmiştir.

8- İlgili kişinin internet arama motorlarında yapılan aramalardan elde edilen iş yeri e-postasının açık rızası alınmaksızın veri sorumlusu bir pazarlama şirketi tarafından ticari elektronik ileti gönderilmesi suretiyle işlenmesi hakkında alınan Kurulun 01/09/2022 tarih ve 2022/861 sayılı Kararında, şikâyete konu e-posta hesabının şikâyet tarihinde internet arama motorları üzerinden herkesin erişimine açık olacak şekilde alenileştirildiği kanaatine varıldığı, Kanun'un 5'inci maddesinde düzenlenen "ilgili kişinin kendisi tarafından alenileştirilmiş olması" şartı kapsamında kişisel verilerin açık rıza olmaksızın işlenmesinin mümkün olduğu, diğer taraftan kişisel verilerin alenileştirme amacıyla bağlantılı ve amaçla sınırlı olarak işlenebileceği, şikâyete konu somut olayda ise ilgili kişinin iş e-posta adresinin avukatlık mesleğine yönelik yapılacak iletişimler kapsamında aleni hale getirildiği ve pazarlama/reklam amacıyla yapılacak işlemlere ilişkin bir alenileştirme iradesini içermediği, diğer taraftan Avukatlık Kanunu'nun ilgili hükmü uyarınca avukatların ne esnaf ne de tacir sıfatıyla hareket edememesi sebebiyle 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 6'ncı maddesinde yer alan "Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir" hükmüne dayanılarak avukat olan ilgili kişiye onay alınmaksızın ticari ileti gönderilemeyeceği değerlendirmelerine yer verilerek,

İlgili kişinin e-posta adresi bilgisinin Kanun'un 5'inci maddesi çerçevesinde herhangi bir kişisel veri işleme şartı bulunmaksızın reklam ve pazarlama amacıyla işlenmesi sebebiyle veri sorumlusu hakkında idari yaptırım uygulanmasına karar verilmiştir.

9- Veri sorumlusu özel sağlık kuruluşuna ait internet sayfasında randevu almak üzere form doldurulması esnasında, sağlık kuruluşuna ait hizmetlerden ve duyurulardan haberdar olmak üzere başvuru sahiplerinin verilerinin işlenmesine ve bu amaçla kişilerle iletişime geçilmesine onay verilmesinin zorunlu tutulduğuna yönelik olarak Kuruma intikal eden ihbar neticesinde alınan Kurulun 02/05/2023 tarih ve 2023/692 sayılı Kararı ile, Kanun uyarınca açık rızanın, *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* şeklinde tanımlanmakta olduğu, açık rızanın *"özgür irade ile verilme"* unsuru ile kastedilenin kişinin yaptığı davranışın bilincinde ve kendi kararı olması gerektiği, herhangi bir ürün ve/veya hizmetin sunumunun da ilgili kişi tarafından açık rıza verilmesi şartına bağlanmaması gerektiği, somut olayda ilgili kişilerin hizmet almalarına ön adım teşkil eden randevu hizmetinin veri sorumlusunun tanıtımına yönelik açık rıza şartına bağlanmış olduğu, söz konusu hususun ilgili kişilerin bu konudaki iradelerini sakatlayacağı, somut olayda açık rızanın ilgili kişiler bakımından taşıması gereken niteliklerini kaybettiği, bu durumun Kanun'un 4'üncü maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırılık teşkil ettiği değerlendirmelerine yer verilerek,

Açık rızanın *"özgür irade ile verilme"* unsurunun sakatlanması ve veri sorumlusunun sunacağı hizmet kapsamında randevu başvuru formunda işlenmesi gereken kişisel verilerin açık rıza işleme şartı dışındaki işleme şartlarına dayanabilmesi mümkün iken açık rıza işleme şartına dayanmasının Kanun'un 4'üncü maddesinin (1) numaralı fıkrasında yer alan hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırılık teşkil etmesi gerekçelerine dayanılarak veri sorumlusu hakkında idari yaptırım uygulanmasına karar verilmiştir.

10- Veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili alınan Kurulun 26/07/2018 tarih ve 2018/90 sayılı Kararında, bir online platformda iş başvurusunda bulunurken üyelik kaydı yapılmasının zorunlu tutulduğunun, üyelik kaydı yapılması sırasında ise aynı kutucuğun işaretlenmesi yoluyla hem aydınlatma metninin okunduğuna hem de kişisel verilerin işlenmesine açık rıza verildiğine ilişkin onay alınması yoluna gidildiğinin tespit edildiği, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ (Tebliğ) uyarınca, kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rıza alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği, öte yandan aydınlatma yükümlülüğünün yerine getirilmesindeki amaç kişisel verilerin işlenmesi noktasında ilgili kişinin bilgi sahibi olmasının temin edilmesi iken açık rıza alınmasındaki amacın ise veri sorumlusu tarafından kişisel verilerinin işlenmesinin hukuki bir gerekçeye dayandırılması olduğu, bu sebeple ilgili kişi aydınlatma metni sayesinde kişisel veri işleme faaliyeti ile ilgili olarak bilgi edinmiş olmakla birlikte, söz konusu metinde yazılanlara ilgili kişinin açık rıza vermek zorunda olmadığı değerlendirmelerine yer verilerek,

Söz konusu uygulamanın 6698 sayılı Kanun'un amacına ve Tebliğ'e uygun olmadığına karar verilerek hukuka aykırılıkların giderilmesi hususunda veri sorumlusu talimatlandırılmıştır.

* Avrupa Komisyonu'nun *"Digital Omnibus on AI"* teklifine ilişkin olarak Avrupa Veri Koruma Kurulu (EDPB) ve Avrupa Veri Koruma Denetçisi (EDPS) tarafından kabul edilen ortak görüş metni yayımlandı[1]. Konuya ilişkin yapılan basın açıklamasında; AB Yapay Zekâ Tüzüğü'nün *(AI Act)* uygulanmasına ilişkin pratik zorlukların ele alınması amacının desteklendiği, bununla birlikte idari açıdan basitleştirmenin temel hakların korunmasını zayıflatmaması gerektiği belirtilerek, temel hakların korunmasına yönelik daha güçlü önlemler benimsenmesine dair çağrıda bulunuldu.

* Avrupa Komisyonu, AB Veri Tüzüğü'nün *(Data Act)* uygulanmasına destek olmak üzere çeşitli paydaşların katkılarıyla hazırlanan sıkça sorulan sorular dokümanının güncellenmiş versiyonunu yayımladı[2].

* Hamburg Veri Koruma ve Bilgi Edinme Özgürlüğü Komiseri (HmbBfDI), veri işleme faaliyetlerinde AB Genel Veri Koruma Tüzüğü (GDPR) kapsamında meşru menfaat işleme şartının değerlendirilmesine yönelik olarak veri sorumlularına rehberlik etmek amacıyla kapsamlı bir soru seti yayımladı[3]. Söz konusu soru setinin, veri sorumlularının veri işleme faaliyetlerindeki meşru menfaatlerinin ne olduğunu ve ilgili kişilerin hak ve menfaatlerinin yeterince dikkate alınıp alınmadığını sistematik biçimde değerlendirmelerine ve belgelendirmelerine yardımcı olmayı amaçladığı belirtilmektedir. Bu çerçevede; veri işlemenin hangi amaçlarla gerçekleştirildiği ve bu amaçların hukuken meşru olup olmadığı, veri işlemenin gerekli olup olmadığı ve yalnızca gerekli verilerin toplanıp toplanmadığı, menfaatlerin dengelenmesi kapsamında ilgili kişilerin hak ve menfaatlerinin yeterince gözetilip gözetilmediği ile yapılan değerlendirmenin nasıl belgelendirildiği ve düzenli olarak güncellenip güncellenmediği gibi hususlara odaklanılmaktadır.

* Avrupa Parlamentosu Araştırma Servisi (EPRS), sanal özel ağlar (VPN) ve çocukların çevrim içi korunması konusunda bir çalışma yayımladı[4]. Çalışmada, yasal düzenlemelerle zorunlu hâle getirilen çevrim içi yaş doğrulama yöntemlerini atlatmak amacıyla VPN kullanımındaki kayda değer artışa dikkat çekilerek, bu durumun çocukların çevrim içi ortamlarda korunması açısından ortaya çıkardığı zorluklar ele alınmaktadır.

