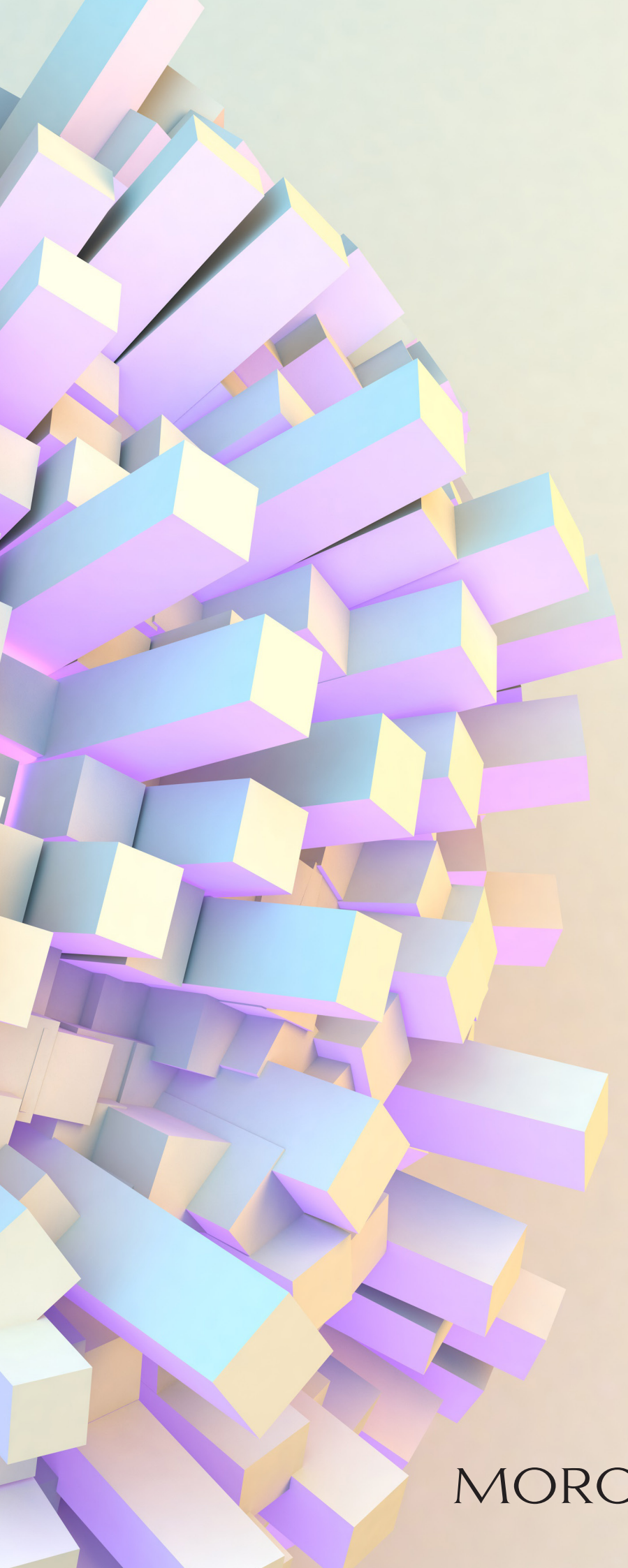
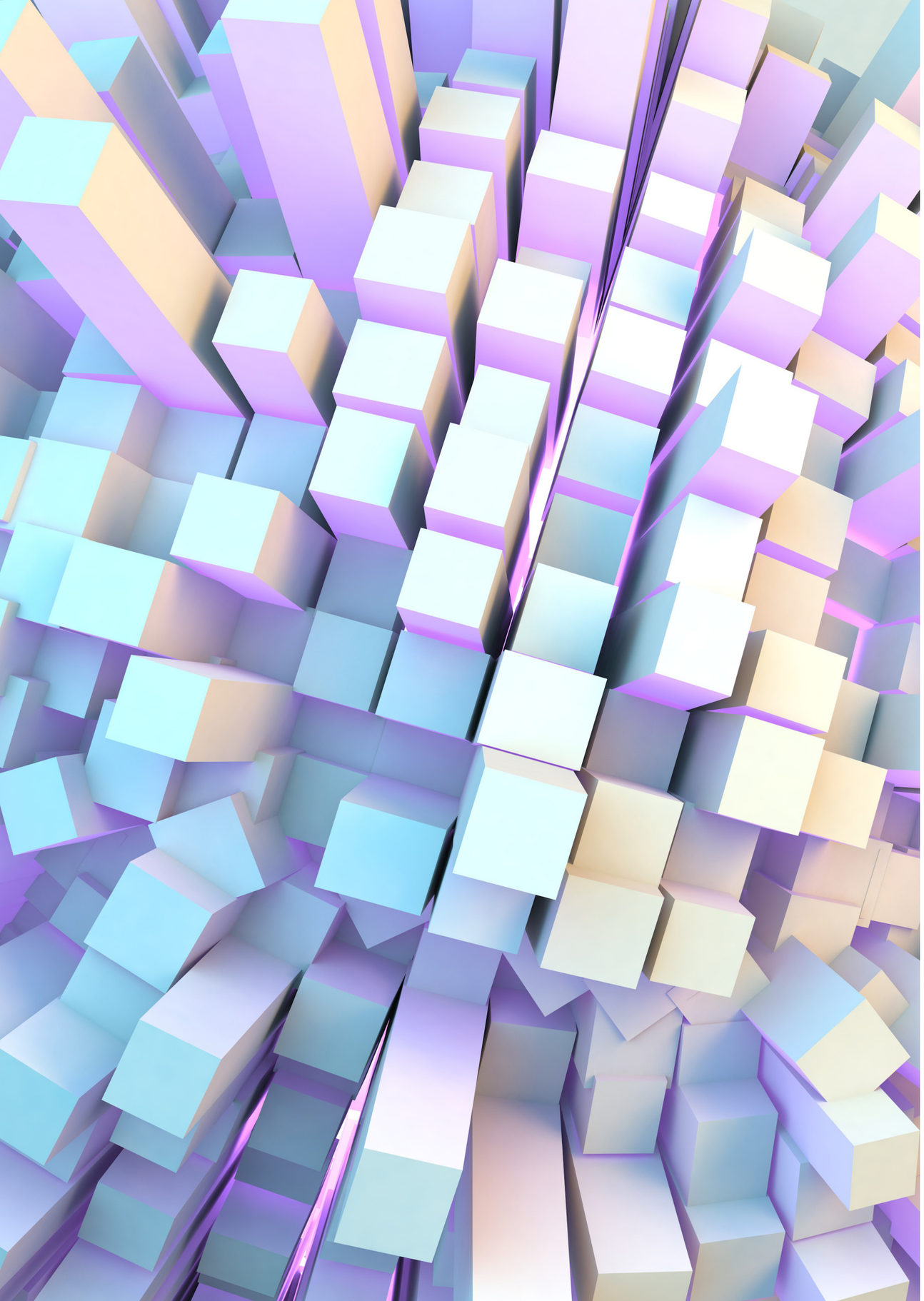


Türk Veri Koruma Hukuku 2021

İlk 5 Yılda Uygulamadaki Gelişmeler

MOROĞLU ARSEVEN



Önsöz

6698 sayılı Kişisel Verilerin Korunması Kanunu hayatımıza gireli yaklaşık beş yıl geçti ve Türkiye'de bir zamanlar standart kabul edilen iş uygulamalarının çoğu bu zaman içerisinde değişiklik gösterdi.

Bu gelişmeler kuruluşların hem kendi faaliyet alanlarına göre kişisel verileri korumak amacıyla birtakım güvenlik önlemleri almasını hem de Kişisel Verilerin Korunması Kanunu'na uyum süreci açısından iş modellerini yeniden değerlendirme ve tasarlama ihtiyacını doğurdu.

Eylül 2020, ana faaliyet konusu özel nitelikli kişisel veri olmayan veri sorumluları için Veri Sorumluları Sicili'ne son kayıt tarihi olarak belirlendi. Bu süreçte birçok veri sorumlusu Kişisel Verileri Koruma Kurulu tarafından incelemeye tabi tutuldu ve bazıları Kişisel Verilerin Korunması Kanunu'na uyumlu olmadığı gerekçesiyle idari yaptırımla karşı karşıya kaldı.

Özellikle kişisel verilerin yurt dışına aktarımı hususu birçok veri sorumlusu için mevcut düzenlemeye uyum sağlama noktasında sorun teşkil etmeye devam etmektedir. Hukuk ve iş çevreleri, hem Kişisel Verileri Koruma Kurulu tarafından yeterli veri korumasına sahip ülkelerin belirlenesini hem de Kişisel Verilerin Korunması Kanunu başta olmak üzere ilgili mevzuatın Avrupa Birliği mevzuatına yakınlaştırılmasını beklemektedir.

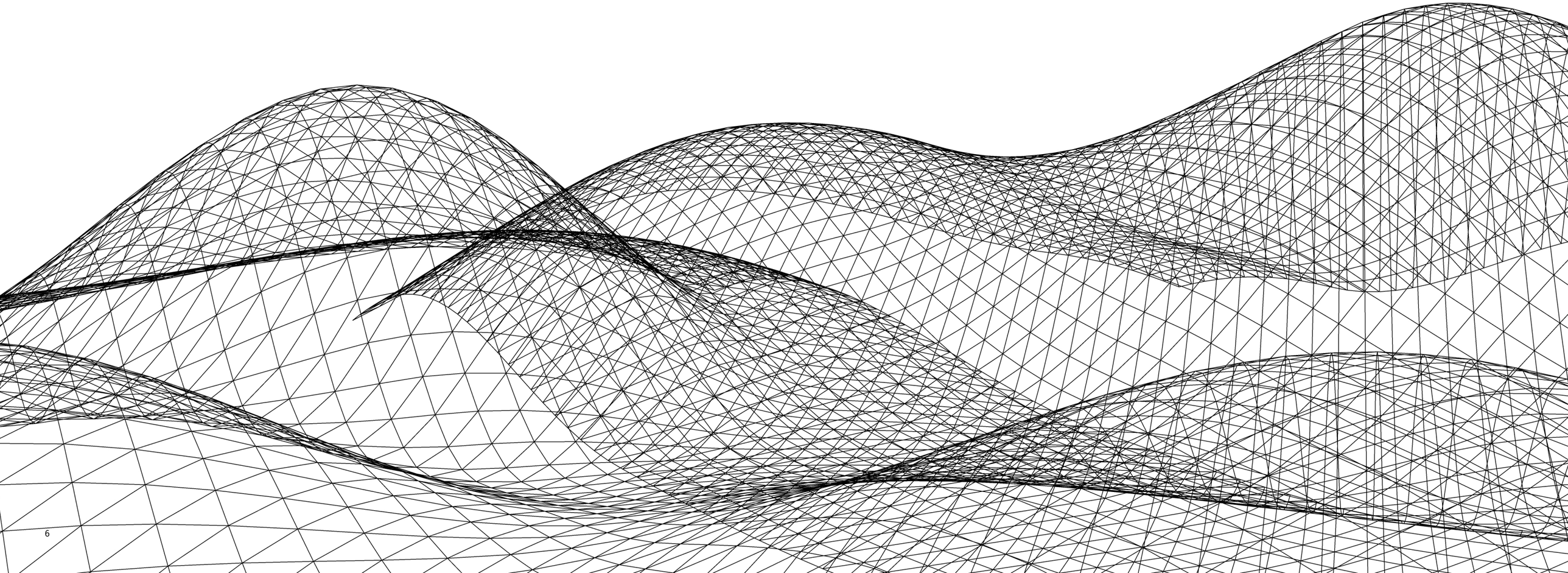
Moroğlu Arseven Veri Koruma Günü vesilesiyle geçtiğimiz beş yılda yaşanan gelişmelere işbu rehberle bir bakış sunuyor. Moroğlu Arseven işbu rehberi yasal gelişmeler çerçevesinde yıllık olarak güncellemeyi hedeflemektedir, dolayısıyla gelişmeleri Türk Veri Koruma Hukuku rehberlerimiz aracılığıyla takip edebilirsiniz.

İçindekiler

MOROĞLU ARSEVEN

MOROĞLU ARSEVEN

I. HUKUKİ ÇERÇEVE



A. Uygulama Süreci

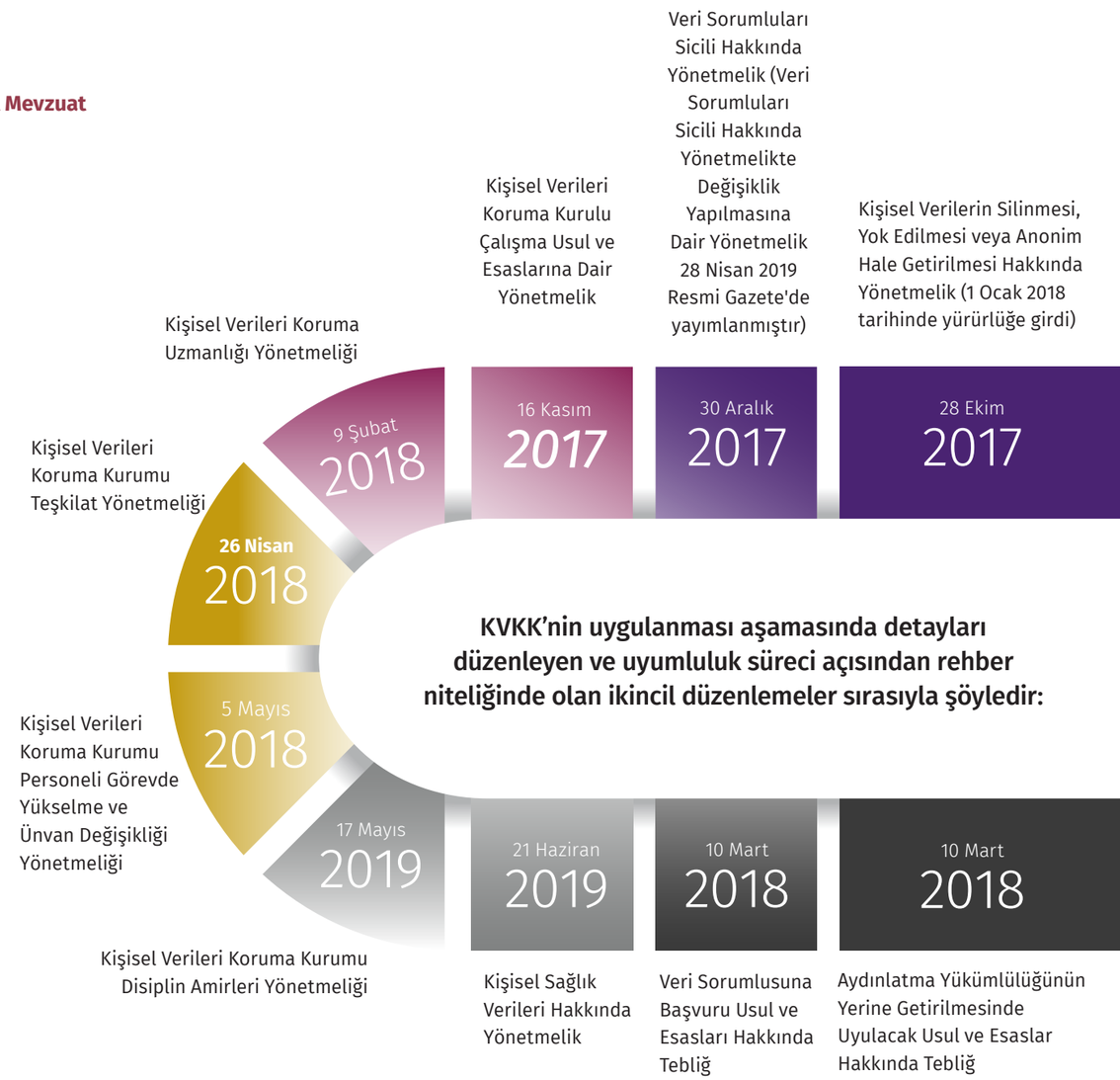
1. Kanunun Hazırlık Süreci

Kişisel Verilerin Korunması Kanunu ("**KVKK**") Türkiye'de 7 Nisan 2016 tarihinde yürürlüğe girmiştir; ancak, KVKK yürürlüğe girmeden önce uzun süre taslak olarak kalmıştır. Aslında, veri korumaya yönelik özel bir kanun her ne kadar ilk kez 2003 yılında, Türkiye'nin Avrupa Birliği'ne ("**AB**") tam üyelik uyum sürecinin bir parçası olarak gündeme gelmiş olsa da ilk taslak daha önceki tarihlere dayanmaktadır. 2016 yılına kadar Türkiye'de veri koruma ile ilgili birçok taslak metin hazırlanmış, ancak bu taslakların hiçbiri yasalaşmamıştır.