* Fransa Veri Koruma Otoritesi (CNIL), kamuoyu görüşüne başvurulmasının ardından, çerezler ve diğer izleme araçlarına ilişkin olarak birden fazla cihaz (cross-device) üzerinden rıza alınması konusunda nihai tavsiyelerini yayımladı[5].

* Hong Kong Veri Koruma Otoritesi (PCPD), okullara ve ebeveynlere yönelik olarak, çocukları ve gençleri içeren deepfake vakalarıyla başa çıkılmasına yardımcı olmak ve kişisel verilerin korunmasını sağlamak amacıyla pratik tavsiyeler içeren bir araç seti yayımladı[6].

* Ontario Bilgi ve Gizlilik Komiseri (IPC) ile Ontario İnsan Hakları Komisyonu'nun (OHRC), yapay zekâ sistemlerinin sorumlu bir şekilde benimsenmesine rehberlik etmek üzere geliştirdikleri ortak ilkeler yayımlandı[7]. Bu ilkelerin, kuruluşların kamu güvenini koruyarak gizliliğe ve insan haklarına saygı gösterecek şekilde yapay zekâ geliştirmelerine, yerleştirmelerine ve kullanmalarına yardımcı olmak üzere tasarlandığı belirtilmektedir. Bu çerçevede, yapay zekânın sorumlu kullanımına rehberlik etmesi gereken ilkeler; geçerlilik ve güvenilirlik, güvenlik, gizliliğin korunması, insan haklarının güvence altına alınması, şeffaflık ve hesap verebilirlik şeklinde ele alınmaktadır.

* İspanya Veri Koruma Otoritesi (AEPD), iş dünyasında yapay zekânın çeşitli kullanımlarından biri olan yapay zekâ destekli ses transkripsiyonunun veri koruma açısından etkilerinin ele alındığı bir içerik yayımladı[8].

* Fransa Veri Koruma Otoritesi (CNIL), yapay zekâ sistemlerinde veri korumaya ilişkin çeşitli konuların ele alındığı dokümanların İngilizce versiyonlarının tamamını yayımladı[9]. AB Genel Veri Koruma Tüzüğü (GDPR) ile uyumlu yapay zekâ sistemleri oluşturulmasına yönelik olarak yol göstermek üzere hazırlanan dokümanlar; amacın belirlenmesi, uygun hukuki dayanağın tespit edilmesi, gerekli durumlarda veri koruma etki değerlendirmesi yapılması, tasarımdan itibaren mahremiyetin gözetilmesi, ilgili kişilerin uygun şekilde bilgilendirilmesi ve haklarını kullanmalarının sağlanması gibi birçok konuyu içermektedir.

* Birleşik Krallık Veri Koruma Otoritesi (ICO), Etken Yapay Zekâ *(Agentic AI)* konusunda bir rapor yayımladı[10]. Bahse konu raporda; etken yapay zekâ sistemlerinin ortaya çıkarabileceği potansiyel faydalar, kişisel verilerin korunması açısından karşılaşılabilecek riskler, bu sistemlerde inovasyon bakımından Otorite'nin olası beklentileri ve geleceğe yönelik senaryolar gibi başlıklara yer verilmektedir.

1 https://www.edps.europa.eu/press-publications/press-news/press-releases/2026/edpb-and-edps-support-streamlining-ai-act-implementation-call-stronger-safeguards-protect-fundamental-rights_en, 21.01.2026.
2 https://ec.europa.eu/newsroom/dae/redirection/document/108144, 22.01.2026.
3 https://datenschutz-hamburg.de/news/hmbbfdi-veroeffentlicht-fragenkatalog-zur-interessenabwaegung-nach-dsgvo, 06.01.2026.
4 https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2026)782618, 20.01.2026.
5 https://www.cnil.fr/fr/cookies-et-autres-traceurs-recommandations-finales-sur-le-consentement-multi-terminaux, 16.01.2026.
6 https://www.pcpd.org.hk/english/news_events/media_statements/press_20251217.html, 17.12.2025.
7 https://www.ipc.on.ca/en/resources/principles-responsible-use-artificial-intelligence, 21.01.2026.
8 https://www.aepd.es/prensa-y-comunicacion/blog/transcripcion-de-voz-con-ai, 14.01.2026.
9 https://www.cnil.fr/fr/ai-how-to-sheets.
10 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/01/ai-ll-get-that/, 08.01.2026

* Singapur'un bilgi ve iletişim teknolojileri ile medya alanlarından sorumlu düzenleyici otoritesi (IMDA), "Etken Yapay Zekâ *(Agentic AI)* için Model Yapay Zekâ Yönetişim Çerçevesi"ni yayımladı[11]. Kuruluşlara etken yapay zekâ sistemlerini sorumlu bir şekilde nasıl kullanabilecekleri konusunda rehberlik sağlayan ve bu kapsamda nihai sorumluluğun insanlara ait olduğunu vurgulayan Çerçeve, bu tür sistemlerin ortaya çıkarabileceği riskler ile söz konusu risklerin yönetilmesine ilişkin olarak gelişmekte olan iyi uygulamalara dair genel bir bakış sunmaktadır. Bu doğrultuda Çerçeve;

- Uygun etken yapay zekâ kullanım durumlarının seçilmesi ve yapay zekâ aracılarının *(AI Agents)* yetkilerine sınırlar getirilmesi yoluyla, risklerin başlangıç aşamasında değerlendirilmesini ve sınırlandırılmasını,
- İnsan onayının gerekli olduğu önemli kontrol noktalarının belirlenmesi suretiyle, yapay zekâ aracıları bakımından insanların anlamlı biçimde hesap verebilir kılınmasını,
- Yapay zekâ aracılarının yaşam döngüsü boyunca teknik kontrollerin ve süreçlerin uygulanmasını,
- Şeffaflık ve eğitim yoluyla son kullanıcıların sorumluluğunun sağlanmasını

öngören dört temel boyut kapsamında kuruluşlara yol göstermektedir.

* OECD, eğitimde üretken yapay zekânın etkili kullanım şekillerinin incelendiği "OECD Dijital Eğitim Görünümü 2026" raporunu yayımladı[12].

* Avrupa Veri Koruma Kurulu (EDPB), AB Genel Veri Koruma Tüzüğü'nün (GDPR) 17'nci maddesinde düzenlenen "silme hakkı (unutulma hakkı)"na ilişkin 2025 yılı Koordineli Uygulama Çerçevesi *(Coordinated Enforcement Framework)* eylemine dair raporun kabul edildiğini duyurdu[13]. AB genelinde silme hakkının etkin biçimde kullanılmasının sağlanması ve veri sorumlularının bu hakkı uygulamada nasıl yerine getirdiğinin değerlendirmesi amacıyla yürütülen girişime, 2025 yılı boyunca 32 veri koruma otoritesinin katıldığı ve süreç kapsamında küçük-orta ölçekli işletmelerden çok uluslu şirketlere ve çeşitli kamu kurumlarına kadar farklı sektörlerden toplam 764 veri sorumlusunun yanıt verdiği belirtilmektedir. Raporda, veri sorumlularına yönelik çeşitli tavsiyelerle birlikte geliştirilmesi gereken alanlar ortaya konulmuş ve bu çerçevede veri koruma otoriteleri tarafından yedi temel zorluk tespit edilmiştir. Bunlar arasında silme taleplerinin ele alınmasına yönelik yeterli iç prosedürlerin bulunmaması, ilgili kişilere sağlanan bilgilerin yetersizliği, bazı veri sorumlularının silme yerine etkisiz anonimleştirme tekniklerine başvurması, uygulamadaki tutarsızlıklar, saklama sürelerinin belirlenmesinde yaşanan güçlükler ile yedekleme sistemlerinde yer alan kişisel verilerin silinmesine ilişkin sorunlar yer almaktadır. Ayrıca silme hakkının mutlak bir hak olmaması nedeniyle veri sorumlularının bu hakkın uygulanma koşullarını değerlendirme ve silme hakkı ile diğer hak ve özgürlükler arasında yapılması gereken dengeleme testlerini yürütme süreçlerinde de zorluklarla karşılaştıkları belirtilmektedir.