2016 yılında KVKK'nin yürürlüğe girmesine kadar, kişisel verilerin korunması alanı Anayasa, Türk Ceza Kanunu ("**TCK**"), Türk Borçlar Kanunu ("**TBK**"), İş Kanunu, Elektronik Haberleşme Kanunu gibi kanuni düzenlemeler ve sektör bazlı yönetmeliklerle düzenlenmekteydi. Bahsi geçen bu düzenlemelerin yeterince kapsamlı olmaması ve ihtiyaç duyulan düzeyde koruma sağlamaması nedenleriyle hazırlanan KVKK Türkiye Büyük Millet Meclisi'nde ("**TBMM**") 24 Mart 2016 tarihinde kabul edilmiş ve 7 Nisan 2016 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Bu gelişmeyle beraber, Türkiye ilk defa özel olarak veri işleme faaliyetlerini düzenleyen bir kanuna sahip olmuştur.

Türkiye'de KVKK'nin veri korumayla ilgili ilk doğrudan kaynak olması sebebiyle, kanuna uyum süreçlerini düzenlemek için KVKK'de çeşitli geçiş hükümleri öngörülmüştür (KVKK Geçici madde 1). Geçiş maddesi uyarınca, tüm veri sorumlularına KVKK'nin yürürlüğe girmesinden önce gerçekleştirilmiş kişisel veri işleme faaliyetlerini KVKK ile uyumlu hale getirmeleri için 2 yıllık bir süre tanınmıştır. 2 yıllık uyumluluk süresi 7 Nisan 2018 tarihinde sona ermiştir.

2. İkincil Mevzuat



Yukarıda belirtilen düzenlemelere ek olarak, Bölüm II.C'de de yer alan Kişisel Verileri Koruma Kurumu'nun düzenleyici ve denetleyici kararları ile yönergeleri, KVKK'niın uygulanması sürecine ışık tutmaktadır.

B. Kurum Yapısı

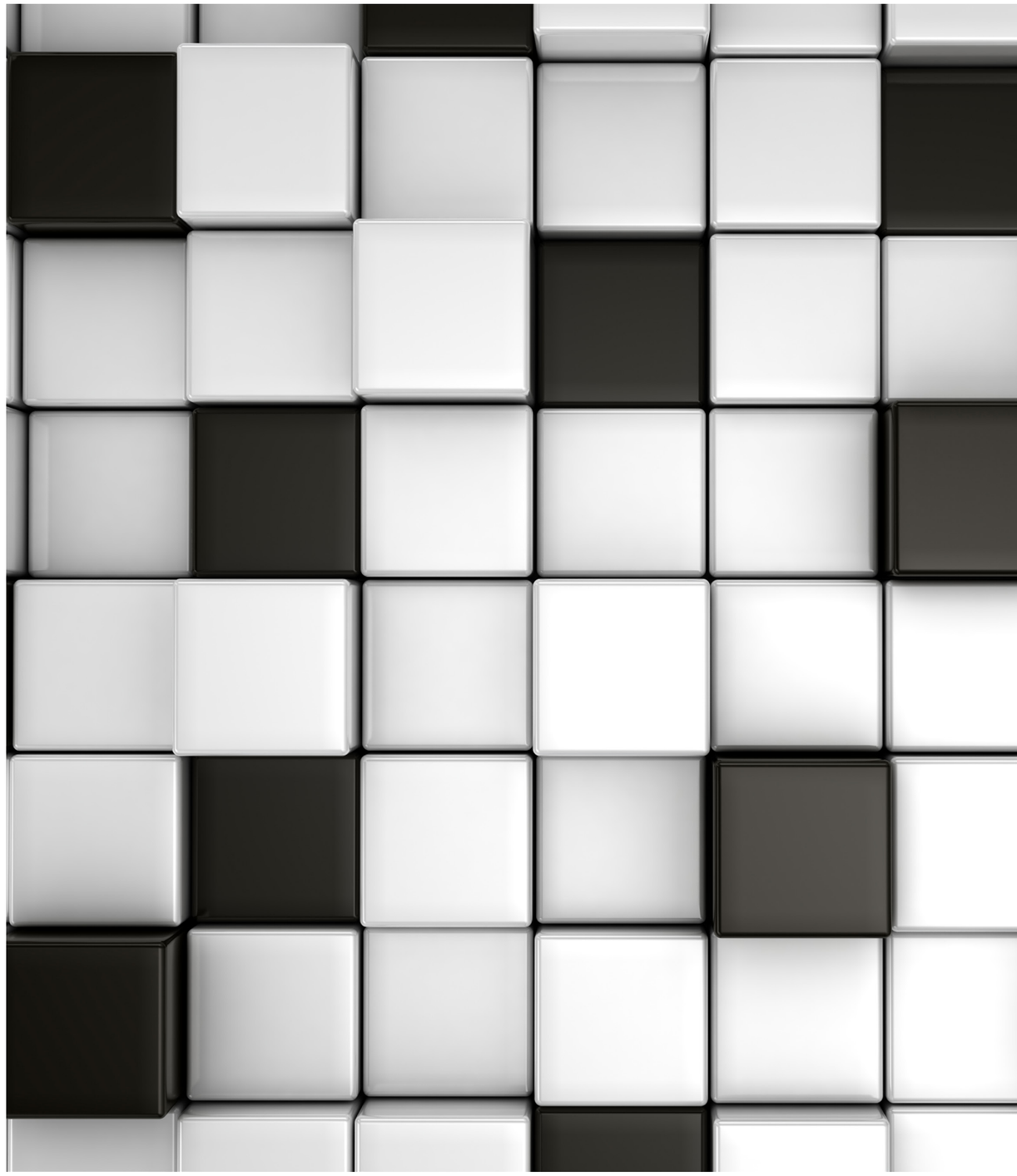
Kişisel Verileri Koruma Kurumu (“**Kurum**”), veri koruma kurallarının doğru uygulanmasını sağlamak amacıyla, KVKK'nin kendisine verdiği görevleri yerine getirmek üzere yapısal ve mali özerkliğe sahip ve kamı tüzel kişiliğini haiz düzenleyici kuruluş olarak kurulmuştur.

Kurum'un misyonu, kişisel verilerin korunmasını sağlamak ve Anayasa ile korunan özel hayatın gizliliği, mahremiyet ile diğer temel hak ve özgürlükler hakkında kamuoyunda farkındalık oluşturmak, veri ekonomisinin başrol oynamaya başladığı günümüz dünyasında kamu ve özel sektörün rekabet kabiliyetlerini artıracak bir ortam sağlamaktır.

Dokuz üyeden oluşan Kişisel Verileri Koruma Kurulu (“**Kurul**”), Kurum’un karar alma organı olarak faaliyet göstermektedir. Dokuz üyeden beşi TBMM, dördü ise Cumhurbaşkanı tarafından atanır. Kurul, Ocak 2017 itibarıyla faaliyete başlamış olup; KVKK kapsamında özetle aşağıdaki hususlarla görevlidir:

Kişisel verilerin KVKK’ye uygun biçimde işlenmesini temin etmek,
• KVKK kapsamında gerekli kuralları ve yönetmelikleri yayımlamak,
• Yeterli düzeyde veri korumasının sağlandığı ve koruma düzeyinin yeterli olmadığı ülkeleri tespit etmek ve duyurmak, Türkiye'de ve ilgili ülkedeki veri sorumlularının yeterli korumanın sağlanacağını yazılı olarak garanti etmesi halinde kişisel verilerin yurt dışına aktarılmasına izin vermek,
• Gerekli görülmesi halinde veri ihlallerini, Kurum’un internet sitesinde yayımlamak suretiyle veya uygun gördüğü diğer yöntemlerle duyurmak,
• Kurum’a yapılan şikayetleri incelemek ve sonuçlandırmak,
• Bir işlemin telafisi zor veya imkânsız zararlara yol açması ve açıkça hukuka aykırı olması halinde, veri işlemenin veya yurt dışına veri aktarımının durdurulmasına karar vermek,
• Veri Sorumluları Sicil Bilgi Sisteminin (“**VERBİS**”) devamlılığını sağlamak,
• Kurum’da çalışan memurlarla ilgili disiplin soruşturmalarını yürütmek ve gerektiğinde idari yaptırımlara karar vermek,
• Düzenleyici prosedürleri yürütmek,
• Kurum’un idari işlevleriyle ilgili taslak raporları onaylamak ve yayınlamak.

VERBİS kayıt prosedürü ve genel anlamda kişisel verilerin korunması konularında arayanlara aydınlatıcı bilgi verilmesi amacıyla Kurum tarafından bir Bilgi Danışma Hattı (ALO 198 Veri Koruma) oluşturulmuştur.



C. Temel Kavramlar

Kişisel Veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi anlamına gelir. Dolayısıyla, kişiyi tanımlamak için kullanılabilecek herhangi bir bilgi kişisel veri niteliğindedir. Örneğin, bir müşterinin adı ve adresi, IP adresi, e-posta adresi veya müşteri e-posta adreslerinden oluşan bir veri tabanı kişisel veri kapsamındadır.

Özel Nitelikli Kişisel Veri Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel verilerdir. KVKK'de yer alan kılık kıyafet, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler, biyometrik ve genetik verilere ilişkin koruma AB düzenlemelerindeki özel nitelikli kişisel verilerin korunmasına yönelik düzenlemelere kıyasla daha kapsamlıdır.

Veri Sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

Veri İşleyen veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.

Açık Rıza ilgili kişi tarafından belirli bir konuya ilişkin olarak özgür iradeyle verilen ve bilgilendirilmeye dayanan onay anlamına gelir. KVKK kişisel verilerin veya özel nitelikli kişisel verilerin kural olarak açık rıza ile işlenmesini öngörmektedir; ancak, açık rızayı almak için belirli bir yöntem KVKK altında düzenlenmemiştir. Bu bağlamda, veri sorumluları açık rızayı yazılı, elektronik veya sözlü olarak temin edebilirler. Her hâlükârda açık rızanın alınmasına ilişkin ispat yükümlülüğü veri sorumlusuna aittir.

Kişisel Verilerin İşlenmesi kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olması kaydıyla, otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanımının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü bir işlemi ifade eder.

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) veri sorumlularının Veri Sorumluları Siciline başvuruda ve sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kişisel Verileri Koruma Kurumu Başkanlığı tarafından oluşturulan ve yönetilen bilişim sistemini ifade eder.

MOROĞLU ARSEVEN

D. Veri Sorumluları ve Veri İşleyenlerin KVKK Kapsamındaki Yükümlülükleri

Genel Veri İşleme İlkelerine Uyum Sağlama	İşleme Şartlarına Uyum Sağlama	Aydınlatma Yükümlülüğü
İlgili Kişinin Tarafından Yapılan Başvuruların Yanıtlanması	Veri Aktarım Kurallarına Uyum Sağlama	Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Gerekliliklerine Uyum Sağlama
Veri Güvenliğine İlişkin Yükümlülükler	Veri İhlal Bildirim Yükümlülüğü	Veri Sorumluları Siciline Kayıt Yükümlülüğü

1. Veri İşleme Sürecine İlişkin Genel İlkeler

Veri Sorumluları tarafından, tüm kişisel veri işleme süreçlerinde KVKK madde 4'te düzenlenen genel ilkelere uyulması esastır. Kişisel veriler:

- Hukuka ve dürüstlük kurallarına uygun olarak,
- Hukuka ve dürüstlük kurallarına uygun olarak,
- Doğru ve gerektiğinde güncel olarak,
- Belirli, açık ve meşru amaçlar için,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma şartıyla işlenmeli;
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

Hukuka Uygun Veri İşlemeye Dair Kararlar	
Karar numarası	2019/331
Karar	Veri sorumlusu verilerin hukuka aykırı işlenmesinde gerekli idari ve teknik tedbirleri almamıştır.
Karar numarası	2019/81 - 2019/165
Karar	Veri sorumlusu özel nitelikli kişisel verilerin hukuka aykırı işlenmesinde gerekli idari ve teknik tedbirleri almamıştır ve orantılılık ilkesiyle uyumluluğu ihmal etmiştir.
Karar numarası	2019/294
Karar	Veri sorumlusu özel nitelikli kişisel verilerin hukuka aykırı işlenmesinde KVKK kapsamında veri sorumlusuna tanınan haklarla uyumlu olan ve yeterli korunmayı sağlayan gerekli idari ve teknik tedbirleri almamıştır.
Karar numarası	2019/ 188
Karar	Veri sorumlusu üniversite tarafından uygulanan duyuru sistemine üçüncü taraflara KVKK altındaki herhangi bir işleme şartına dayanmaksızın erişim imkanı verilmiştir.

2. Kişisel Verilerin İşlenme Şartları

KVKK kapsamında kişisel verilerin ve özel nitelikli kişisel verilerin işlenme şartları farklı maddeler altında düzenlenmiştir.