* Avrupa Parlamentosu Araştırma Servisi (EPRS), Avrupa Birliği'nin veri koruma politikasına ilişkin genel çerçeveyi ortaya koyan bir çalışma yayımladı[14]. Bahse konu çalışmada Avrupa Birliği'nin veri koruma politikasının hukuki temelleri, kamuoyundaki algı, veri korumaya ilişkin olarak Avrupa Parlamentosu ve Avrupa Birliği Adalet Divanı'nın rolü ile geleceğe yönelik zorluklar gibi hususlar ele alınmaktadır.

* "Digital Omnibus" teklifine ilişkin olarak Avrupa Veri Koruma Kurulu (EDPB) ile Avrupa Veri Koruma Denetçisi (EDPS) tarafından kabul edilen ortak görüş yayımlandı[15].

* Avrupa Parlamentosu Araştırma Servisi (EPRS), "Digital Omnibus on AI" teklifinin temel noktaları, Parlamento'nun ve diğer AB kurumlarının tutumları, teklifin hazırlanma süreci ve teklife ilişkin başlıca görüşler gibi başlıkların genel olarak ele alındığı bir çalışma yayımladı[16].

* Birleşik Krallık Veri Koruma Otoritesi (ICO), Veri (Kullanım ve Erişim) Yasası kapsamında veri korumaya ilişkin başvuruların veri sorumluları tarafından nasıl ele alınması gerektiğine yönelik bir rehber yayımladı[17].

* Birleşik Krallık Veri Koruma Otoritesi (ICO), kendilerine iletilen şikâyetlerin Otorite tarafından nasıl ele alındığına yönelik bir içerik yayımladı[18].

* Fransa Veri Koruma Otoritesi (CNIL), deepfake'in ne olduğu, ortaya çıkardığı riskler, bireylerin kendilerini nasıl koruyabilecekleri ve yasa dışı içerikleri nasıl bildirebilecekleri ile Otorite'nin bu konudaki faaliyetlerine ilişkin olarak bilgilendirici mahiyette bir içerik yayımladı[19].

* OECD, finans alanında yapay zekânın kullanımına yönelik denetim yaklaşımlarının ve bu çerçevede karşılaşılan zorlukların ele alındığı bir çalışma yayımladı[20]. Söz konusu çalışmada, finansal istikrar ve piyasa bütünlüğü ile finansal tüketicinin korunmasına ilişkin politika hedefleri doğrultusunda, finans alanında sorumlu yapay zekâ kullanımını teşvik etmeyi amaçlayan denetim uygulamaları da incelenmektedir.

11 https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf, 22.01.2026.

12 https://www.oecd.org/en/publications/oecd-digital-education-outlook-2026_062a7394-en.html, 19.01.2026.

13 https://www.edpb.europa.eu/news/news/2026/edpb-identifies-challenges-hindering-full-implementation-right-erasure_en, 18.02.2026.

14 https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)698898, 28.01.2026.

15 Konuya ilişkin olarak Avrupa Veri Koruma Kurulu tarafından yapılan açıklama için bkz. https://www.edpb.europa.eu/news/news/2026/digital-omnibus-edpb-and-edps-support-simplification-and-competitiveness-while_en, 11.02.2026. Konuya ilişkin olarak Avrupa Veri Koruma Denetçisi tarafından yapılan açıklama için bkz. https://www.edps.europa.eu/press-publications/press-news/press-releases/2026/digital-omnibus-edpb-and-edps-support-simplification-and-competitiveness-while-raising-key-concerns_en, 11.02.2026

16 https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2026)782651, 09.02.2026.

17 https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/, 12.02.2026.

18 https://ico.org.uk/make-a-complaint/data-protection-framework/.

19 https://www.cnil.fr/fr/hypertrucage-deepfake, 03.02.2026.

20 https://www.oecd.org/en/publications/supervision-of-artificial-intelligence-in-finance_92743dc1-en.html, 27.01.2026.

* Avrupa Sigorta ve Mesleki Emeklilik Otoritesi (EIOPA), Avrupa sigorta sektöründe üretken yapay zekâ kullanımına ilişkin yürütülen araştırmanın sonuçlarını içeren bir rapor yayımladı[21]. 25 ülkeden 347 kuruluştan alınan yanıtlara dayanan raporda; sektörde üretken yapay zekânın benimsenme düzeyi, sunduğu fırsatlar ve ortaya çıkardığı riskler ile kuruluşların uygulamada karşılaştıkları başlıca zorluklar ele alınmaktadır.

* ABD Çalışma Bakanlığı, ülke genelinde yürütülecek yapay zekâ okuryazarlığı çalışmalarına rehberlik etmek amacıyla Yapay Zekâ Okuryazarlığı Çerçevesi'ni yayımladı[22]. Yapay zekâ okuryazarlığına ilişkin beş temel içerik alanı ile yedi uygulama ilkesinin ortaya konulduğu Çerçeve'nin; işverenler, eğitim sağlayıcıları, eyalet ve yerel kamu kurumları dâhil olmak üzere çeşitli paydaşlardan alınan görüşler doğrultusunda şekillendirildiği, ayrıca yapay zekâ teknolojilerindeki gelişmeler ve iş gücü piyasasındaki dönüşümler doğrultusunda güncelleneceği ifade edilmektedir. Bahse konu Çerçeve'de yapay zekâ okuryazarlığının temel içerik alanları; (1) yapay zekâ ilkelerinin anlaşılması, (2) yapay zekâ kullanım alanlarının keşfedilmesi, (3) yapay zekânın etkili bir şekilde yönlendirilmesi, (4) yapay zekâ çıktılarının değerlendirilmesi ve (5) yapay zekânın sorumlu şekilde kullanılması olarak belirtilmektedir. Diğer taraftan yapay zekâ okuryazarlığının hayata geçirilmesine ilişkin uygulama ilkeleri ise şu unsurları içermektedir: (1) deneyim temelli öğrenmenin teşvik edilmesi, (2) öğrenmenin bağlam içerisine yerleştirilmesi, (3) yapay zekâyı tamamlayıcı nitelikte insan becerilerinin geliştirilmesi, (4) yapay zekâ okuryazarlığı için gerekli ön koşulların ele alınması, (5) sürekli öğrenmeye imkân tanıyan öğrenme yollarının oluşturulması, (6) uygulamayı destekleyecek rollerin hazırlanması ve (7) değişen koşullara hızlı ve uyarlanabilir biçimde yanıt verebilen bir tasarım yaklaşımının benimsenmesi.

* Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bünyesinde faaliyet gösteren Yapay Zekâ Standartları ve İnovasyon Merkezi (CAISI), "Yapay Zekâ Aracısı *(AI Agent)* Standartları Girişimi"nin başlatıldığını duyurdu[23]. Söz konusu girişimin; otonom eylemler gerçekleştirme kapasitesine sahip yapay zekâ aracılarının güven içinde yaygınlaştırılmasını, kullanıcıları adına güvenli biçimde faaliyet göstermesini ve dijital ekosistem genelinde birlikte çalışabilirliğin sağlanmasını amaçladığı belirtilmektedir.

* Avrupa Parlamentosu, "*Digital Omnibus*" teklifini analiz eden ve dijital kurallar arasındaki bağlantılar ile olası örtüşmeleri ortaya koyan bir çalışma yayımladı[24].

* Brezilya Veri Koruma Otoritesi (ANPD), yaş güvence mekanizmalarına ilişkin olarak hazırlanan çalışmanın İngilizce versiyonunu yayımladı[25]. Bahse konu çalışmada; çocukların uygunsuz içeriklere erişmesini veya dijital platformlarda verilerinin hukuka aykırı şekilde işlenmesini önlemeyi amaçlayan farklı teknolojik çözümler analiz edilmektedir.

21 https://www.eiopa.europa.eu/eiopa-survey-generative-ai-shows-swift-cautious-adoption-among-europes-insurers-2026-02-02_en, 02.02.2026.

22 https://www.dol.gov/newsroom/releases/eta/eta20260213, 13.02.2026.

23 https://www.nist.gov/news-events/news/2026/02/announcing-ai-agent-standards-initiative-interoperable-and-secure, 17.02.2026.

24 https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU(2026)772641, 24.02.2026.

25 https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-launches-english-version-of-study-on-age-assurance-mechanisms, 27.02.2026.