KVKK madde 5 uyarınca kişisel veriler aşağıdaki şartlardan birinin varlığı halinde işlenebilir:

- Açık rıza
- Kanunlarda açıkça öngörülmesi
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması
- İlgili kişinin kendisi tarafından alenileştirilmiş olması
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

KVKK madde 6 uyarınca kural olarak özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenmesi yasaktır.

KVKK açık rıza dışındaki veri işleme şartları bakımından özel nitelikli kişisel verileri iki farklı kategori altında düzenlenmiştir:

- Sağlık veya cinsel hayata ilişin kişisel veriler
- Diğer özel nitelikli kişisel veriler

Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilirken sağlık ve cinsel hayata ilişkin kişisel veriler, ilgili kişinin açık rızası olmaksızın yalnızca sır saklama yükümlülüğüne tabi kişiler veya yetkili kurum ve kuruluşlarca, aşağıdaki amaçlarla sınırlı olarak işlenebilir:

- Kamu sağlığının korunması
- Koruyucu hekimlik
- Tıbbi teşhis
- Tedavi ve bakım hizmetlerinin yürütülmesi
- Sağlık hizmetlerinin ve finansmanının planlanması ve yönetimi.

Sağlık verilerinin işlenmesine ilişkin diğer bir gelişme Sağlık Bakanlığı tarafından 21 Haziran 2019 tarih ve 30808 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik'in ("**Sağlık Verileri Yönetmeliği**") yürürlüğe girmesidir. Bu suretle 2016 yılında çıkarılan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetin Sağlanması Hakkında Yönetmelik yürürlükten kaldırılmıştır. Sağlık Verileri Yönetmeliği, kamu kurumları ve özel kuruluşlar tarafından uyulması gereken kişisel sağlık verisi işleme koşullarını ortaya koymakta ve sağlık verilerinin korunmasına yönelik yükümlülükleri detaylı şekilde düzenlemektedir.

Sağlık Verileri Yönetmeliği, sağlık verilerinin korunmasına yönelik önlemleri artırmak adına ilgili kişilere sağlık verilerine yönelik kapsamlı haklar tanımakta ve sağlık verisi işleyen veri sorumlularına ek yükümlülükler getirmektedir. Her halükârda, Sağlık Verileri Yönetmeliği kapsamında öngörülen tedbirlerin özel nitelikli kişisel veri olan sağlık verilerini korumak için yeterli olup olmadığına karar verme yetkisi Kurul'a aittir.

Sağlık Verileri Yönetmeliği sağlık kurumlarının sağlık verilerine erişimine ilişkin özel düzenlemeler içermekte ve ilgili sağlık hizmetlerinin sağlanması için erişim gerekmedikçe sağlık çalışanlarının sağlık verilerine erişimini sınırlandırmaktadır. Bu bağlamda, Sağlık Verileri Yönetmeliği e-Nabız (e-Devlet uygulamalarına uygun olarak Sağlık Bakanlığı tarafından kurulan çevrimiçi sağlık sistemi) hesabı bulunan kişilerin sağlık verilerine, ilgili kişilerin kendi gizlilik tercihleri çerçevesinde erişim sağlanabileceğini düzenlemektedir. Dolayısıyla, ilgili kişiler gizlilik tercihlerini değiştirerek hekimlerin veya sair üçüncü kişilerin e-Nabız hesaplarına erişimini kısıtlayabilirler.

Sağlık Verileri Yönetmeliği ile getirilen erişim sınırlamaları kapsamında, avukatlar müvekkilinin sağlık verilerini genel vekâletname ile talep edemezler. Müvekkile ait sağlık verilerinin avukata aktarılması için düzenlenmiş olan vekâletnamede, ilgili kişinin özel nitelikli kişisel verilerinin işlenmesi ve aktarılmasına ilişkin açık rızasını gösteren özel bir hüküm bulunması gerekir.

Sağlık Verileri Yönetmeliği, ölmüş kişilerin sağlık verilerinin en az 20 yıl süreyle saklanmasını ve işbu sağlık verilerine ölen kişinin veraset ilamını ibraz eden yasal mirasçılarına erişim hakkı tanınmasını düzenlemektedir.

Sağlık verilerinin ilgili kişiler için hassasiyeti göz önüne alındığında, sağlık verilerinin ileri düzey koruma gerektirdiği açıktır. Bu bakımdan Sağlık Verileri Yönetmeliği'nin sağlık verilerinin mahremiyetinin ve gizliliğinin sağlanması bakımından önemi ortadadır. Sağlık Bakanlığı'nın, AB Genel Veri Koruma Tüzüğü'nü ("**GDPR**") kaynak alarak hazırlamış ve yayımlamış olduğu Sağlık Verileri Yönetmeliği, aynı zamanda AB rehberleri ile de paralellik arz etmektedir.

Kurul'un bugüne kadar başta sağlık verileri olmak üzere, özel nitelikli kişisel verilerin işlenmesine dair yayımlanmış olduğu çok sayıda kararı bulunmaktadır. Örneğin, Kurul tarafından, tanınmış biri olan ilgili kişinin özel nitelikteki kişisel verilerini içeren sağlık raporunun tedavi görmekte olduğu hastane personeli tarafından internet ve sosyal medya kanallarında paylaşılmasına

istinaden verilmiş olan 31 Ocak 2018 tarih ve 2018/10 sayılı karar uyarınca; ilgili kişinin sağlık verilerinin sosyal medya aracılığıyla geniş bir kitle için aleni hale getirilmiş olması gerekçesi ile KVKK'nin 12. maddesinin (1) numaralı fıkrasının (c) bendi kapsamında kişisel verilerin korunması için uygun güvenlik düzeyini sağlayamayan veri sorumlusuna 18. madde uyarınca idari para cezası öngörülmüştür.

2.1 Açık Rıza

Kurul tarafından yayımlanmış olan rehberlerde belirtildiği üzere, açık rıza veri sorumluları tarafından ancak diğer hukuki sebeplerin olay bazında uygulanabilir olmadığı durumlarda işleme şartı olarak kullanılabilecektir. Kurul; başka herhangi bir hukuki sebebe dayanmanın mümkün olduğu hallerde, veri sorumlusunun veri işleme faaliyetini açık rızaya dayandırmasını aldatıcı ve hakkın kötüye kullanılması olarak değerlendirmektedir.

Bu kapsamda, veri sorumlusu tarafından ilgili kişilerin açık rızasına başvurulmadan önce, veri işleme faaliyetinin açık rıza dışındaki işleme şartlarından herhangi birine dayanıp dayanmadığının değerlendirilmesi ve doğru hukuki sebebin belirlenmesi önem teşkil etmektedir. Kurul, 2 Ağustos 2018 tarihli kararında açık rıza konusundaki yaklaşımını, kişisel verilerin işlenmesi için başka işleme şartları mevcutsa, ilgili kişilerden açık rıza alınmasının veri sorumlusu tarafından hakkın kötüye kullanılması anlamına geldiğini ve bu durumun ilgili kişilerin yanıltılmasına sebebiyet vereceğini açıkça ortaya koymuştur.

KVKK'nin 3. maddesinde açık rıza; "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" şeklinde tanımlanmıştır. Kurul tarafından rehberlerde detaylandırıldığı üzere, açık rıza ilgili kişinin sahip olduğu kişisel verilerin işlenmesine kendi isteğiyle ve olumlu irade beyanı ile onay göstermesidir. Açık rızadan söz edebilmek için ilgili kişiye veri sorumlusunun veri işleme faaliyetlerine yönelik yeterli düzeyde bilgilendirme yapılmış olunması gerekmektedir. Bu bağlamda, açık rıza metinlerinde kişisel verilerin işlenme amaçlarının açık ve anlaşılır şekilde belirtilmesi gerekir.

Açık rızanın geçerli olması için, açık rızanın ilgili kişinin özgür iradesiyle açıklanması gerekmektedir. Özgür iradeden bahsedebilmek için ilgili kişinin iradesinin herhangi bir surette sakatlanmamış olması gerekir. Bir başka ifade ile, ilgili kişi veri işleme faaliyetini kendi hür iradesi ve kararı ile kabul etmelidir. Bu nedenle, önceden işaretlenmiş onay kutuları, pasif onay gibi reddetmeye dayalı olarak alınan onaylar Kurul tarafından geçerli bir açık rıza olarak kabul edilmemektedir.

İlgili kişinin özgür iradesine dayanarak açık rıza toplanması; ilgili kişinin rıza vermeyi reddedebilmesi ve/veya açık rızasını istediği zaman geri çekebileceği anlamına gelmektedir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ ("**Aydınlatma Tebliği**") uyarınca, kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekir. Kurul bu hususu 2018/90 sayılı kararında aydınlatma metni ve açık rıza metinlerinin farklı belgeler olarak düzenlenmesi gerekliliğini vurgulayarak ortaya koymuştur. İlgili kararda ayrıca dijital ortamlarda aydınlatma yükümlülüğünün yerine getirildiğine dair ispat niteliğinde

olacak onay kutusu ile açık rıza verilmesine ilişkin onay kutusunun aynı olamayacağına da değinilmiştir.

KVKK ve ikincil düzenlemeler, açık rızanın kâğıt üzerinde, elektronik veya dijital imzalar kullanılarak, elektronik biçimde onay kutuları işaretlenerek ya da onaylayıcı e-postalar gönderilerek alınmasına imkân tanımaktadır. AB'deki bazı düzenlemelerin aksine, ispat yükü veri sorumlusuna ait olmak kaydı ile KVKK kapsamında açık rızanın yazılı olarak alınması zaruri olmayıp; elektronik yollarla ve/veya çağrı merkezleri kanalları üzerinden de açık rızanın alınması mümkündür.

Veri sorumlusu ile ilgili kişinin arasında ast üst ilişkisi gibi tarafların eşit durumda olmadığı durumların varlığı halinde de açık rızanın özgür iradeye dayanıp dayanmadığı hususu tartışmalı hale gelmektedir. Özellikle, işveren-işçi ilişkisinde açık rızanın özgür irade ile verilip verilmediği hususu oldukça tartışmalıdır. Bu bağlamda, veri sorumluların iş ilişkilerinde açık rızaya dayandırdıkları veri işleme faaliyetlerini dikkatli bir biçimde yönetmeleri gerekmektedir.

Açık rıza bilgilendirmeye dayanmalıdır. Bu kapsamda, ilgili kişiler tüm veri işleme süreçlerinin açıkça yer aldığı bir metin vasıtasıyla veri sorumlusu tarafından bilgilendirilmelidir. İlgili kişilerin anlaşılabilir bir metin ile bilgilendirilmesi oldukça önem arz etmektedir. Bilgilendirmenin mutlaka veri işleme faaliyetinden önce yapılması gerekir.

Açık rıza belirli bir konuya ilişkin olmalıdır. Bu bağlamda, veri sorumlularının hangi veri işlemeye faaliyetine yönelik olarak açık rıza talep ettiklerini açık bir şekilde ortaya koyması gerekmekte ve ilgili kişilerden talep edilen açık rızalar söz konusu veri işleme faaliyetine özgü olmalıdır. Genel nitelikte açık rızalar Kurul tarafından geçerli kabul edilmemektedir. Açık rıza verilmesi ilgili kişiye sıkı sıkıya bağlı bir haktır ve ilgili kişi kişisel verilerinin akıbetini belirleme hakkına sahiptir. Bu nedenle ilgili kişi, açık rızasını istediği zaman geri çekebilir. Açık rızanın geri çekilmesi ileriye dönük şekilde etki doğuracaktır. Açık rızanın geri çekilmesi durumunda, veri sorumlusu, söz konusu açık rızaya dayalı olarak gerçekleştirilen tüm işleme faaliyetlerini açık rızanın geri çekilme talebinin kendisine ulaştığı tarih itibariyle durdurmalıdır.

2.2 Açık Rıza Dışındaki İşleme Şartları

Kişisel verilerin işlenmesine yönelik genel kural ilgili kişinin açık rızasının alınması olsa da istisnai durumlar olarak kabul edilen ve KVKK Madde 5 uyarınca açık rıza gerekliliğinden muaf tutulan belirli haller mevcuttur. İlgili kişilere yapılacak bilgilendirmelerde veri sorumluları veri işleme faaliyetinin işleme şartını açıkça belirtmekle yükümlüdür. Muğlak ve kapsamı belirsiz şekilde yapılan atıflar Kurul tarafından geçerli bir işleme şartı olarak kabul edilmemektedir.

a) Kanunlarda öngörülmesi halinde: Kanunlarda kişisel verilerin işlenebileceği açıkça belirtilmişse, kişisel veriler ilgili kişinin açık rızası olmaksızın işlenebilir. İşverenler tarafından personel dosyaları hazırlanması, banka ve finans kurumları tarafından belirli bilgilerin toplanması ve bildirilmesi ile yeni işe başlayan çalışanın kişisel bilgilerinin işverenlerce kolluk kuvvetlerine bildirilmesi kanunun izin verdiği veri işleme faaliyetlerine örnek olarak sayılabilir.

b) Fiili imkânsızlık nedeniyle açık rızanın alınamayacak olması halinde: Kişisel veriler, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde işlenebilir. Örneğin, kayıp bir kişinin taşıdığı telefonundaki konum verileri veya güvenlik kamerası kayıtları söz konusu kişinin yerini tespit etmek maksadıyla işlenebilir.

c) Bir sözleşmenin kurulması veya ifası gerekçesiyle: Bir sözleşmenin kurulması veya ifasıyla doğudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel veriler işlenmesi gerekli olduğu sürece diğer tarafça işlenebilir. Çalışanın kişisel verilerinin işveren tarafından iş sözleşmesi yapmak amacıyla işlenmesi bu hukuka uygunluk haline bir örnek teşkil eder.

d) Veri sorumlusunun hukuki yükümlülüğü gerekçesiyle: Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması halinde, veri işleme faaliyetine söz konusu hukuki yükümlülüğün yerine getirilmesi için zorunlu ve ilgili olduğu ölçekte izin verilir. Çalışanın finansal verilerinin işveren tarafından ücret ödemesi için işlenmesi ve alıcının adres verilerinin kargo şirketi tarafından işlenmesi bu hukuka uygunluk haline örnek olarak verilebilir.

e) Kişisel verinin ilgili kişi tarafından alenileştirilmiş olması halinde: İlgili kişi tarafından herhangi bir şekilde kamuya açıklınmış olan kişisel veriler ilgili kişinin açık rızası olmaksızın işlenebilir ancak veri işleme faaliyeti söz konusu verinin kamuya açıklanma sebebi ile sınırlı şekilde gerçekleştirilmelidir. Örneğin, bir kişi aracının satışı için kendisiyle iletişime geçilmesi için telefon numarasını aleni hale getirirse, bu numara sadece satış konusu araca ilişkin bilgi almak üzere işlenebilir.

f) Bir hakkın tesisi, kullanılması veya korunması gerekçesiyle: Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması halinde kişisel veriler ilgili kişinin açık rızası olmaksızın işlenebilir. Bir işveren aleyhine dava açılması durumunda, çalışanın belirli kişisel verileri işverenin haklarını savunmak için mahkemeye aktarılabilir.

g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla meşru menfaat gerekçesiyle: Kişisel veriler, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için işlemenin zorunlu olması halinde ilgili kişinin açık rızası olmaksızın işlenebilir. KVKK'nin giriş bölümünde ifade edildiği şekilde, bir işverenin, çalışanlarının kişisel verilerini, meşru menfaatleri oluşturan terfilerini, sosyal haklarını düzenlemek veya şirketin yeniden yapılandırılmasındaki rollerini belirlemek için işlemesi veri sorumlusunun meşru menfaatine örnek teşkil etmektedir. Kanun koyucu bu durumlarda ilgili kişinin açık rızasını aramamakla birlikte, kişisel verilerin korunmasına ilişkin temel ilkelere her halükârda uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi ve değerlendirilmesi gerektiğini vurgulamaktadır.

GDPR'ye göre, meşru menfaate dayalı olarak kişisel verilerin işlendiğinin kabulü için söz konusu faaliyet hukuka uygun olmalı ve ilgili kişinin temel hak ve özgürlüklerini ihlal eder nitelikte olmamalıdır. Veri işleme faaliyetinin bu kapsamda hukuka uygun sayılabilmesi için üç kriter vardır: (i) zorunluluk, (ii) meşru menfaatin varlığı ve (iii) orantılılık. Bu kapsamda, veri sorumlusunun menfaati ile ilgili kişinin hak ve özgürlükleri arasında bir denge testi yapıldıktan sonra veri işlemenin veri sorumlusu açısından zorunlu olduğunu söylemek mümkünse veri sorumlusunun meşru menfaatinin var olduğu kabul edilir. KVKK, veri sorumlusunun meşru menfaati söz konusu olduğunda kişisel verilerin açık rıza olmadan işlenmesini öngörmesine rağmen, ne KVKK ne de Kurul veri sorumlusunun menfaatlerini veya ilgili kişinin temel hak ve özgürlüklerini değerlendirmeye yönelik kriterler ve/veya denge test ile ilgili detaylı düzenlemeler ortaya koymamıştır. Veri işleme faaliyetinde işleme şartı olarak meşru menfaate dayanmak, veri sorumlusunun yalnızca kişisel verileri işlemek için meşru menfaat sahibi olmasından çok daha karmaşık bir süreç olduğundan ve Kurul'un bu konudaki yaklaşımının belirsizliği göz önünde alındığında veri sorumlusu, dayanabileceği başkaca bir işleme şartı olduğunda meşru menfaat yerine alternatif işleme şartına dayanabilir.

3. Aydınlatma Yükümlülüğü

Kişisel veri işleme şartlarından bağımsız olarak, veri sorumluları veya yetkilendirdiği kişi, kişisel verilerin elde edilmesi sırasında aşağıdaki konulara yönelik ilgili kişilere bilgi vermekle yükümlüdür (KVKK madde 10);

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel verilerin toplanma yöntemleri ve hukuki nedenleri,
- İlgili kişilerin KVKK madde 11 kapsamındaki hakları.

Aydınlatma yükümlülüğü ilgili kişinin talebine bağlı değildir; bu yükümlülük en geç kişisel verilerin elde edilmesi esnasında yerine getirilmelidir.

Aydınlatma metinlerinin ilgili kişilere sunulmasına ilişkin yöntemler Aydınlatma Tebliği ile belirlenmiştir. Bu doğrultuda aydınlatma yükümlülüğü sözlü, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle yerine getirilebilir. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir. Aydınlatma metninin açık rızadan, gizlilik sözleşmeleri veya kullanım koşulları gibi diğer sözleşmelerden ayrı olarak temin edilmesi gerekir. 26 Temmuz 2018 tarih ve 2018/90 sayılı Kurul kararı ile de ortaya konulduğu üzere, veri sorumlusunun aydınlatma yükümlülüğünü ve (gerekirse) açık rıza alma yükümlülüğünü ayrı ayrı yerine getirmesi gerekmektedir.

Aydınlatma Yükümlülüğü ve Açık Rızaya ilişkin Örnek Kararlar	
Karar numarası	2018/90
Karar	Veri sorumlusu tarafından aydınlatma metninin ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerekmektedir.
Karar numarası	2019/82
Karar	Sadakat kartı uygulamalarında sadakat kart sürecinin açık rızaya bağlanmış olması KVKK'yi ihlal etmez. Market zincirinin aydınlatma metni ve anonim hale getirme uygulamaları KVKK ile uyumlu değildir.
Karar numarası	2019/206
Karar	Veri sorumlusu tarafından verilen açık rıza ancak başka bir hukuki işleme şartının olmadığı hallerde geçerlidir. Aydınlatma metninin onaylanması ve açık rızanın alınması ayrı ayrı yapılmalıdır.

4. Kişisel Verilerin Aktarılması

4.1 Veri Aktarımının Şartları

KVKK, kişisel verilerin işlenmesi ve kişisel verilerin Türkiye içinde aktarılması için aynı işleme şartlarına atıfta bulunmaktadır (KVKK madde 8). Bu bağlamda, kişisel verilerin Türkiye içinde bir veri sorumlusuna veya bir veri işleyene aktarılabilmesi için, KVKK'nin 5. maddesinde belirtilen işleme şartlarından birinin veri sorumlusu tarafından esas alınması gerekmektedir.

GDPR'den farklı olarak, KVKK kapsamında veri sorumlularından veri işleyenlere veri aktarımları için özel bir kural öngörülmemiştir, bu kapsamda üçüncü kişilere aktarım ile veri işleyenlere aktarım KVKK altındaki genel veri aktarım kurallarına tabidir.

4.2 Kişisel Verilerin Yurt Dışına Aktarılması

a. Yurt Dışına Aktarımın Şartları

KVKK'nin 9. maddesi uyarınca kişisel veriler yurtdışına aşağıdaki şartlarda aktarılabilir:

- İlgili kişi tarafından açık rıza verilmesi VEYA
- KVKK'de öngörülen (açık rıza dışında) işleme şartlarından birine dayalı yurt dışına aktarımlarda:
  - Kişisel verinin aktarılacağı yabancı ülkenin Kurul tarafından yeterli korumanın bulunduğu ülkeler arasında sayılması,
  - Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması.

Yeterli korumanın bulunduğu ülkeler Kurul tarafından henüz belirlenmemiştir, dolayısıyla bu aşamada tüm ülkeler veri aktarımı açısından güvensiz olarak değerlendirilmektedir. Bu kapsamda, mevcut aşamada veri sorumlularının kişisel verileri yurt dışına aktarması için; (i) ilgili kişinin açık rızasının alması veya (ii) veri aktaran ile veri alıcısı arasında yazılı bir taahhüt düzenlenmesi ve veri aktarımı için Kurul'dan onay alınması gerekmektedir.

Kurul, internet sitesinde yurtdışına aktarım için kullanılacak taslak taahhütnameleri yayımlamıştır. Veri aktaran ile veri alıcısı arasında yapılacak taahhütnamelerde Kurul'un yayımladığı asgari içeriğin yer alması zorunludur. Taahhütnameler, veri sorumlusundan veri sorumlusuna aktarım ve veri sorumlusundan veri işleyene aktarım olmak üzere iki ayrı şekilde düzenlenmiştir. Kurul tarafından öngörülen asgari içerik, AB'deki standart veri koruma hükümleri (Standard Contractual Clauses) ile benzerdir.

Kurul, veri aktarımına izin verirken, uluslararası anlaşmaları, karşılıklılık ilkesini, kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından alınan önlemleri, ayrıca aktarılan verilerin niteliği ile veri işleme süresi ve amacını göz önünde

bulundurmalıdır. Kurul, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda yurt dışına veri aktarımını sınırlayabilir. Kurul'un bu durumlara yönelik ne şekilde değerlendirme yapacağı henüz net değildir.

b. Bağlayıcı Şirket Kuralları

Yeterli korumanın bulunduğu ülkelerin açıklanmamış olması, olağan iş akışları çerçevesinde kurumsal, altyapısal ve raporlama amaçlarıyla kişisel verileri yurtdışına aktaran çok uluslu grup şirketler açısından operasyonel ve hukuki sorunlara neden olmaktadır. Bu bağlamda, Kurul, piyasa aktörlerinin ihtiyaçları ile grup şirketlerinin kurumsal yapılarını göz önünde bulundurarak, 10 Nisan 2020 tarihinde, AB'deki düzenlemelerle aynı doğrultuda, çok uluslu grup şirketlerin kendi aralarında gerçekleştirilecekleri veri aktarımlarında kullanılmak üzere Bağlayıcı Şirket Kurallarını ("**BŞK**") açıklamıştır.

BŞK, Kurul tarafından yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için kişisel verilerin yurt dışına aktarımında kullanılan ve yeterli bir korumanın yazılı olarak taahhüt edilmesini sağlayan veri koruma kuralları olarak tanımlanmıştır. BŞK, yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren grup şirketler için grup içi aktarımlarda yeterli korumanın taahhüt edilmesine imkân veren alternatif bir yurtdışına veri aktarımı yöntemidir.

BŞK, şirketler topluluğunda veri koruması için gereken temel ilkeleri ve yeterli veri güvenliği önlemlerini içermelidir. Kurul, BŞK'nin asgari ve zorunlu içeriğine ilişkin yayımlamış olduğu rehberin yanı sıra kurumsal internet sitesinde standart bir başvuru formuna da yer vermiştir. BŞK'de bulunması gereken temel hususlar aşağıdaki gibidir:

- Bağlayıcılık,
- Etkili uygulama,
- Kurum ile koordinasyon,
- Kişisel Verilerin İşlenmesi ve Aktarılmasına İlişkin İlkeler,
- Raporlama ve Kayıt Değişikliği Mekanizmaları,
- Veri Güvenliği,
- Hesap Verebilirlik ve Diğer Araçlar.

Yukarıdakilere ek olarak, başvuru sahipleri, başvuru sürecini kolaylaştırmak için BŞK'ye zorunlu olmayan yardımcı bilgi ve belgeleri de ekleyebilir.

Şirketler topluluğu içindeki yurt dışına veri aktarımlarını BŞK çerçevesinde gerçekleştirmek isteyen çok uluslu grup şirketlerin, Kurum'un rehberleri çerçevesinde BŞK için gerekli hazırlıkları yaparak gerekli belgeleri oluşturmaları, Kurum tarafından yayımlanan başvuru formunu doldurmaları ve söz konusu belgeleri ibraz ederek BŞK'nin onaylanması için Kurum'a başvuruda bulunmaları gerekmektedir. Başvurular, resmi başvuru tarihinden itibaren 1 yıl içinde Kurum tarafından sonuçlandırılır. Kurum, gereken hallerde bu süreyi 6 ay uzatabilir.

Kurum 26 Ekim 2020 tarihinde yayımladığı Yurt Dışına Veri Aktarımı Kamuoyu Duyurusunda, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne ("**108 sayılı Sözleşme**") atfen yurt dışına aktarımlarına yönelik de bir değerlendirme yapmıştır. Bu duyuru ile Kurum, 108 sayılı Sözleşmenin varlığının tek başına yurtdışına veri aktarımını hukuka uygun kılmak için geçerli bir dayanak olmadığının altını çizmiştir.

Kurul'un 27 Şubat 2020 tarih ve 2020/173 sayılı önceki bir kararına konu olayda Amazon Turkey, kullanıcı verilerini, ilgili kişilerden açık rıza almaksızın AB ve Amerika Birleşik Devletleri'ne aktarmış, ancak Kurul'a veri aktarımına yönelik bir taahhüt de sunmuştur. Kurula göre; "Yapılan incelemede veri sorumlusunun yurtdışına veri aktarımını sağlamak amacıyla Kurulun onayını almak üzere taahhütname mektuplarını Kurula sunduğu görülmüştür. Ancak Kurulun henüz bu yönde bir karar vermediği ve yeterli korumaya sahip ülkelerin de henüz belirlenmediği değerlendirildiğinde kişisel verilerin yurtdışına aktarılması için tek yöntem ilgilinin açık rızasının alınması olarak değerlendirilmektedir." Kurul, 22 Temmuz 2020 tarih ve 2020/559 sayılı kararında ise, 108 sayılı Sözleşme'nin KVKK'nin yurtdışına veri aktarımı hükümlerine alternatif bir mekanizma olarak kabul edilemeyeceğini açıkça ortaya koymuştur.

Yurt Dışı Veri Aktarımına İlişkin Kararlar	
Karar numarası	**2019/157**
Karar	Kurul, verileri dünyanın farklı yerlerindeki veri merkezlerinde tutan e-posta hizmetlerinin kullanımında yurtdışına veri aktarımı yapıldığına karar vermiştir.
Karar numarası	**2020/173**
Karar	Kurul yurt dışına veri aktarımında açık rızanın alınmadığı ve Amazon Turkey'nin veri aktarımına ilişkin taahhütname mektubunun onaylanmadığını belirtmiştir. Dolayısıyla Amazon Turkey tarafından yapılan yurtdışına veri aktarımının hukuka uygun olmadığına karar vermiştir.
Karar numarası	**2020/559**
Karar	Kurul yurt dışına veri aktarımının hukuka uygunluğu için 108 sayılı Sözleşmenin tek başına yeterli sayılamayacağına ve KVKK'deki hükümlere her hâlükârda uyumlu davranılması gerektiğine karar vermiştir.

5. İlgili Kişiler Tarafından Yapılan Başvuruların Cevaplanması Yükümlülüğü

KVKK'nin 11. maddesi uyarınca herkes veri sorumlusuna başvurarak kendisiyle ilgili aşağıdaki taleplerde bulunabilir:

- Kişisel verilerinin işlenip işlenmediğine ilişkin bilgi verilmesi,
- Kişisel verileri işlenmişse, hangi verilerin işlendiğine ve işlemeye ilişkin bilgi verilmesi,
- Kişisel veri işlemenin amacı ve verilerin bu amacına uygun kullanılıp kullanılmadığı hakkında bilgi verilmesi;
- kişisel verilerin yurt içinde veya yurt dışında aktarıldığı gerçek veya tüzel kişilere yönelik bilgi verilmesi,
- kişisel verilerin eksik veya yanlış işlenmiş olması halinde düzeltilmesini ve KVKK'ya uygun şekilde kişisel verilerin silinmesi veya yok edilmesini talep etme,
- veri aktarımı yapıldığı takdirde, veri sorumlusundan veri alıcısına kişisel verilerin düzeltilmesi, silinmesi ve yok edilmesine yönelik işlemlerin bildirilmesini isteme.

İlgili kişiler ayrıca işlenen verilerinin münhasıran otomatik sistemler aracılığıyla analiz edilmesi suretiyle kendileri aleyhine ortaya çıkan bir sonuca itiraz edebilecekleri gibi; kişisel verilerinin kanuna aykırı olarak işlenmesi nedeniyle herhangi bir zarara uğramaları durumunda zararlarının giderilmesini talep edebilirler.