* Yeni Zelanda Mahremiyet Komisyonerliği Ofisi, eğitim sektöründe rol alan kişilere yönelik olarak çocukların ve gençlerin mahremiyetlerinin korunması konusunda kapsamlı bir rehber yayımladı[26].

* Dünya genelindeki çeşitli veri koruma otoriteleri, yapay zekâ tarafından üretilen görüntülerin mahremiyetin korunması açısından ortaya çıkarabileceği risklere ilişkin ortak bir bildiri yayımladı[27]. Toplamda 61 otoritenin ortak tutumunu yansıtan bildirinin, yapay zekâ sistemlerinin bireylerin bilgisi ve rızası olmaksızın kişilere ait gerçekçi görüntü ve videolar üretebilmesine ilişkin artan endişeler üzerine hazırlandığı belirtilmekte olup bildiri kapsamında özellikle çocuklara yönelik olarak ortaya çıkabilecek potansiyel zararlara dikkat çekilmektedir.

* OECD, "Etken Yapay Zekâ" *(Agentic AI)* ve "Yapay Zekâ Aracıları" *(AI Agents)* kavramlarının literatürde nasıl tanımlandığını ve kullanıldığını inceleyen; bu kavramların temel özelliklerini, örtüştükleri ve farklılaştıkları noktaları ve bu özelliklerin OECD'nin yapay zekâ sistemi tanımının temel unsurlarıyla ilişkisini analiz eden bir çalışma yayımladı[28].

* UNESCO, yargısal süreçler bağlamında yapay zekâ hakkında sıkça sorulan sorulara yer verilen "Yargıçlar için Yapay Zekânın Temelleri" başlıklı dokümanı yayımladı[29]. Söz konusu dokümanda; "yapay zekâ" ve "üretken yapay zekâ" kavramlarının tanımı, yargı sektöründe yapay zekânın geliştirilmesi ve kullanımı, yargıçlar tarafından yapay zekâ kullanımı, taraflar açısından potansiyel faydalar, olası riskler ile önleyici ve düzeltici tedbirlere ilişkin çeşitli soru ve cevaplar ele alınmaktadır. Dokümanın; yargıçlar, savcılar, mahkeme personeli ve avukatların yapay zekâya, bu teknolojinin yargı alanındaki kullanımına ve sınırlarına ilişkin olarak bilgilendirilmesini amaçladığı, ayrıca doğruluğunun ve güncelliğinin korunması amacıyla belirli aralıklarla gözden geçirileceği ifade edilmektedir.

* Singapur Adalet Bakanlığı, hukuk alanında üretken yapay zekânın kullanımına ilişkin bir rehber yayımladı[30]. Hukuk alanında üretken yapay zekânın güvenli ve sorumlu kullanımını teşvik etmek amacıyla hazırlandığı belirtilen Rehber'de; hukuki çalışmalarda üretken yapay zekâ kullanımına ilişkin yol gösterici üç temel ilke meslek etiği, gizlilik ve şeffaflık olarak ifade edilmektedir. Diğer taraftan bahse konu dokümanda, çeşitli büyüklükteki hukuk bürolarından ve kurum içi hukuk birimlerinden örnek olay incelemelerine de yer verilmektedir.

* Avrupa Veri Koruma Kurulu (EDPB), "Uzman Destek Havuzu" *(Support Pool of Experts)* programı kapsamında, "meşru menfaat" işleme şartına ilişkin tek durak noktası *(one-stop-shop)* mekanizması kapsamında alınan kararlara dair bir vaka özeti çalışması yayımladı[31]. Bahse konu çalışmada, veri koruma otoritelerinin meşru menfaat işleme şartını nasıl değerlendirdiğine ilişkin açıklamalara yer verilmekte ve özellikle meşru menfaatin varlığı, işlemenin gerekliliği ile ilgili kişinin hak ve özgürlükleriyle

26 https://www.privacy.org.nz/tuhono-connect/statements-media-releases/education-sector-guidance-will-help-frontline-workers/, 11.03.2026.

27 https://www.edps.europa.eu/data-protection/our-work/publications/international-conferences/2026-02-23-joint-statement-ai-generated-imagery-and-protection-privacy_en, 23.02.2026.

28 https://www.oecd.org/en/publications/the-agentic-ai-landscape-and-its-conceptual-foundations_396cf758-en.html, Şubat 2026.

29 https://unesdoc.unesco.org/ark:/48223/pf0000396991, Şubat 2026.

30 https://www.mlaw.gov.sg/launch-of-guide-for-using-generative-artificial-intelligence-in-the-legal-sector/, 06.03.2026.

31 https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/one-stop-shop-case-digest-legal-basis_en, 26.03.2026.

dengeleme aşamalarından oluşan üç aşamalı testin uygulanışı örnekler üzerinden ortaya konulmaktadır. Çalışmada ayrıca EDPB'nin 1/2024 sayılı Rehberi, Avrupa Birliği Adalet Divanı içtihadı ile belirli konular bakımından veri koruma otoritelerinin çeşitli kararları ve ulusal mahkeme kararlarına atıfta bulunulmaktadır.

* Birleşik Krallık Veri Koruma Otoritesi (ICO), kişisel verilerin yeniden kullanımının amaçla sınırlılık ilkesi kapsamında hangi durumlarda ilk işleme amacıyla uyumlu kabul edilebileceğine ilişkin bir rehber yayımladı[32]. Söz konusu rehberin, veri koruma ilkelerine ilişkin rehberde amaçla sınırlılık ilkesinin ele alındığı kısmı tamamlayıcı nitelikte olduğu belirtilmektedir.

* Fransa Veri Koruma Otoritesi (CNIL), video gözetimine eşlik eden ses kayıt cihazlarının kullanımına ilişkin olarak yol gösterici mahiyette bir içerik yayımladı[33]. Bahse konu içerikte; kamera/video gözetimi ile ses kaydının kural olarak yasak olduğu, ancak video gözetimi altındaki bir alana ses kaydı yapan bir cihaz kurulmasının çok istisnai durumlarda hukuka uygun olabileceği belirtilmekte olup, bu durumda uygulanacak tedbirlerin gerekli ve ölçülü olması, kayıtların yalnızca doğrulanmış bir olayın varlığı hâlinde saklanması, ilgili kişilerin bilgilendirilmesi ve haklarının güvence altına alınması, çalışanların uygun şekilde eğitilmesi ve belirli durumlarda çalışan temilcilerinin bilgilendirilmesi ve/veya kendilerine danışılması gerektiği vurgulanmaktadır.

* Avrupa Komisyonu'nun "Avrupa Biyoteknoloji Tüzüğü" (European Biotech Act) önerisine ilişkin olarak Avrupa Veri Koruma Kurulu (EDPB) ile Avrupa Veri Koruma Denetçisi (EDPS) tarafından kabul edilen ortak görüş yayımlandı[34].

* İsviçre Federal Veri Koruma ve Bilgi Komiseri (FDPIC), farkındalık kampanyasının bir parçası olarak, çerezler ve benzeri teknolojilerin kullanımına ilişkin bir bilgi notu yayımladı[35]. Söz konusu bilgi notunda, bireylerin verileri üzerindeki kontrollerini korumalarını ve çevrim içi ortamda bıraktıkları dijital izleri en aza indirmelerini sağlamak amacıyla tavsiyeler sunulmakta olup bu çalışmanın, çerez kullanan web siteleri ve uygulamaları işleten veri sorumlularına yönelik hazırlanan Ocak 2025 tarihli rehberin devamı niteliğinde olduğu belirtilmektedir.

* İsviçre Federal Veri Koruma ve Bilgi Komiseri (FDPIC), giyilebilir cihazlara ilişkin bilgilendirici mahiyette bir içerik yayımladı[36]. Söz konusu içerikte; akıllı saatler, fitness takip cihazları ve akıllı gözlükler gibi giyilebilir cihazların veri korumaya ilişkin ortaya çıkarabileceği riskler ele alınmakta olup bu cihazlar aracılığıyla işlenen veriler, cihazların satın alınmasından önce dikkat edilebilecek hususlar, ürünlerin kullanımı sırasında alınabilecek tedbirler, çocuklara ilişkin veriler, üçüncü kişilere ait veriler ile akıllı gözlüklerin durumu başlıkları altında çeşitli açıklamalara yer verilmektedir.