5.1 Usul

Kurul, veri sorumlularından talepte bulunma yöntem ve usullerini düzenleyen Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'i ("**Başvuru Tebliği**") yayımlamıştır. Başvuru Tebliği kapsamında, veri sorumluları ilgili kişiler tarafından usulüne uygun olarak iletilen taleplere, talebin niteliğine göre en kısa sürede ve en geç 30 gün içinde yanıt vermek zorundadır. Başvuru Tebliği ayrıca, on sayfayı aşan cevaplarda sınırı aşan her sayfa için 1 Türk lirası işlem ücreti veya veri kayıt ortamının maliyetine eşdeğer bir ücret alınabileceğini öngörmektedir.

KVKK'nin 13. ve 14. maddeleri Kurul'a şikâyette bulunma ve veri sorumlularına başvurma sürelerini düzenlenmektedir. Başvuru Sürelerine yönelik detaylar Kurul'un 24 Ocak 2019 tarih ve 2019/9 sayılı kararı ile belirlenmiştir. Karar uyarınca başvuru sürelerinin hesaplanmasında aşağıdaki esaslar geçerlidir:

(i) Veri sorumlusu 30 gün içinde ilgili kişinin talebine yanıt vermezse, ilgili kişi veri sorumlusuna başvuru tarihinden başlayarak 60 gün içinde Kurul'a başvurabilir.
(ii) Veri sorumlusu, ilgili kişinin talebine 30 gün içinde yanıt verirse, ilgili kişi söz konusu yanıtı izleyen 30 gün içinde Kurul'a şikâyette bulunabilir. Bu itibarla söz konusu hallerde ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 günlük süresi bulunmamaktadır.
(iii) Veri sorumlusu KVKK'de tanınan 30 günlük sürenin bitiminden sonra yanıt verdiği durumlarda, ilgili kişi veri sorumlusunun kendisine yanıt verdiği tarihten itibaren 30 gün değil, veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurul'a şikâyette bulunabilir.

İlgili Kişinin Haklarına İlişkin Kararlar	
Karar numarası	**2020/41**
Karar	İlgili kişi kişilik haklarının ihlal edilmesinden doğan tazminat istemlerini genel mahkemeler huzurunda kullanabilir.
Karar numarası	**2019/296**
Karar	Kurul, operatör şirketi olan veri sorumlusunun ilgili kişilere yönelik yeterli başvuru imkânı tanımamış olmasının Başvuru Tebliği'nin 6.maddesini ihlal ettiğine karar vermiştir.
Kurul'un Yetkisine İlişkin Kararlar	
Karar numarası	**2018/156**
Karar	Yargı organlarının yetkisi dahilinde olan ihbar ve şikayetler Kurul tarafından soruşturmaya tabi tutulamaz.
Karar numarası	**2019/138**
Karar	Yargı organlarının yetkisi dahilinde olan ihbar ve şikayetler Kurul tarafından soruşturmaya tabi tutulamaz.

5.2 İlgili Kişinin Başvurusu Kapsamında Atılacak Adımlar

- İlgili kişi taleplerini, veri sorumlusu veya mevcutsa veri sorumlusu tarafından kurulmuş olan veri koruma komitesine iletir.
- İlgili kişinin talebinin önem seviyesi ve türü belirlenir. İlgili kişilerin talepleri şu şekilde sınıflandırılabilir: (i) veri sorumlusu nezdinde işlenen kişisel verilere ilişkin bilgi talepleri, (ii) veri sorumlusu nezdinde işlenen kişisel verilere ilişkin silme talepleri ve (iii) veri sorumlusu nezdinde özel nitelikli kişisel veri işleme faaliyetine ilişkin bilgi talepleri.
- İlgili kişinin talebine KVKK'de öngörülen 30 günlük süre içinde cevap verebilmek için veri sorumlularının bir takip sistemi kullanmaları gerekmektedir.
- Taleplere yönelik veri sorumlusu bünyesindeki ilgili departman resmi bir yanıt hazırlar ve KVKK'nin öngördüğü yollarla ilgili kişiye bu yanıtı iletir. Silme talebinde bulunulması durumunda, silme ve imha politikasına göre kişisel verilerin silinip silinmeyeceği konusunda ilgili departman ve hukuk birimi karar verir. İlgili departmanların kişisel verileri silmeye karar vermesi durumunda, bu işleme ilişkin log kayıtları tutulmalı ve yine ilgili kişiye resmi bir bildirim ile gönderilmelidir.

6. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

Kişisel veriler, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin gerektirdiği şekilde, işlendikleri amaç için gereken süre boyunca saklanacaktır. Bu bağlamda, veri sorumlusu aşağıdaki idari ve teknik önlemleri almakla yükümlüdür;

- Kişisel veri saklama ve imha politikası oluşturmak,
- Veri saklama süreleri ile saklamada uygulanacak teknik ve idari tedbirleri belirlemek,
- Kişisel verilerin bu ilkelere uygun olarak saklanmasını sağlamak.

Veri sorumluları, kişisel veri işlemeleri için ilgili mevzuatta öngörülen sürelere uymak zorundadır. Kanuni bir sürenin açıkça mevcut olmaması durumunda, kişisel veriler yalnızca işlendikleri amaç için gerekli olduğu süre boyunca işlenebilecektir.

Veri sorumluları, kişisel verilerin işlenmesini gerektiren sebeplerinin ortadan kalması halinde kişisel verileri re'sen veya ilgili kişinin talebi üzerine, silmek, yok etmek veya anonim hale getirmekle yükümlüdür (KVKK madde 7).

Silme, yok etme ve anonim hale getirilme işlemlerinin detayları Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ile düzenlenmiştir. Ayrıca bu konudaki uygulamaya açıklık getirmek amacıyla Kurul tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi hazırlanmıştır. Veri Sorumluları Siciline kaydolmakla yükümlü veri sorumluları söz konusu yönetmelik kapsamında öngörülen zorunlu içeriğe uygun şekilde kişisel veri saklama ve imha politikası hazırlamakla yükümlülerdir.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Karar

Karar numarası	**2018/142**
Karar	Banka ilgili bankacılık mevzuatı gereği kişisel verileri saklamak mecburiyetindedir. Dolayısıyla veri işleme faaliyetini sürdürmede hukuka uygunluk sebebini haizdir.

7. Veri Güvenliğine İlişkin Yükümlülükler

KVKK madde 12 uyarınca veri sorumluları aşağıdakileri yapmakla yükümlüdür:

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak

Veri sorumlusu, bu yükümlülükleri yerine getirmek adına uygun bir koruma sağlamak için gerekli tüm teknik ve idari tedbirleri almak zorundadır. GDPR'den farklı olarak, veri işleyenlerin hakları ve yükümlülükleri, KVKK kapsamında ayrı ve özel olarak düzenlenmemiştir. Ancak veri güvenliğine yönelik olarak veri işleyenlerin veri güvenliğini tedbirleri ile ilgili veri sorumlusu ile birlikte müştereken sorumlu olduğu KVKK'de belirtilmiştir. Bu çerçevede, veri işleyenler, kendilerine aktarılan kişisel verileri işlerken veri sorumlusunun talimatlarına uymakla, edindikleri kişisel verileri herhangi bir şekilde açıklamamakla ve kişisel verileri veri sorumlusu tarafından belirlenen işleme amacı dışında işlememekle yükümlülerdir.

KVKK altındaki veri güvenliği tedbirlerine ek olarak, özel nitelikli kişisel verilerin korunmasının hassasiyetini göz önünde bulunduran Kurul, özel nitelikli kişisel veriler için daha nitelikli ve kapsamlı bir koruma sağlamak amacıyla bir kararında veri sorumluları için özel nitelikli verilere ilişkin ek veri güvenliği tedbirleri alma koşulu getirmiştir.

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 10 Temmuz 2020 tarihinde kamu otoriteleri ve kritik altyapı hizmeti veren işletmeler tarafından verilerin korunması için alınacak veri güvenliği tedbirlerine ilişkin bir rehber yayımlamıştır. Kurul'un uygulaması ile uyumlu olan rehber, telefonlarda internet güvenliği ve siber güvenlik, bulut bilişim uygulamaları, kripto uygulamaları, sıkılaştırma tedbirleri gibi çeşitli konularda veri korunmasına yönelik oldukça detaylı kurallar içermektedir. İşbu rehber, kamu otoritelerine ve kritik altyapı hizmeti veren işletmelere rehberlik etmek için yayınlanmış olsa da özel kuruluşlar açısından da yol gösterici niteliktedir. Bir kamu otoritesi olması itibariyle rehberle de paralel hareket etmesi beklenen Kurum'un, veri sorumluları tarafından yeterli koruma tedbirlerinin alınıp alınmadığını değerlendirirken bu rehberde öngörülen hususları da dikkate alacağını varsaymak yanlış olmayacaktır.

Veri Güvenliğine İlişkin Kararlar

Karar numarası **2018/10**

Bu karar ile Kurul, özel nitelikteki kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemleri ortaya koymuştur.

Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikteki kişisel veridir.

Kararda alınması gereken önlemler aşağıdaki başlıklar altında detaylandırılmıştır:
- Özel nitelikli kişisel verilerin güvenliğine ilişkin politika ve prosedürler
- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik önlemler
- Özel nitelikli kişisel verilerin elektronik ortamda işlenmesi halinde alınacak önlemler
- Özel nitelikli kişisel verilerin fiziki ortamda işlenmesi halinde alınacak önlemler
- Özel nitelikli kişisel verilerin aktarımında alınacak önlemler

Karar numarası **2019/308 sayılı ilke kararı**

Kurul bu ilke kararında kullanıcıların kimlik ve iletişim bilgileri gibi kişisel verilerine erişim imkanı sağlayan belirli yazılım, program ve uygulamaların hukuk büroları, finans ve gayrimenkul danışmanları veya sigorta gibi sektörlerde faaliyet gösteren firmalar tarafından kullanılmasının KVKK'nin 12. maddesinde öngörülen veri güvenliği ilkesini ihlal ettiğini tespit etmiştir.

Kurul, veri sorumlusu olarak hareket eden ve yukarıda ifade edilen yazılımları kullananlar hakkında savcılık nezdinde suç duyurusunda bulunacağını ve KVKK madde18 kapsamında idari para cezasına çarptıracağını ilan etmiştir.

Karar numarası	**2019/269**
Karar	Kurul Facebook'u muhtemel veri ihlallerini engellemek ve ihlalin gerçekleşmesi durumunda Kurul'a bildirmek konusunda gerekli teknik ve idari tedbirleri almadığı gerekçesiyle idari para cezasına çarptırmıştır.
Karar numarası	**2019/ 389**
Karar	Kurul, duyuru süreçlerinde bir üniversitenin gerekli veri güvenliği önlemlerini alması gerektiğine ve ilgili kişileri veri işleme faaliyetleri konusunda bilgilendirmesi gerektiğine karar vermiştir.

8. Kişisel Veri İhlali Bildirimi

Veri sorumluları, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirmekle yükümlüdür. Kurul, gerekmesi halinde veri ihlalini kurumsal internet sitesinde veya uygun gördüğü diğer yöntemlerle ilan edebilir.

8.1 Bildirim Usulüne İlişkin Kurallar

Kişisel veri ihlali bildirimi süreci için özel bir kanuni düzenleme öngörülmemiştir; öte yandan Kurul, 24 Ocak 2019 tarih ve 2019/10 sayılı kararı ile ihlal bildirimine ilişkin süreçleri belirlemiştir. Söz konusu karar kapsamında açıklanan prosedürle ilgili gereklilikler aşağıdaki şekilde özetlenebilir:

- Veri sorumlusu, ihlali öğrendiği andan itibaren 72 saat içinde Kurul'u ve veri ihlalinden etkilenen kişileri belirlenmesini müteakip makul olan en kısa süre içerisinde uygun yöntemlerle ilgili kişileri bilgilendirir.
- Veri sorumlusu haklı bir gerekçe ile 72 saat içinde Kurul'a bildirimde bulunamazsa, ayrıca gecikmeye sebep olan nedenleri Kurul'a belirtmelidir.
- Kişisel veri ihlali bildirimleri, Kurul tarafından ilan edilen standart form (Kişisel Veri İhlali Bildirim Formu) üzerinden yapılır.
- Formda istenen bilgilerin veri sorumlusu tarafından bir defada sağlanamaması durumunda, veri sorumlusu herhangi bir gecikmeye mahal vermeksizin bu bilgileri aşamalı olarak Kurul'a iletebilir.
- Veri sorumlusu, veri ihlali ile ilgili bilgileri, ihlalin etkilerini ve bu kapsamda alınan önlemleri kayıt altına almalı ve gerekirse Kurul'un incelemesine hazır halde bulundurmalıdır.
- Veri işleyenlerin işleme faaliyetlerinde bir veri ihlali meydana gelirse, veri işleyenler kendi organizasyonları içinde oluşan ihlalleri derhal veri sorumlularına bildirmekle yükümlüdür.
- Yurt dışında bulunan veri sorumlusu nezdinde bir veri ihlali meydana gelmesi durumunda: (i) ihlalin sonuçları Türkiye'de yerleşik ilgili kişileri etkiliyorsa ve (ii) ilgili kişiler veri sorumlusu tarafından sağlanan ürün ve hizmetlerden Türkiye'de faydalanıyorsa, yurt dışında yerleşik veri sorumlusu tarafından Kurul'a bildirimde bulunulur.
- Veri sorumluları, bir "veri ihlali müdahale planı" hazırlamak ve bunu periyodik olarak gözden geçirmekle yükümlüdür. Bu plan, veri sorumlusunun organizasyonu içerisinde veri ihlalinin kime bildirilmesi gerektiği, kimin veri ihlalinin olası sonuçlarının değerlendirilmesinden sorumlu tutulacağı ve KVKK kapsamında yapılacak bildirimler gibi sürece yönelik önemli bilgileri içermelidir.