* İsveç Veri Koruma Otoritesi (IMY), akıllı gözlüklerin kullanımına ilişkin bilgilendirici mahiyette bir içerik yayımladı[37]. Bu kapsamda bahse konu içerikte; akıllı gözlüklerle kayıt yapılmasının cep telefonu kamerasıyla kayıt yapılmasına benzer şekilde değerlendirilmesi gerektiği, bu cihazların kayıt yapılmadığı durumlarda dahi kişilerde rahatsızlık ortaya çıkarabileceği, gelişmiş mikrofonları nedeniyle arka plandaki konuşmaların istemeden kaydedilebileceği, elde edilen görüntüler ile diğer verilerin üçüncü kişilerin eline geçme riski bulunduğu, bazı durumlarda kayıt alınmasının veya kayıtların paylaşıma konu edilmesinin suç teşkil edebileceği, başka kişilerin görüntülerinin çevrim içi paylaşımı veya akıllı gözlüklerin ticari kullanımı durumlarında AB Genel Veri Koruma Tüzüğü (GDPR) kapsamındaki yükümlülüklerin gündeme gelebileceği ve ziyaret edilen bazı yerlerde akıllı gözlük kullanımına izin verilmeyebileceği hususlarının akılda tutulması önerilmektedir.

* Birleşik Krallık Veri Koruma Otoritesi (ICO), Birleşik Krallık'ta faaliyet gösteren sosyal medya ve video paylaşım platformlarına yönelik olarak, çocukların kendileri için tasarlanmamış hizmetlere erişimini önlemek amacıyla yaş doğrulama önlemlerinin güçlendirilmesi çağrısında bulunan açık mektup yayımladı[38].

* Birleşik Krallık Veri Koruma Otoritesi (ICO) ile İletişim Ofisi (Ofcom), yaş güvencesi bağlamında çevrim içi güvenlik ile veri koruma alanlarının kesişiminde yer alan temel hususlara ilişkin ortak bir açıklama yayımladı[39]. Bahse konu açıklamanın, Çevrim içi Güvenlik Yasası ile Birleşik Krallık veri koruma mevzuatı kapsamına giren ve çocuklar tarafından erişilmesi muhtemel hizmetlere yönelik olduğu, öte yandan kuruluşların hem çevrim içi güvenlik hem de veri koruma yükümlülüklerine uyum sağlamasına destek olmak amacıyla ICO ve Ofcom'un yaş güvencesine ilişkin mevcut politika çerçevesinin temel unsurlarını pratik bir yaklaşımla özetlediği belirtilmektedir.

* Avustralya Bilgi Komiserliği Ofisi (OAIC), çevrim içi ortamlarda yaş kontrolleriyle karşılaşan bireylerin mahremiyetinin korunmasını sağlamaya yardımcı olmak üzere, yaş güvencesi teknolojileri konusunda kuruluşlara yol gösterici mahiyette bir rehber yayımladı[40]. Bu kapsamda kuruluşlara yönelik tavsiyeler arasında; yaş kontrollerinin gerekli olup olmadığının değerlendirilmesi ve tasarımdan itibaren mahremiyet yaklaşımının benimsenmesi, yaş güvencesi ekosisteminin güvenliğinin sağlanması için gerekli özenin gösterilmesi, risk değerlendirmesi temelinde ölçülü ve veri minimizasyonuna uygun yöntemlerin seçilmesi, hassas nitelikteki bilgilerin toplanması veya verilerin ikincil kullanımı ya da paylaşılması söz konusu olduğunda rıza taleplerinin açık ve anlaşılır bir şekilde oluşturulması ve aydınlatma metinlerinde şeffaflık sağlanarak bireylere basit ve kolay erişilebilir şikâyet mekanizmaları sunulması gibi hususlar yer almaktadır.

32 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/compatibility-and-the-reuse-of-personal-information/, 23.03.2026.

33 https://www.cnil.fr/fr/les-dispositifs-de-captation-sonore-couples-la-videoprotection, 20.03.2026.

34 Konuya ilişkin olarak Avrupa Veri Koruma Kurulu tarafından yapılan açıklama için bkz. https://www.edpb.europa.eu/news/news/2026/edpb-and-edps-support-harmonisation-clinical-trials-under-european-biotech-act-call_en, 12.03.2026. Konuya ilişkin olarak Avrupa Veri Koruma Denetçisi tarafından yapılan açıklama için bkz. https://www.edps.europa.eu/press-publications/press-news/press-releases/2026/edpb-and-edps-support-harmonisation-clinical-trials-under-european-biotech-act-call-specific-safeguards-sensitive-health-data_en, 12.03.2026.

35 https://www.edoeb.admin.ch/en/factsheet-cookies, 31.03.2026.

36 https://www.edoeb.admin.ch/en/smart-devices, 25.03.2026.

37 https://www.imy.se/en/individuals/camera-surveillance/to-be-a-controller-of-personal-data/smart-glasses/, 25.03.2026.

38 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/03/open-letter-issued-to-tech-firms-to-strengthen-age-checks-and-protect-children-s-data/, 12.03.2026.

39 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/03/joint-statement-from-ico-and-ofcom-on-age-assurance/, 25.03.2026.

40 https://www.oaic.gov.au/news/media-centre/privacy-commissioner-publishes-new-guidance-to-ensure-proportionate-age-assurance-as-a-gateway-to-access-online-experiences, 17.03.2026.

* Avrupa Parlamentosu Araştırma Servisi (EPRS), AB Yapay Zekâ Tüzüğü'nün *(AI Act)* uygulanmasına ilişkin bir bilgi notu yayımladı[41]. Söz konusu dokümanda, yapay zekâ sistemleri ve genel amaçlı yapay zekâ modellerine yönelik kurallar, yönetişim çerçevesi, ulusal düzeyde uygulama ile AB düzeyinde uygulama gibi hususlara yer verilmektedir.

* Dünya Ekonomik Forumu, kuruluşların yapay zekânın potansiyelini en üst düzeye çıkarabilmesine yönelik kurumsal dönüşümü ele alan bir çalışma yayımladı[42]. Bahse konu çalışmada, yapay zekânın merak ve erken deneme aşamalarının ötesine geçtiği, farklı sektörlerde kuruluşların yapay zekânın benimsenmesinden ölçülebilir kazanımlar elde ettiği, ancak bu kazanımların çoğunun kuruluş bakımından hâlen kurumsal işleyişe tam olarak gömülü olmayan, parçalı faydalar olarak kaldığı belirtilmektedir. Bu çerçevede çalışmada, artık temel meselenin yapay zekânın işe yarayıp yaramadığı değil, kuruluşların bu teknolojinin tam ve sürdürülebilir değerini ortaya çıkarabilmek için nasıl değişmesi gerektiği olduğu ifade edilmektedir. Çeşitli sektörlerden 450'den fazla yöneticiyle yapılan görüşmelere dayanan çalışmada, yapay zekânın hâlihazırda kurumsal düzeyde etki yarattığı beş kritik odak alanı incelenmekte olup bunlar gerçek zamanlı ve bireyselleştirilmiş müşteri deneyimleri, verimli ve dayanıklı operasyonlar, hızlandırılmış araştırma ve geliştirme ile çığır açıcı inovasyon, öngörücü ve yapay zekâ destekli stratejik planlama ile veriye dayalı, kişiselleştirilmiş çalışan deneyimi ve iş gücü planlaması olarak belirtilmektedir.

* Avrupa Veri Koruma Kurulu (EDPB), bilimsel araştırma amaçlarıyla kişisel verilerin işlenmesine ilişkin hazırlanan rehberin kamuoyu görüşüne açıldığını ve görüşlerin 25 Haziran tarihine kadar iletilebileceğini duyurdu[43]. Söz konusu rehberde; "bilimsel araştırma" kavramına açıklık getirilmekte ve bir veri işleme faaliyetinin AB Genel Veri Koruma Tüzüğü (GDPR) anlamında bilimsel araştırma amacı taşıyıp taşımadığının değerlendirilmesinde dikkate alınabilecek faktörlere dikkat çekilmektedir. Rehber'de ayrıca; bilimsel araştırma amacıyla kişisel verilerin işlenmesine ilişkin hukuki çerçeve, ilgili kişilerin hakları, araştırma faaliyetlerinde yer alan tarafların rolleri ile uygun güvenceler ve gerekli teknik-idari tedbirler gibi hususlar ele alınmaktadır.

* Avrupa Veri Koruma Kurulu (EDPB), veri koruma etki değerlendirmesi şablonunun kamuoyu görüşüne açıldığını ve görüşlerin 9 Haziran tarihine kadar iletilebileceğini duyurdu[44].

* Fransa Veri Koruma Otoritesi (CNIL), insan kaynakları yönetimi faaliyetleri bakımından kişisel verilerin saklanma sürelerinin belirlenmesine yardımcı olmak amacıyla hazırlanan bir rehber yayımladı[45]. Bahse konu rehberin; işe alım, personelin idari yönetimi, ücret yönetimi, mal ve kişi güvenliği, şirket araçlarının yönetimi, iş yerinde telefon görüşmelerinin dinlenmesi ve kaydedilmesi, toplu iş ilişkilerinin yönetimi, iş kazalarının yönetimi, dava ve dava öncesi süreçlerin yönetimi ile uyarı mekanizmalarının yönetimi gibi insan kaynakları yönetimi bağlamında sık karşılaşılan süreçleri kapsadığı belirtilmektedir.

* Avustralya'da sosyal medya asgari yaş sınırının uygulanmasına ilişkin mevcut görünümü ortaya koyan, eSafety'nin Mart 2026 tarihli uyum güncellemesi yayımlandı[46].

- Bu kapsamda, platformların söz konusu yükümlülüğe uyum sağlamak amacıyla birtakım adımlar attığı, bu doğrultuda 10 Aralık 2025'ten bu yana 16 yaş altındaki çocuklara ait çok sayıda sosyal medya hesabının kaldırıldığı, devre dışı bırakıldığı veya platformlara girişinin kısıtlandığı ifade edilmektedir. Ayrıca Mart 2026 başı itibarıyla 310 binden fazla ilave hesabın platformlara erişiminin engellendiği belirtilmektedir.

- Bununla birlikte, 16 yaş altındaki çocukların önemli bir bölümünün hesaplarını korumaya devam ettiğine, yeni hesaplar oluşturabildiğine veya platformların yaş güvencesi sistemlerini geçebildiğine dikkat çekilmektedir.

- Belgede ayrıca, 10 Aralık 2025 öncesinde beyan edilen yaş 16'nın altında olmasına rağmen bazı platformların kullanıcılara yaş güvencesi süreçlerine başvurmalarını teşvik eden mesajlar gönderdiği, bazı durumlarda 16 yaş altındaki kullanıcıların aynı yöntemi tekrar tekrar deneyerek 16 yaş ve üzeri sonucuna ulaşabildiği, 16 yaş altındaki kullanıcıların bildirilmesine yönelik mekanizmaların özellikle ebeveynler bakımından yeterince erişilebilir ve etkili olmadığı ve bazı platformların 16 yaş altındaki çocukların hesap sahibi olmasını önlemek için yeterli tedbirleri almamış göründüğü yönündeki temel uyum tespitlerine yer verilmektedir.

- Diğer taraftan yaptırım önceliğinin, 16 yaş altı çocukları platformlarından uzak tutmak için makul adımları atmayan, sistematik yetersizlik gösteren ve genç kullanıcılar bakımından daha yüksek risk taşıyan platformlara verileceği ifade edilmektedir.

- Bunun yanında, "makul adımlar" ölçütünün sabit ve tek tip bir test olarak değil, her platform bakımından somut koşullar çerçevesinde değerlendirileceği, sistem ve süreçlerin iyileştirilmesinin zaman aldığı kabul edilmekle birlikte düzenlemenin yürürlüğe girmesinin üzerinden üç aydan fazla süre geçmiş olması nedeniyle daha fazla iyileştirmenin kısa sürede görülmesinin beklendiği belirtilmektedir.

* Birleşik Krallık Veri Koruma Otoritesi (ICO), 4-11 yaş arası çocuğu bulunan ebeveynlere, çocukların çevrim içi mahremiyetinin korunmasına yönelik bilgi, rehberlik ve materyal sunmak amacıyla *"Switched on to Privacy"* isimli bir kampanya başlatıldığını ve ilgili içeriklere kampanya sayfası üzerinden ulaşılabileceğini duyurdu[47].

* Avrupa Komisyonu, çevrim içi platformlara erişimde kullanılmak üzere geliştirilen yaş doğrulama uygulamasının teknik olarak hazır olduğunu ve yakın bir zamanda kullanıma sunulacağını duyurdu[48]. Konuya ilişkin yapılan açıklamada, söz konusu uygulamanın kullanıcı dostu olduğu,

41 https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2026)785670, 17.03.2026.

42 https://www.weforum.org/publications/organizational-transformation-in-the-age-of-ai-how-organizations-maximize-ais-potential/, 16.03.2026.

43 https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/guidelines-12026-processing-personal-data_en, 16.04.2026.

44 https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en, 14.04.2026.

45 https://www.cnil.fr/fr/referentiel-durees-conservation-donnees-rh, 02.04.2026.

46 https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf?v=1774905032806.

47 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/04/one-click-too-many-75-of-parents-fear-their-kids-arent-making-safe-choices-online/, 07.04.2026. Bahse konu kampanya sayfasını görüntülemek için bkz. https://ico.org.uk/switched-on-to-privacy/.

48 https://ec.europa.eu/commission/presscorner/detail/en/statement_26_817, 15.04.2026.

pasaport veya kimlik kartı kullanılarak kurulabildiği, telefon, tablet ve bilgisayar dâhil olmak üzere farklı cihazlarda çalıştığı ve açık kaynak kodlu olarak geliştirildiği ifade edildi. Ayrıca uygulamanın, kullanıcıların başka kişisel bilgilerini paylaşmaksızın yaşlarını doğrulamalarına imkân tanıdığı, bu yönüyle yüksek mahremiyet standartlarını gözettiği ve anonimliğin sağlanması nedeniyle kullanıcıların takip edilemeyeceği belirtildi.

* Belçika Veri Koruma Otoritesi (APD), "Yapay Zekâ & Veri Koruma" başlıklı seri kapsamında, yapay zekânın mahremiyet üzerindeki etkisini ele alan bir çalışma yayımladı[49]. Bireyler ve işletmeler nezdinde yapay zekâ ile veri koruma arasındaki ilişkiye dair farkındalığın artırılmasını amaçlayan girişimin ilk yayını niteliğinde olan çalışma, günlük hayatta yapay zekâ sistemlerini kullanan veya bu sistemlerle etkileşimde bulunan bireylere yönelik hazırlanmıştır. Bu kapsamda, yapay zekâ sistemlerinin nasıl çalıştığı, hangi tür kişisel verilerin işlendiği, bu sistemlerin bireyler açısından doğurabileceği riskler ile veri koruma mevzuatı kapsamında bireylere tanınan haklar genel hatlarıyla ele alınmaktadır.

* Birleşik Krallık'ta dijital düzenleme alanında yetkili düzenleyici kurumlar arasında iş birliği platformu olan Digital Regulation Cooperation Forum (DRCF), etken yapay zekânın *(agentic AI)* geleceğine ilişkin bir çalışma yayımladı[50]. Söz konusu çalışmada, etken yapay zekâdan ne anlaşılması gerektiği, ortaya çıkardığı fırsatlar ve riskler, bu sistemlerin güvenli ve güvenilir biçimde benimsenmesi için dikkate alınması gereken hususlar ile yönetişim, veri koruma ve siber güvenlik, tüketici hakları ile pazar dinamikleri ve rekabet alanlarındaki olası düzenleyici yansımalar ele alınmaktadır.

* Avrupa Veri Koruma Kurulu (EDPB)[51], Hollanda Veri Koruma Otoritesi (AP)[52] ve Danimarka Veri Koruma Otoritesi (Datatilsynet)[53] 2025 yılına ilişkin faaliyet raporunu yayımladı.