8.2 Bildirim İçeriği

Kişisel Veri İhlali Bildirim Formunda, aşağıdaki konularla ilgili bilgiler Kurul'un incelemesine sunulmalıdır:

- **Veri Sorumlusuna İlişkin Bilgiler:** Veri sorumlusunun unvanı/adı ve adresi doldurulmalı ve söz konusu bildirim formunu hazırlayan kişiye ilişkin bilgiler verilmelidir.
- **Veri İhlaliyle İlgili Bilgiler:** Veri sorumluları, veri ihlalinin nasıl meydana geldiği, veri ihlalinin kaynağı, veri ihlalinin nasıl ve ne zaman tespit edildiği, ihlalden etkilenen kişisel veri kategorileri ve ihlalden etkilenen ilgili kişiler gibi hususlarda ayrıntılı bilgi sağlamalıdır.
- **Kurula ve Etkilenen İlgili Kişilere Yapılacak Bildirime İlişkin Bilgiler:** Veri sorumluları, Kurul'a zamanında bildirimde bulunmama nedenleri (veri ihlalinin tespiti ve bildirimi arasında 72 saatten fazla zaman geçmişse), etkilenen ilgili kişilerin ne zaman ve nasıl bildirileceği, hangi kurumlara bildirimde bulunulacağına yönelik bilgi verir.
- **Olası Sonuçlara İlişkin Bilgiler:** Veri sorumluları, ihlal sebebiyle ilgili kişilerin önemli olumsuz etkilere maruz kalma olasılığı ve kendi organizasyonu içinde ihlalin etkileri konusunda Kurul'u bilgilendirmelidir.
- **Veri İhlalinden Sonra Alınan veya Alınacak Önlemlere İlişkin Bilgiler:** Veri sorumluları, veri ihlaline karışan çalışanların aldıkları eğitimleri, veri ihlallerinin önlenmesi için teknik ve idari önlemlerin önceden alındığını, veri ihlalinden sonra alınacak teknik ve idari önlemlere ilişkin planlamaları belirtmelidir.

8.3 Veri İhlali Durumunda Alınacak Aksiyonlar

Veri sorumlusu nezdinde bir veri ihlali meydana gelmesi durumunda aşağıdaki adımlar atılmalıdır;

- Öncelikle, tüm veri sorumlularının bir veri ihlali müdahale planına sahip olması ve bunu periyodik olarak gözden geçirmesi gerekir.
- Veri sorumlusu, veri ihlali ile ilgili kayıtları tutmak için gerekli altyapılara sahip olmalıdır.
- İhlalin tespiti üzerine veri sorumluları, veri ihlalinin meydana geldiği sistemleri kapatmalı ve veri ihlalinin kaynağını araştırılmalıdır.
- Veri ihlalinin kaynağı araştırılırken, veri ihlalinden etkilenen veri grupları, ihlalden etkilenen kişi sayısı ve veri sahibi kategorileri belirlenmelidir.
- Veri güvenliği için teknik ve idari tedbirler derhal alınmalıdır.
- Kişisel Veri İhlali Bildirim Formu,

gecikmeden ve veri sorumlusunun bu tür ihlali öğrendiği tarihten itibaren 72 saat içinde doldurulmalıdır. Bildirimin kısmen yapılabileceği ve veri sorumlularının Veri İhlal Bildirim Formunu Kurula gönderdikten sonra yenileyebilecekleri unutulmamalıdır.

- Veri sorumluları ayrıca etkilenen veri gruplarının bildirimi için bir bildirim formu hazırlamalıdır.
- Kurula ve ilgili kişilere bildirim yapıldıktan sonra, veri sorumluları veri güvenliğini yeterli düzeyde temin etmek için ek teknik ve idari önlemler alınmalıdır.

Kurul ayrıca Kişisel Veri İhlali Bildirim Formunun nasıl doldurulacağına ve Kurul tarafından oluşturulan veri ihlali bildirim sisteminin nasıl kullanılacağına dair bir rehber yayınlamıştır.

Kurul, 18 Eylül 2019 tarihli 2019/271 sayılı kararı kapsamında, veri ihlali bildiriminin amacının, ilgili kişilerin ihlal nedeniyle maruz kalabileceği olumsuz sonuçların hızlı bir şekilde önlenmesi veya en aza indirilmesi olduğunun altını çizmiştir. Bu bağlamda; Kurul, ilgili kişilere yapılan veri ihlali bildirimlerin açık ve sade bir dille yapılması gerektiğini ve asgari olarak aşağıdaki hususları içermesi gerektiğini belirtmiştir:

- Veri ihlalinin meydana geldiği zaman,
- Veri ihlalinden etkilenen veri kategorileri (kişisel veriler / özel nitelikli kişisel veriler ayrımı yapılarak),
- Veri ihlalinin olası sonuçları,
- Veri sorumlusu tarafından olası olumsuz etkileri azaltmak adına alınmış veya alınması önerilen tedbirler,
- İlgili kişilerin veri ihlali ile daha fazla bilgi edinebileceği irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun internet sitesinin tam adresi, çağrı merkezi vb. iletişim yolları.

Veri İhlali Bildirimlerine İlişkin Örnek Kararlar	
Karar numarası	**2019/104**
Karar	Kurul, Facebook'u zamanında veri ihlalini bildirme yükümlülüğünü yerine getirmediği gerekçesiyle idari para cezasına çarptırmıştır. İhlal 19.09.2018 tarihinde tespit edilmesine karşılık süresi içinde herhangi bir bildirimde bulunulmamış ve ihlal 13.09.2018- 25.09.2018 sürmesine rağmen bildirim 17.12.2018 tarihinde yapılmıştır.
Karar numarası	**2019/222**
Karar	Kurul Dubsmah Inc. Şirketini ihlalden ancak 19 gün sonra bildirim yapmış olması nedeniyle idari para cezasına çarptırmıştır
Karar numarası	**2019/269**
Karar	Kurul, Facebook'u zamanında veri ihlalini bildirme yükümlülüğünü yerine getirmediği gerekçesiyle idari para cezasına çarptırmıştır

9. Veri Sorumluları Sicil Bilgi Sistemi

VERBİS, veri sorumlularının veri işleme faaliyetlerini kaydettikleri bir çevrimiçi sicil kayıt sistemidir. Kural olarak, tüm veri sorumluları kişisel verileri işlemeden önce VERBİS'e kayıt yaptırmakla yükümlüdür (KVKK madde 16). Bununla birlikte, Kurul bazı durumlarda kayıt yükümlülüğüne istisna getirebilir.

Bu bağlamda Kurul, belirli meslek gruplarını, dernekleri ve siyasi partileri kayıt zorunluluğundan istisna tutan çeşitli kararlar yayımlamıştır. Kurul ayrıca yurtiçinde yerleşik veri sorumlularına da ilk etapta genel bir muafiyet tanımıştır:

• Çalışan sayısı 50'den az VEYA
• Yıllık mali bilanço toplamı 25 Milyon TL'nin altında olan veri sorumluları kayıt yükümlülüğünden muaftır.

Bu eşiklerden birini aşan tüm yurtiçinde yerleşik veri sorumluları, diğer istisnalara dahil olmadıkları sürece VERBİS'e kaydolmalıdır.

Yurt dışında yerleşik veri sorumluları için Kurul herhangi bir özel koşul öngörmemektedir. Bu nedenle Türkiye kaynaklı kişisel veri işleyen yurt dışında yerleşik tüm veri sorumluları (bilanço tutarı veya çalışan sayısına bakılmaksızın) VERBİS'e kayıt yaptırmakla yükümlüdür.

Kayıt yükümlülüğü için son tarih Kurul tarafından üç kez uzatılmıştır. Yılda 50'den fazla çalışanı olan veya yıllık toplam mali bilançosu 25 milyon TL'yi aşan veri sorumluları ve/veya Türkiye dışında yerleşik veri sorumluları için başta son tarih 30 Eylül 2019 olarak belirlenmiş; ancak sırasıyla 31 Aralık 2019, 6 Haziran 2020 ve 30 Eylül 2020 tarihlerine ertelenmek suretiyle kayıt süresi uzatılmıştır.

Kayıt için güncel tarihler aşağıdaki gibidir:

- Yıllık 50'den fazla çalışanı olan veya yıllık mali bilanço toplamı 25 milyon TL'yi aşan veri sorumluları ve / veya yurtdışında yerleşik veya kayıtlı veri sorumluları için **30 Eylül 2020,**
- 50'den az çalışanı olan ve yıllık mali bilanço toplamı 25 milyon TL'nin üzerinde olan ancak ana faaliyet konusu özel nitelikli kişisel veriler işleme olan veri sorumluları için **31 Mart 2021,**
- Kamu kurum ve kuruluşu veri sorumluları için **31 Mart 2021**

Kurul, 1 Ekim 2020 tarihinde sicile kayıt yükümlülüğü hakkında kamuoyu duyurusu yayınlamış ve bazı veri sorumlularının 01 Ekim 2020 tarihi itibarıyla VERBİS kaydı için başvuruda bulunmadığını veya başvurularına rağmen bildirimlerini tamamlamadıklarını belirtmiştir. Kurul, 1 Ekim 2020 tarih ve 2020/760 sayılı kararında COVID-19 nedeniyle fiili, teknik veya hukuki imkansızlıklar nedeniyle bazı veri sorumlularının VERBİS'e kayıt yükümlülüğünü yerine getiremediğini göz önüne alarak, VERBİS'e kayıt yükümlülüğünü yerine getirmemiş olan veri sorumlularına bu durumun Kurul tarafından gönderilecek bir yazı ile bildirilmesini uygun bulmuştur. Bu doğrultuda Kurul tarafından yazılı olarak kendisine bildirim yapılan veri sorumlularının Kurul tarafından kendilerine verilen süre içerisinde VERBİS'e kaydolması gerekmektedir. Kurul'un bu kararı veri sorumluları açısından bir erteleme olarak yorumlanmamalı ve veri sorumlularına verilen son bir hak olarak görülmelidir.

Yurt dışında yerleşik veri sorumlularının VERBİS'e kaydolmaları için yapmaları gereken işlemlerin ana hatları aşağıda açıklanmıştır. Kayıt sürecinin ilk aşaması olarak, veri sorumlularının VERBİS kullanıcı hesaplarını oluşturmaları ve VERBİS üzerinden irtibat kişilerini atamaları gerekmektedir.

9.1 Kişisel Verilere Yönelik Veri Envanterinin Hazırlanması

Veri sorumluları, Türkiye kaynaklı işlediği tüm kişisel veri işleme süreçlerini içeren bir veri envanteri hazırlamalılardır. Veri envanteri, KVKK kapsamında belirlenen gerekli tüm bilgileri içermeli ve bu bilgilerin doğru ve güncel olması veri sorumluları tarafından sağlanmalıdır. Veri sorumlularının VERBİS'e bildirdikleri bilgilerde herhangi bir değişiklik meydana gelirse, söz konusu değişikliklerin meydana geldiği tarihten itibaren 7 gün içinde VERBİS üzerinden Kurum'a bildirilmesi gerekmektedir.

Veri envanteri asgari olarak aşağıdaki bilgileri içermelidir:

- Tanıtıcı bilgiler (veri sorumlusunun veya temsilcisinin adresi dahil),
- Veri sorumlusu tarafından işlenen veri kategorileri,
- Her veri kategorisi için işlemenin amaçları,
- Her veri kategorisi için azami muhafaza edilme süresi,
- Her veri kategorisi için veri konusu kişi grupları,
- Seçilen veri kategorilerinin yurt dışına aktarılıp aktarılmadığına ilişkin bilgiler,
- Kişisel verilerin aktarıldığı veri alıcısı grupları,
- Veri sorumlusu tarafından alınan veri güvenliği tedbirleri.

VERBİS kayıtları kamuya açık biçimde tutulur, dolayısıyla herkes VERBİS'teki kayıtlara ulaşarak veri sorumlularının veri işleme süreçlerine yönelik detayları takip edebilir.

9.2 Veri Sorumlusu Temsilcisi Atanması

Yurt dışındaki veri sorumlularının VERBİS'e kayıt süreci, hem veri sorumlusu temsilcisi (Türkiye'de yerleşik tüzel kişiliği veya Türkiye'de yerleşik gerçek kişi) hem de irtibat kişisi (Türk vatandaşı gerçek kişi) atamayı gerektirdiğinden Türkiye'de yerleşik veri sorumlularının kayıt süreçlerine nazaran daha karmaşıktır.

Türkiye'de yerleşik olmayan veri sorumluları tarafından, Türkiye'de bir veri sorumlusu temsilcisi atamak için öncelikle veri sorumlusunun yetkili organ veya kişisi tarafından atamaya yönelik bir karar alınmalıdır. Veri sorumlusu temsilcisi, VERBİS üzerinden çevrimiçi kayıt formunu doldurmalı ve veri sorumlusu temsilcisinin atanmasına ilişkin kararın tasdikli örneği ile birlikte Kurul'a sunmalıdır.

Kurul tarafından kullanıcı kaydının oluşturulması akabinde, veri sorumlusu temsilcisi VERBİS üzerinden bir irtibat kişisi atar.

VERBİS'e kayıt işleminin hızlı bir şekilde yürütülmesi için, kayıt sürecinin veri sorumlusu temsilcisinin kayıtlı e-posta adresi (KEP) üzerinden yürütülmesi tavsiye edilir, veri sorumlusu temsilcisinin kayıtlı e-postası yoksa yetkili kuruluşlardan alabilir veya gerekli belgeleri Kurum'a posta yoluyla gönderebilir

9.3 İrtibat Kişisinin Atanması

Veri sorumluları, Kurul ile iletişimden sorumlu bir irtibat kişisi atamakla yükümlüdür. İlgili kişi VERBİS'e bildirilecek ve VERBİS ile ilgili bildirimler, ilgili kişinin e-devlet hesabı üzerinden yapılacaktır. İrtibat kişisinin atanmasına ilişkin kurallar aşağıdaki gibidir:

- İrtibat kişisi Türk vatandaşı ve Türkiye'de ikamet eden gerçek kişi olmalıdır.
- İrtibat kişisi 18 yaşından büyük olmalıdır.
- İrtibat kişisi aynı anda birden fazla veri sorumlusunun irtibat kişisi olamaz.
- Veri sorumlusunun aynı anda birden fazla irtibat kişisi olamaz
- Veri sorumlusu, irtibat kişisini istediği zaman değiştirebilir.
- Veri sorumlusu, kendi irtibat kişisi olarak kendi bünyesinde çalışan birini veya kurum dışından üçüncü bir kişiyi atamayı seçebilir.

[2] KEP, kayıtlı e-posta hizmeti vermeye yetkili firmalardan alınan elektronik posta adresidir. Bilgi Teknolojileri ve İletişim Kurumu'nun yetkili sağlayıcılar listesine bu bağlantıdan ulaşabilirsiniz: https://www.btk.gov.tr/kayitli-elektronik-posta-hizmet-saglayicilar

Veri Sorumlusu KEP'e sahip değilse, yetkili bir servis sağlayıcıya başvurmalı ve aşağıdaki belgeleri sağlamalıdır:
- Başvuru Formu
- Veri sorumlusunun MERSİS numarasını içeren ticari faaliyet sertifikası
- Veri Sorumlusunun imza sirküleri
- Başvuru, veri sorumlusunun yasal temsilcisi olmayan bir gerçek kişi tarafından yapılacak ise vekaletname
- Asıl başvuru sahibi için uygun kimlik belgeleri

KEP adresi aktif ve çalışır durumda olmalıdır.

E. Yaptırımlar

1. İdari ve Cezai Yaptırımlar

KVKK hükümlerine uygun davranılmaması halinde KVKK altında ciddi yaptırımlar öngörülmüştür. KVKK hükümlerinin ihlali, ihlalin türüne ve derecesine bağlı olarak idari para cezasına (KVKK madde 12) ve cezai yaptırımlara (5237 sayılı TCK madde135-140) yol açabilir.