* Ülkemizde Rekabet Kurumu, yapay zekâ alanında yaşanan hızlı gelişmelerin veri, hesaplama gücü ve platform ekosistemleri etrafında şekillenen yeni bir rekabet düzeni ortaya çıkardığını ve bu yeni düzende rekabetin nasıl oluştuğunun, nasıl sürdürüldüğünün ve kimler tarafından belirlendiğinin yeniden tanımlandığını ifade ederek, bu dönüşümün piyasalar üzerindeki etkilerini bütüncül bir perspektifle değerlendirmek ve ortaya çıkan rekabet risklerini zamanında tespit edebilmek amacıyla yapay zekâ ekosistemine yönelik kapsamlı bir sektör incelemesi başlatıldığını duyurdu[54].

49 https://www.autoriteprotectiondonnees.be/citoyen/actualites/2026/04/13/serie-ia-protection-des-donnees---l-impact-de-l-intelligence-artificielle-sur-la-vie-privee, 13.04.2026.

50 https://www.drcf.org.uk/publications/papers/thefutureofagenticai, 31.03.2026.

51 https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2025_en, 09.04.2026.

52 https://www.autoriteitpersoonsgegevens.nl/actueel/jaarverslag-ap-2025-sneller-zichtbaar-en-richtinggevend-optreden-in-de-digitale-wereld, 02.04.2026.

53 https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/mar/datatilsynets-aarsberetning-2025, 31.03.2026.

54 https://www.rekabet.gov.tr/tr/Guncel/yapay-zekaya-rekabet-kurumu-sektor-incel-d21eee058332f11193f70050568585c9, 07.04.2026.

28 OCAK VERİ KORUMA GÜNÜ

28 Ocak Veri Koruma Günü münasebetiyle, Kurumumuz ve Karadeniz Teknik Üniversitesi iş birliğinde, "Kamuda Yapay Zekâ Kullanımı ve Kişisel Verilerin Korunması" etkinliği gerçekleştirildi. Kamu kurum ve kuruluşlarının temsilcileri, akademisyenler ve sektör temsilcilerinin katılımıyla düzenlenen etkinlikte; yapay zekâya genel bakış, kamuda yapay zekâ kullanımı, yapay zekâ ve kişisel verilerin korunması konuları ele alındı.

7 NİSAN KİŞİSEL VERİLERİ KORUMA GÜNÜ

7 Nisan Kişisel Verileri Koruma Günü, Kurumumuz tarafından düzenlenen çeşitli etkinliklerle kutlandı. Programın açılış konuşması Kurum Başkanımız Prof. Dr. Faruk BİLİR tarafından yapıldı. Etkinlikte ortaöğretim öğrencilerine yönelik olarak Kurumumuz uzmanları tarafından kişisel veri farkındalığını artırmaya yönelik sunumlar gerçekleştirildi.

Etkinlik çerçevesinde düzenlenen slogan, karikatür ve makale yarışmalarında dereceye giren katılımcılara ödülleri takdim edildi. Ayrıca etkinlik kapsamında kişisel verilerin korunması temalı sergi ziyarete açıldı, ayrıca öğrenciler Kurumumuz kütüphanesini ziyaret ederek bilgi kaynaklarıyla buluşma imkanı elde etti.

Öte yandan, Kişisel Verilerin Korunması Kanunu'nun 10. yılı vesilesiyle, Kurum Başkanımız Prof. Dr. Faruk BİLİR ve Kurumumuz personelinin katılımıyla fidan dikme etkinliği gerçekleştirildi.

10. YILINDA KİŞİSEL VERİLERİN KORUNMASI KANUNU

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girişinin onuncu yılı vesilesiyle, Kurumumuz ve Selçuk Üniversitesi iş birliği ile "Mahremiyetin On Yılı: Geleceği Mahremiyetle Tasarlamak" etkinliği gerçekleştirildi. Etkinlikte; veri koruma hukukunun gelişimi, mahremiyet hakkının dönüşümü ve yeni nesil veri koruma mimarisi gibi konular uzmanlar tarafından değerlendirildi.

VERİ KORUMANIN 10. YILI: GDPR IŞIĞINDA GELECEK PERSPEKTİFİ

Kişisel Verilerin Koruması Kanunu'nun yürürlüğe girişinin onuncu yılı vesilesiyle, Kurumumuz, Mevzuat Uyum Derneği, İTÜ Yapay Zekâ ve Veri Bilimi Uygulama ve Araştırma Merkezi iş birliğinde "Veri Korumanın 10. Yılı: GDPR Işığında Gelecek Perspektifi" etkinliği gerçekleştirildi.

YAPAY ZEKÂ ÇAĞINDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN YAKLAŞIMLAR SEMPOZYUMU

Kurumumuz ve Trabzon Üniversitesi iş birliği ile, "Yapay Zekâ Çağında Kişisel Verilerin Korunmasına İlişkin Hukuki, Etik ve Toplumsal Yaklaşımlar" sempozyumu düzenlendi. Etkinlikte; hukukun regülasyon gücü ve sınırları, yapay zekâ uygulamalarının değerlendirilmesi ve yapay zekâ tarafından kişisel verilerin işlenmesinde olası riskler ve önlemler konuları masaya yatırıldı.

YAPAY ZEKÂ ÇAĞINDA KİŞİSEL VERİLERİN KORUNMASI ETKİNLİĞİ

Kurumumuz ve Atılım Üniversitesi iş birliğinde "Yapay Zekâ Çağında Kişisel Verilerin Korunması" etkinliği gerçekleştirildi. Etkinlikte, gelişen yapay zekâ teknolojilerinin hukuk sistemi ve veri mahremiyeti üzerindeki etkileri değerlendirildi.

KİŞİSEL VERİLERİN KORUNMASI KANUNU VE UYGULANMASI SEMİNERİ

Kurumumuz ve Bursa Uludağ Üniversitesi iş birliğinde, Kişisel Verilerin Korunması Kanunu hakkında seminer düzenlendi. Seminerde, Kanuna ilişkin genel hususlar ve Kanun'un uygulanması hususunda bilgiler paylaşıldı.

KVKK VE DİJİTAL DÜNYADA VERİ GÜVENLİĞİ ETKİNLİĞİ

Kurum Başkanımız Prof. Dr. Faruk BİLİR, Recep Tayyip Erdoğan Üniversitesi (RTEÜ) ve Türkiye Gençlik Vakfı (TÜGVA) iş birliğiyle düzenlenen etkinlik kapsamında öğrencilerle bir araya geldi. Etkinlikte, dijital dönüşüm sürecinde veri güvenliğinin önemi ve Kişisel Verilerin Korunması Kanunu'nun bu çerçevedeki rolü ele alındı.

ADALET TEŞKİLATINI GÜÇLENDİRME VAKFI (ATGV) İLE FARKINDALIK ETKİNLİĞİ

Kurumumuz tarafından Adalet Teşkilatını Güçlendirme Vakfı (ATGV) personeline yönelik farkındalık etkinliği gerçekleştirildi. Etkinlikte, Kişisel Verilerin Korunması Kanunu ile ilgili temel konularda bilgi paylaşımında bulunuldu.

DİJİTAL OKURYAZARLIK PROJESİ (2.ETAP)

Öğretmenlere yönelik olarak düzenlenen, bu kapsamda Kişisel Verilerin Korunması Kanunu, dijital okuryazarlık, okulda veri güvenliği, dijital ayak izleri, dijital mahremiyet ve dijital etik konularında bilgi paylaşımını hedefleyen Güvenli Gelecek İçin Dijital Okuryazarlık Projesi'nin ikinci etabı tamamlandı. Projenin ikinci etabı Trabzon, Ordu, Samsun, Bursa, Balıkesir, Aydın, Denizli, Nevşehir, Kayseri, Yozgat, Tekirdağ, Kocaeli, Sakarya, Eskişehir, Van, Erzurum ve Malatya olmak üzere 17 ilimizde gerçekleştirildi.

ÇARŞAMBA SEMİNERLERİ

Kamuoyunu kişisel verilerin korunması mevzuatı hakkında bilgilendirmeye yönelik olarak akademisyenlerin, Kurum personelinin veya diğer kurum ve kuruluşlarda görev yapan ve alanında uzman olan kişilerin katılımıyla düzenlenen "Çarşamba Seminerleri" devam ediyor.

Bu kapsamda;

"Dijital Profilleme ve Algoritmik Yönlendirme"

"Klinik Araştırmalarda Kişisel Verilerin Korunması"

"İşe Alım Sürecinde Yapay Zekâ Kullanımı"

"Yapay Zekâ Hukuku ile Kişisel Verilerin Korunması Arasındaki İlişki"

"Kişisel Verilerin Ölümden Sonra Korunması"

"Yapay Zekânın Seçim Süreçlerinde Kullanımı: Türkiye-ABD Karşılaştırması"

"Finansal Okuryazarlıkta Güncel Gelişmeler"

konuları, alanında uzman kişiler tarafından ele alınarak çeşitli bakış açılarıyla değerlendirildi.

İLKE KARARLARI

Kişisel Verileri Koruma Kurulu tarafından;

- Sadakat Kart Üyeliği Bulunan Bir Kişinin Cep Telefonu Numarasının veya Sadakat Kart Numarasının Üçüncü Bir Kişi Tarafından Alışveriş Esnasında Kullanılması Hakkında İlke Kararı

- Veri Sorumluları Tarafından Açık Rıza ve Aydınlatma Metinlerinin Ayrı Ayrı Düzenlenmesi Gerektiği Hakkında İlke Kararı

- Toplu Yapılarda Apartman/Site Sakinlerine Ait Borç Bilgilerinin Ortak Yerlere Asılması Hakkında İlke Kararı

yayımlandı.

KAMUOYU DUYURULARI

Kişisel Verileri Koruma Kurulu tarafından;

- 04.09.2025 tarihli ve 2025/1572 sayılı Kurul Kararının Uygulama Esaslarına İlişkin Kamuoyu Duyurusu

- Mobil Uygulamalar Üzerinden Gönderilen Anlık Bildirimlere İlişkin Kamuoyu Duyurusu

- Kişisel Veri İhlal Bildirimlerine İlişkin Kamuoyu Duyurusu

- Kamu Kurumlarında Yurt Dışı Menşeli Haberleşme Uygulamaları Kullanımına İlişkin Kamuoyu Duyurusu

- Google Assistant Hakkında Kamuoyu Duyurusu

- GROK Yapay Zekâ Asistanı Hakkında Kamuoyu Duyurusu

- Çocukların Sosyal Medya Kullanımında Kişisel Verilerinin Korunmasına İlişkin Kamuoyu Duyurusu

- İş Ortaklığı/Konsorsiyum/Adi Ortaklık Gibi Yapılar Nezdinde Gerçekleştirilen Faaliyetlerde İşlenen Kişisel Verilerin VERBİS'e Bildirimi Hakkındaki Kamuoyu Duyurusu

yayımlandı.

Kişisel Verilerin VERBİS'e Bildirimi Hakkındaki Kamuoyu Duyurusu yayımlandı.

“ETKEN YAPAY ZEKÂ (AGENTIC AI)” DOKÜMANI

Etken yapay zekâ sistemlerinin ne olduğuna, bu sistemlerde “Yapay Zekâ Aracıları”nın (AI Agents) hangi işlevleri yerine getirdiğine, potansiyel kullanım durumlarına ve beraberinde getirebileceği risklere ilişkin genel bir değerlendirme sunan; etken yapay zekâ sistemlerinin yaşam döngüsü boyunca kişisel verilerin korunması açısından dikkate alınabilecek hususları genel hatlarıyla ele alan “Etken Yapay Zekâ (Agentic AI)” dokümanı yayımlandı.

“İŞ YERLERİNDE ÜRETKEN YAPAY ZEKÂ ARAÇLARININ KULLANIMI” DOKÜMANI

Üçüncü taraflarca sunulan ve kamuya açık olarak erişilebilen üretken yapay zekâ araçlarının iş yerlerinde kullanımına ilişkin genel bir çerçeve sunmak amacıyla hazırlanan; şirket, kurum ve kuruluşlar nezdinde farkındalık oluşturmayı, olası risklere dikkat çekmeyi ve bilinçli kullanımı teşvik etmeyi hedefleyen “İş Yerlerinde Üretken Yapay Zekâ Araçlarının Kullanımı” dokümanı yayımlandı.

“QR KODLARLA GELEN RİSK: QUISHING” DOKÜMANI

QR kodlar aracılığıyla gerçekleştirilen oltalama saldırılarının (Quishing) ele alındığı; bu saldırı türünün ne olduğunu, nasıl gerçekleştirildiğini, nasıl tespit edilebileceğini ve quishing saldırılarına karşı bireyler tarafından dikkat edilmesi gereken hususları genel hatlarıyla açıklayan “QR Kodlarla Gelen Risk: Quishing” dokümanı yayımlandı.

“YAPAY ZEKÂ ARAÇLARI KULLANAN ÇOCUKLAR İÇİN EBEVEYNLERE YÖNELİK TAVSİYELER”

Ebeveynlerin, çocuklarının yapay zekâ araçlarını hangi amaçlarla ve nasıl kullandığını bilmesi ve bu teknolojilerle kurdukları ilişkiye rehberlik etmesine yardımcı olması bakımından “Yapay Zekâ Araçları Kullanan Çocuklar İçin Ebeveynlere Yönelik Tavsiyeler” yayımlandı.

KURUMUMUZ İLE JANDARMA GENEL KOMUTANLIĞI ARASINDA İŞ BİRLİĞİ

Jandarma Genel Komutanlığı'nın yetki ve görev alanlarına giren konularda kişisel verilerin hukuka uygun olarak işlenmesi, Jandarma Genel Komutanlığı personelinin kişisel verilere ilişkin farkındalığının artırılması ve tecrübe paylaşımı amacıyla, Kurumumuz ile Jandarma Genel Komutanlığı arasında iş birliği protokolü imzalandı.

OTORİTE ZİYARETLERİ

Kurum Başkanımız Prof. Dr. Faruk BİLİR başkanlığındaki Kurumumuz heyeti, Macaristan Ulusal Veri Koruma ve Bilgi Özgürlüğü Otoritesine çalışma ziyaretinde bulundu.

Öte yandan Kurul İkinci Başkanı ve Kurulu Üyesi Hasan AYDIN ile Kurul Üyesi Şaban BABA, İslam ülkeleri arasında kişisel verilerin korunması alanında iş birliğinin geliştirilmesi amacıyla Daimî Sekretaryasını yürütmekte olduğumuz Kişisel Veri Koruma Otoriteleri İslami Ağı'nın (INPDPA) kuruluş çalışmaları kapsamında Fas'ta düzenlenen toplantıya katılım sağladılar.

AYIN TARİHİ DERGİSİ

Cumhurbaşkanlığı İletişim Başkanlığı'nın süreli yayını olan "Ayın Tarihi" dergisinin son sayısında "7 Nisan Kişisel Verileri Koruma Günü" ele alındı. Dergide, Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girdiği 7 Nisan gününün, Türkiye'de dijital mahremiyet bilincinin inşasındaki rolüne vurgu yapıldı. Ayrıca Kurumumuzun farkındalık ve bilgilendirme faaliyetleri başta olmak üzere, kurumsal projelerine yer verildi.

HACİVAT VE KARAGÖZ İLE KİŞİSEL VERİLERİMİ ÖĞRENİYORUM

Çocuklara yönelik "Hacivat ve Karagöz ile Kişisel Verilerimi Öğreniyorum" temalı video serisi yayınlandı.

"Hacivat ve Karagöz Kişisel Veriyi Buluyor"

"Hacivat ve Karagöz Çöp Kutusunda Kişisel Veri Buluyor"

"Karagöz'ün Şifresi Hacivat'ta"

"Hacivat ve Karagöz ile Dijital Temizlik"

"Hacivat ve Karagöz Sosyal Medyada"

"Karagöz'ün Gizlilik Ayarları"

"Hacivat ve Karagöz Veri Dedektifi Oluyor"

"Hacivat ve Karagöz Kişisel Verileri Koruma Günü'nü Kutluyor"

olmak üzere sekiz videodan oluşan seride, çocuklara veri koruma ve mahremiyetin önemi anlatıldı.

2026 KVKK ÇOCUK TAKVİMİ

Çocuklara yönelik olarak Kurumumuz tarafından "2026 KVKK Çocuk Takvimi" hazırlandı.

kvkkkurumu

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Kişisel Verileri Koruma Kurumu
Nasuh Akar Mahallesi 1407. Sokak
No.4 06520 Çankaya | ANKARA
T. 0312 216 50 00
www.kvkk.gov.tr