İdari yaptırım uygulandığı hallerde, yaptırımın muhatabı, veri sorumlusu olarak tüzel kişiliğin kendisi olacaktır. Cezai yaptırımlar konusunda ise, diğer bazı hukuk sistemlerinden farklı olarak, Türkiye'de tüzel kişilerin cezai sorumluluğu olmadığından cezai sorumluluk, veri sorumlusu şirketlerde yönetim kademesindeki çalışanlar nezdinde doğacaktır. Bunun dışında tüzel kişilere yönelik güvenlik tedbirleri uygulanması da mümkündür.

Şikâyette bulunanlar, KVKK'nin ihlalinin suç teşkil ettiği durumlarda TCK ve KVKK hükümleri kapsamında ilgili savcılıklara başvurabilirler. Ayrıca söz konusu ihlal nedeniyle kişilik haklarının ihlali halinde ilgili kişiler tarafından genel mahkemeler nezdinde dava açılabilir.

1.1 İdari Yaptırımlar

KVKK kapsamındaki belirli yükümlülüklere uyulmaması halinde çeşitli idari yaptırımlar gündeme gelir. (KVKK madde 18):

- Bilgilendirme yükümlülüğüne aykırılıkta 9.0384 TL- 196.689 TL arasında idari para cezası verilir.
- Veri güvenliği yükümlülüğünün ihlalinde 29.503 TL- 1.966.862 TL arasında idari para cezası verilir.
- Kurul kararına uyulmaması halinde 49.172 TL- 1.966.862 TL arası idari para cezası verilir.
- VERBİS'e kayıt yükümlülüğünün ihlalinde 39.337 TL - 1.966.862 TL arasında idari para cezası verilir

1.2 Cezai Yaptırımlar

TCK;

• Madde135 uyarınca kişisel verileri hukuka aykırı olarak kaydeden kişiye 1 yıldan 3 yıla kadar hapis cezası verilir. Kanuna aykırı olarak kaydedilen kişisel verilerin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda ise hapis cezası 4,5 yıla kadar çıkarılabilir.

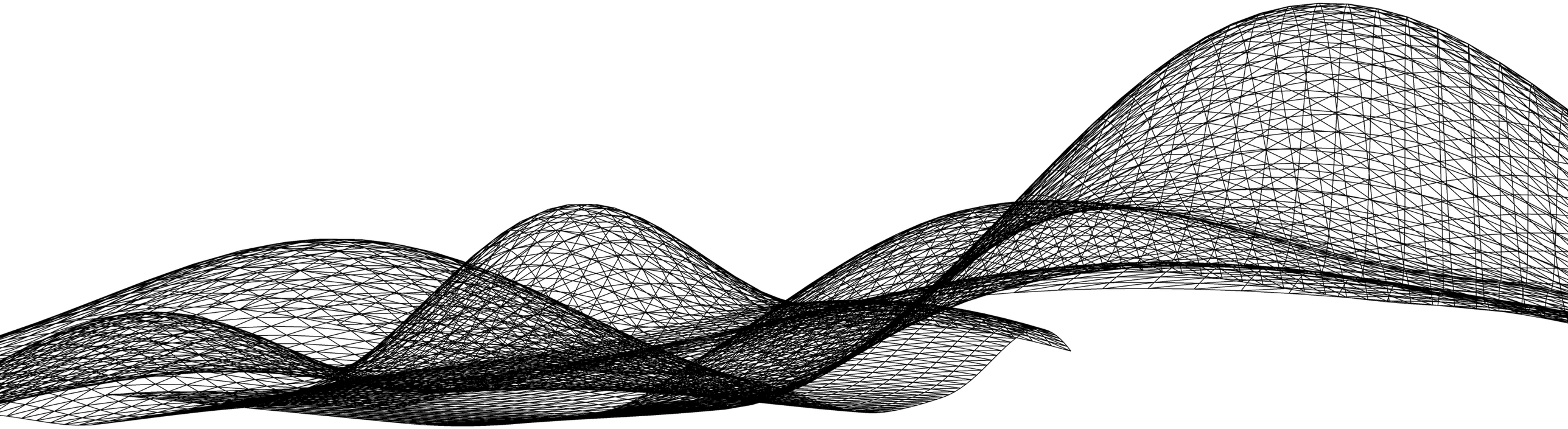
• Madde136 uyarınca kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişiye 2 yıldan 4 yıla kadar hapis cezası verilir. Bu suçların, (i) bir kamu görevlisinin görevinin verdiği yetkisini kötüye kullanması veya (ii) bir meslekten veya ticaretten elde edilen ayrıcalıklardan yararlanma yoluyla işlenmesi halinde, hapis cezası 6 yıla kadar yükseltilebilir.

• Madde138 uyarınca kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde 1 yıldan 2 yıla kadar hapis cezası verilir. Suç konusu Ceza Muhakemesi Kanunu hükümleri uyarınca imhası zorunlu olan bir veri ise verilen ceza 4 yıla kadar artırılabilir.

[2] KVKK kapsamında belirlenen idari para cezası tutarları her yıl güncellenmektedir. Burada 2021 yılı tutarlarına yer verilmiştir

MOROĞLU ARSEVEN

II. KURUL FAALİYETLERİNİN İNCELENMESİ



A. Genel Bakış

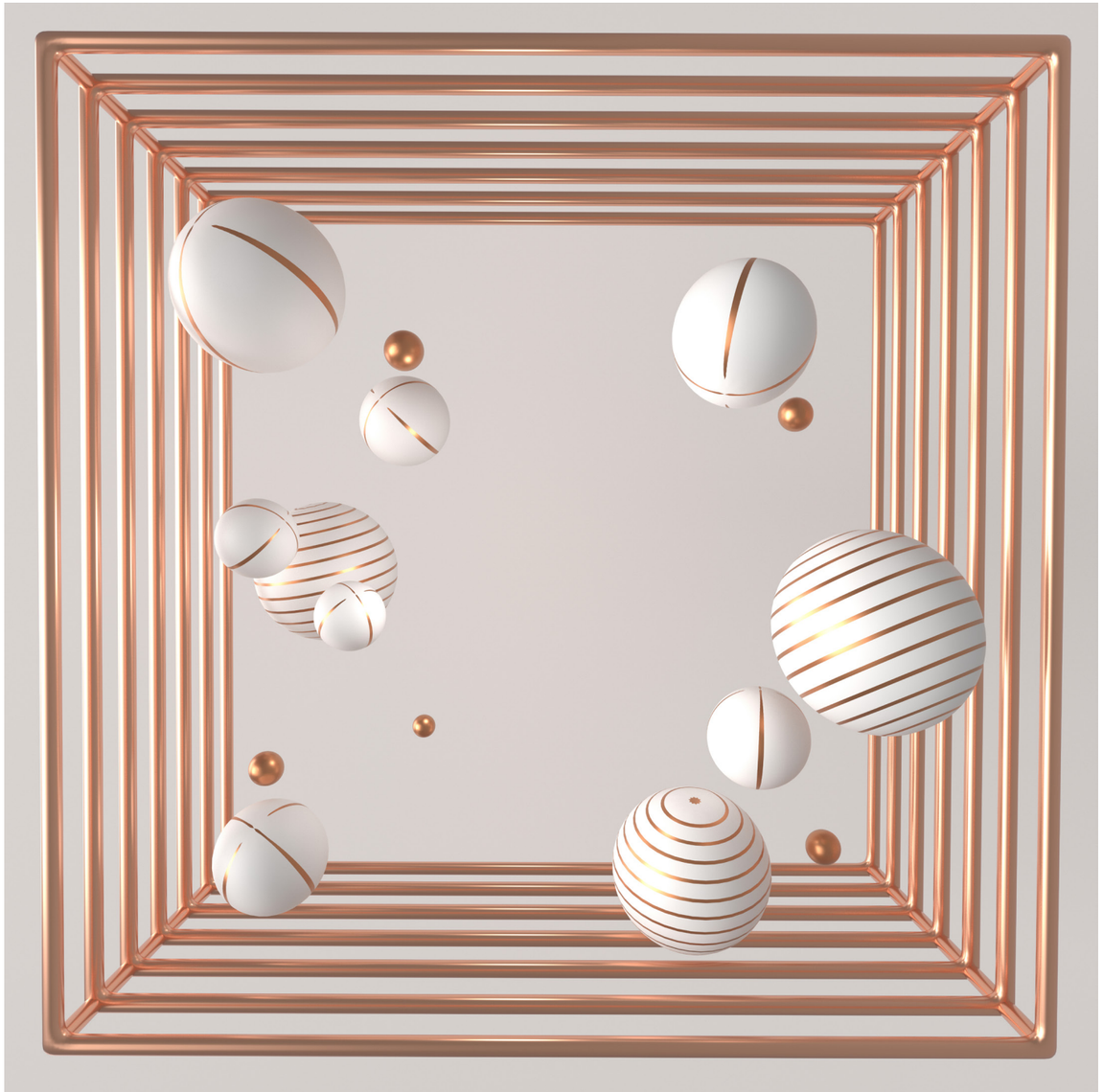
Kurum'un karar organı olan Kurul tarafından 2017 yılından bu yana pek çok karar alınmıştır. Kararların bir kısmı düzenleyici nitelikte olup ikincil mevzuat niteliği taşırken, birçoğu ise icrai nitelikte olup gerçek ve tüzel kişi veri sorumluları hakkında uygulanan bireysel kararlardır.

Türkiye'deki Rekabet Kurulu ve Sermaye Piyasası Kurulu gibi diğer düzenleyici kurumlardan farklı olarak Kurul'un kararlarının yayımlanmasına yönelik herhangi bir zorunluluk bulunmamaktadır. Kurul, hangi kararın, ne şekilde ve ne kadar ayrıntılı olarak paylaşılması gerektiğine kendi takdir yetkisi ile karar vermektedir.

Kurul bugüne kadar toplam 86 karar yayımlamıştır. Yayınlanan kararların 6 tanesi ilke kararı olarak yayımlanmıştır ve kararların tam metnine Kurum'un kurumsal internet sitesinde yer verilmiştir.

Yayımlanan kararların geri kalan 75 adedi bireysel nitelikte olup; bu kararların sadece kısa özetleri detaylara girilmeksizin Kurum'un kurumsal internet sitesinde yayımlanmıştır. Birkaç istisna dışında yayımlanan bireysel kararlarda genel olarak karara konu ilgililerin isimleri/unvanları yer almamaktadır. Buna karşılık son zamanlarda yayımlanan bireysel kararların daha detaylı, bilgilendirici olduğu ve özetlenen kararlarda veri sorumlularının sektör bilgilerine yer verildiği görülmektedir.

Ek olarak, Kurul KVKK madde12/5 uyarınca; etkilenmesi muhtemel ilgili kişileri bilgilendirmek için gerekli gördüğü veri ihlali bildirimlerini yayımlamaktadır ve şimdiye kadar Kurul'un resmi internet sitesinde yaklaşık 60 adet veri ihlal bildirimi yayımlanmıştır. Yayımlanan bu bildirimler genellikle veri sorumluları tarafından sunulan veri ihlali bildirim formunda yer alan bilgilerin özetlenmiş versiyonlarıdır.



MOROĞLU ARSEVEN

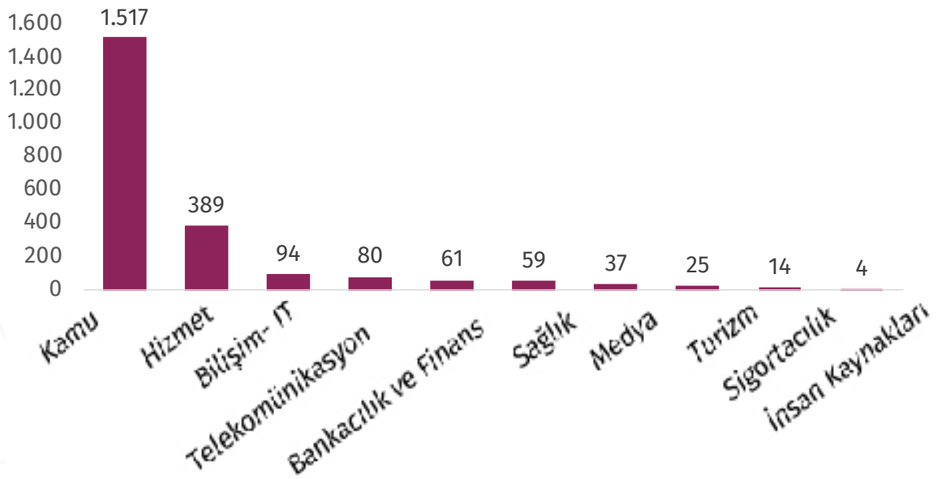
MOROĞLU ARSEVEN

B. Kurul'un Faaliyetlerine Yönelik İstatistiki Veriler

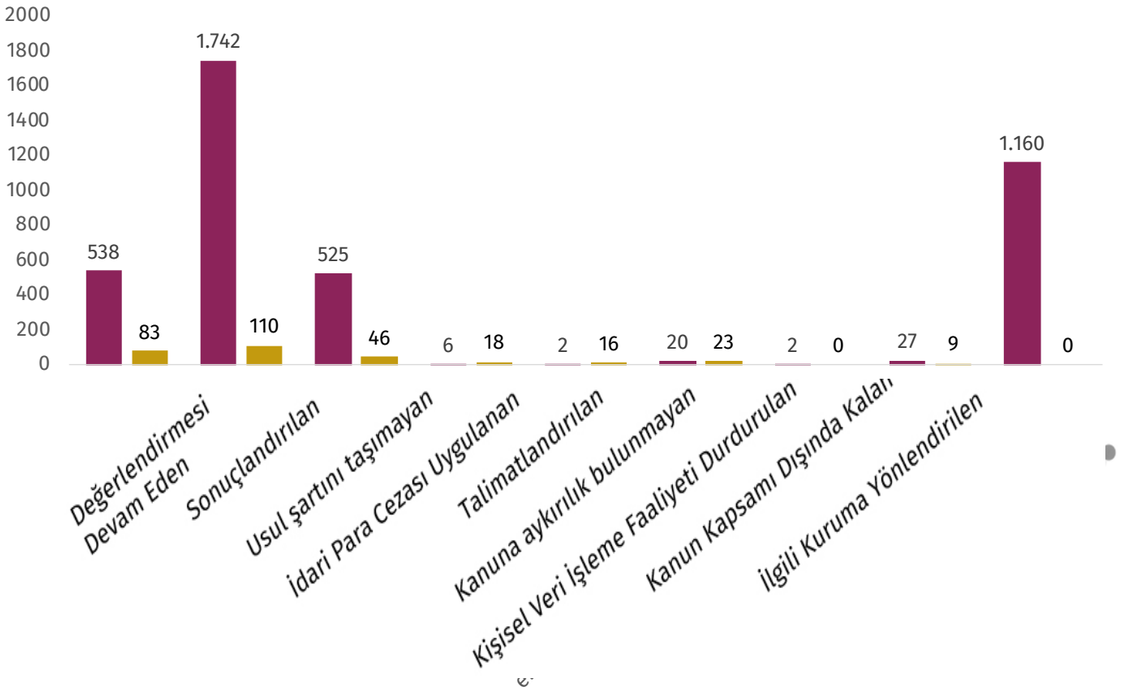
Kurul'un yayımlamış olduğu 2019 yılı Faaliyet Raporunda açıklanan bazı istatistiki veriler aşağıdaki gibidir:

1. Şikayetler

1.1 Şikayetlerin Sektör Bazında Dağılımı

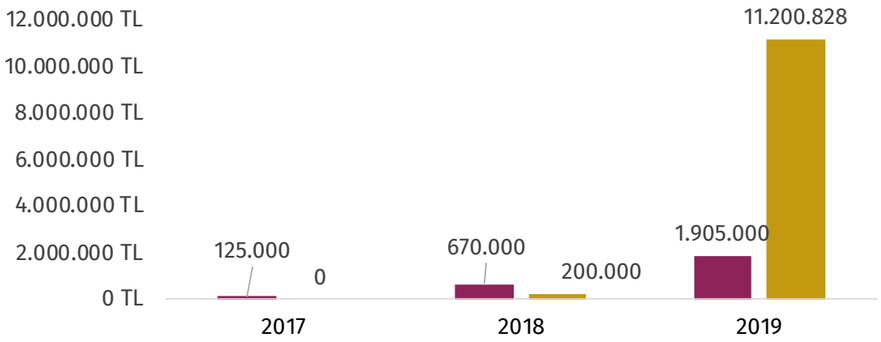


1.2 Şikâyet ve İhbar Sayıları

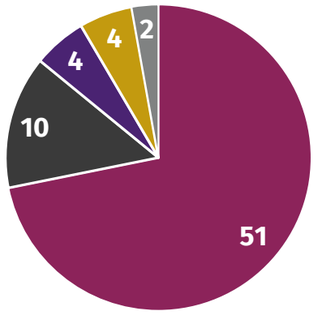


2. Kurul Kararları

2.1 İdari Yaptırımlar

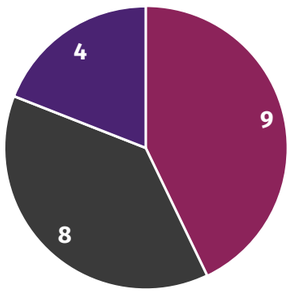


2.2 Yaptırımların İncelenmesi



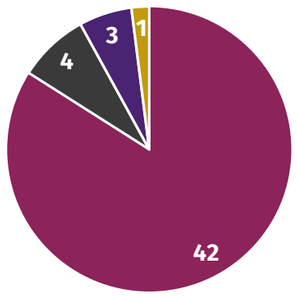
- Kişisel verilerin hukuka aykırı işlenmesini önlemek için gerekli teknik ve idari tedbirlerin alınmaması nedeniyle idari para cezası,
- Kişisel verilerin hukuka aykırı olarak işlendiğinin makul bir sürede Kurula ve veri sahiplerine bildirilmemesi nedeniyle idari para cezası,
- Kurulun talimatlarını ve ihlalleri giderme emirlerini yerine getirmeme nedeniyle idari para cezası,
- Genel veri koruma ilkelerine uyulmaması nedeniyle idari para cezası,
- Veri sahiplerinin haklarını düzenleyen 11. maddeye uyulmaması nedeniyle idari para cezası.

• Sektörlere Göre Yayınlanan Kararlar



- Bankacılık ve Finans
- Bilişim ve Telekomünikasyon
- Sağlık

İlgili Kanun Maddelerine Göre Yayınlanan Kararlar



- Aydınlatma Yükümlülüğünün İhlal Edilmesi nedeniyle idari para cezası – madde18/1 (a)
- Veri Güvenliği Kurallarına Uyulmaması nedeniyle idari para cezası-madde 18/1 (b)
- Kurul kararlarına uyulmaması nedeniyle idari para cezası-madde 18/1 (c)
- Kayıt yükümlülüklerine uyulmaması nedeniyle idari para cezası madde 18/1 (ç)
- Kamu kurumları ve resmi makamların kararlarına ilişkin disiplin hükümleri-madde 18/3

EN YÜKSEK İDARİ PARA CEZALARI

Aşağıdaki tablodan görülebileceği üzere, en çok idari para cezası kesilen ilk beş karara bakıldığında Bilişim ve Medya sektörünün en çok ceza alan sektör olarak ilk sırada geldiği görülmektedir. İlgili kararlar incelendiğinde ise, bu beş karardan dördünde veri ihlallerinin idari aksaklıklardan çok bilgi sistemlerindeki aksaklıklar ve Kurul'a zamanında bildirimde bulunulmamasından kaynaklandığı anlaşılmaktadır.

No	Veri Sorumlusunun Adı	Sektör	İhlal Edilen Madde	Toplam Ceza	Tarih
1	Facebook	Bilgi Teknolojileri ve Medya	Madde 12/1, Madde 12/5	TRY 1.650.000	11.04.2019
2	Facebook	Bilgi Teknolojileri ve Medya	Madde 12/1,Madde 12/5	TRY 1.550.000	18.09.2019
3	Marriott International Inc.	Turizm	Madde 12/1, Madde 12/5	TRY 1.450.000	16.05.2019
4	Dubsmash Inc.	Bilgi Teknolojileri ve Medya	Madde 12/1, Madde 12/5	TRY 730.000	17.07.2019
5	Clickbus Seyahat Hizmetleri A.Ş.	Ulaşım	Madde 12/1, Madde 12/5	TRY 550.000	16.05.2019
6	Cathay Pasific Airway Limited	Ulaşım	Madde 12/1, Madde 12/5	TRY 550.000	16.05.2019
7	Belirtilmemiş	Turizm	Madde 12/1, Madde 12/3, Madde 12/5	TRY 500.000	27.08.2019
8	Belirtilmemiş	Spor salonu	Madde 12/1, Madde 12/3 Madde 12/5	TRY 225.000	27.02.2020
9	Belirtilmemiş	Bankacılık ve Finans	Madde 12/1	TRY 210.000	06.02.2020
10	Belirtilmemiş	Elektronik	Madde 12/1, Madde 15/5	TRY 200.000	14.02.2019 05.03.2019
11	S Şans Oyunları A.Ş.	Bilgi Teknolojileri ve Medya	Madde 12/1, Madde 12/5	TRY 180.000	27.08.2019
12	Belirtilmemiş	Teknik servis	Madde 12/1	TRY 150.000	14.02.2019
13	Belirtilmemiş	Medya	Madde 12/1	TRY 125.000	09.12.2019
14	Belirtilmemiş	Bilgi Teknolojileri ve Medya	Madde 11, Madde 12/1 Madde 10	TRY 110.000	27/01/2020
15	Belirtilmemiş	Bankacılık ve Finans	Madde 4/2, Madde 12/1	TRY 100.000	18.09.2019
16	Belirtilmemiş	Havayolları	Madde 12/1	TRY 100.000	01.10.2019
17	Belirtilmemiş	Sigorta	Madde 12/1	TRY 100.000	07.11.2019
18	Belirtilmemiş	Bankacılık ve Finans	Madde12/1Madde12/5	TRY 100.000	26.11.2019

Madde 12/1: Kişisel verilerin hukuka aykırı olarak işlemeyi önlemek için gereken teknik ve idari önlemlerin alınmaması
Madde 12/3: Kuruluş içinde KVKK'ye uygunluğun denetlenmemesi
Madde 12/5: İşlenen kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edildiğinin makul bir sürede Kurula ve ilgili kişilere bildirilmemesi
Madde 15/5: Kurulun ihlallerin giderilmesine yönelik talimat ve emirlerinin yerine getirilmemesi.

C. Önemli Kararlar

1. Gerekli Teknik ve İdari Tedbirlere İlişkin Kararlar

Karar No: 2019/104
Sektör: Bilişim teknolojileri ve medya

Karara konu olay Facebook sistemindeki bir API hatasına ilişkindir. Facebook çalışanları Facebook platformuna giriş yapan ve üçüncü taraf uygulamalara izin veren kullanıcıların, fotoğraf API'si hatasından etkilendiğini tespit etmiştir. Bu bağlamda bazı üçüncü taraf uygulamaların 13-25 Eylül 2018 tarihleri arasında 12 günlük bir sürede yetkilerini aşan düzeyde fotoğrafa erişmiş olabilecekleri duyurulmuştur. Kurul'a göre 12 gün süren ihlale Facebook tarafından zamanında müdahale edilmemesi gerekli teknik ve idari tedbirlerin alınmasında eksiklerin olduğunu göstergesidir . Söz konusu veri ihlalinin toplamda 6.8 milyon, Türkiye'de de yaklaşık 300 bin kullanıcıyı etkileme ihtimali bulunmaktadır. Ayrıca Facebook'un üçüncü taraf uygulamaların normalde erişime izin verilmiş olan sayıdan daha fazla spesifik fotoğrafa gerçekten erişip erişemediklerini belirleyemediği dikkate alınmış ve bu durum Facebook'un kendi platformundaki veri akışını kontrol etme noktasında sıkıntılar yaşadığı şeklinde yorumlanmıştır. Sonuçta Kurul bugüne kadar verdiği en yüksek tutarlı cezayı vererek, Facebook'u 1.650.000 TL idari para cezasına çarptırmıştır.

Karar No: 2019/269
Sektör: Bilişim teknolojileri ve medya

Facebook temsilcileri, 25 Eylül 2018'de e-posta yoluyla, farklı Facebook özellikleriyle ilgili birden fazla hatanın, kompleks etkileşiminden kaynaklanan bir veri ihlaline neden olduğunu Kurul'a bildirmiştir. 14 Eylül 2018 ile 28 Eylül 2018 arasında, saldırganlar, Facebook'un üç farklı özelliğindeki hatanın etkileşimiyle oluşan erişimler aracılığıyla kullanıcıların kişisel verilerine ulaşabilmişlerdir. Saldırıdan Facebook'u Türkçe kullanan 280.959 kullanıcı etkilenmiştir. Söz konusu hataların test aşamasında tespit edilip düzeltilmesi gerekirken, Facebook, bu konuda gerekli idari ve teknik önlemleri zamanında alamamıştır. Ayrıca, güvenlik açığının 21 Temmuz 2017 ile 27 Eylül 2018 tarihleri arasında 14 ay sürdüğü ve hatayla ilgili herhangi önlemin zamanında alınmadığı göz önüne alındığında, Kurul, Facebook'un bu konuda gerekli idari ve teknik önlemleri almadığına karar vermiştir.

Karar No: 2019/143
Sektör: Turizm ve otelcilik

Karara konu veri ihlali Marriott tarafından devralınan ve misafir verileri içeren Starwood veri tabanına yetkisiz erişim sağlanmasından kaynaklanmıştır. Söz konusu erişim 2014 yılından 2018 yılına kadar devam etmiştir. Saldırgan sunucuya eriştikten sonra truva atı (RAT) yükleyerek uzaktan erişim imkanı elde etmiştir. İhlalin 4 yıl sürdüğü, pek çok kişinin bundan olumsuz etkilendiği, veri ihlalinin ağırlığı ve bildiriminin zamanında yapılmadığı hususları göz önüne alınarak Kurul tarafından 1.450.000 TL idari para cezasına karar verilmiştir.

Karar No: 2020/191, 2020/192, 2020/193, 2020/194
Sektör: Bankacılık ve finans

Risk Merkezi üyeleri tarafından kredi puanı sorgu adetlerindeki artışa dair yapılan ihbar neticesinde Kurul tarafından bir soruşturma başlatılmıştır. Soruşturma neticesinde 4 faktoring şirketinin çalışanlarının Risk Merkezi verilerini kullanarak kredi puanlarını ve üçüncü kişilere ait verileri kontrol ettikleri ve bu bilgileri başka üçüncü kişilere aktardıkları tespit edilmiştir. Gerekli teknik ve idari tedbirlerin alınmamış olmasından bahisle, Kurul ihlalin önlenmemesi ve bildirimin yapılmamış olmasını da dikkate alarak faktoring şirketlerine toplam 1.400.000 TL idari para cezası uygulamıştır.

Karar No: 2020/286
Sektör: Bilişim ve medya

Karara konu ihlalde oyuncu bilgilerini içeren oyun şirketine ait bulut sistemlerine yetkisiz erişim sağlanması söz konusudur. Log kayıtlarının incelenmesiyle bu erişim tespit edilmiştir. Kurul'a göre saldırganların bulut sistemine erişimi, zafiyet testlerinin yetersiz olduğu anlamına gelmektedir. Ayrıca gerekli teknik önlemler ancak ihlal gerçekleştikten sonra alınmıştır. Yine ihlal bildiriminin yapılmamış olmasından da hareketle Kurul oyun şirketinie1.100.000 TL idari para cezası kesmiştir.

2. Kişisel Veri Aktarımı

Karar No: 2020/559
Sektör: Otomotiv

Otomotiv sektöründe faaliyet gösteren veri sorumlusu tarafından reklam/bilgilendirme amaçlı gönderilen bir kısa mesaj (SMS) hakkında ilgili kişinin şikayeti üzerine yürütülen inceleme sürecinde anlaşıldığı kadarıyla, veri sorumlusunun kullandığı web tabanlı toplu mesaj gönderme yazılımı kapsamında kişisel verilerin bir AB ülkesindeki bulut veri tabanına aktarılması söz konusu olmakta ve ilgili kişilere tanıtım mesajları gönderilmektedir. Buradaki temel hukuki sorun verinin işlenmesi ve aktarımının KVKK'ye uyumlu biçimde olup olmadığıdır.

Kurul, bu kararında 108 sayılı Sözleşme'nin yurt dışına aktarım için yeterli olup olmadığını değerlendirmiş, 108 sayılı Sözleşme'ye taraf olmasının, bir ülkenin güvenli ülke statüsü tayini bakımından tek başına yeterli olmadığını, ancak bu hususun Kurul tarafından yeterli korumaya sahip ülkeler belirlenirken Kurul tarafından göz önüne alınacağını belirtmiştir. Bu kapsamda, veri sorumlusunun yurt dışı veri aktarımı için 108 sayılı Sözleşmeye dayanmasını KVKK'ye aykırılık olarak değerlendirip veri sorumlusuna 900.000 TL idari para cezası kesmiştir.

Karar No: 2020/173
Sektör: Bilişim ve medya

Karara konu olan olay, e-ticaret sektöründe faaliyet gösteren veri sorumlusunun ilgili kişilerin açık rızası olmaksızın kişisel verileri yurtdışına aktarımıdır. Gizlilik bildiriminde, internet sitesi ziyaret edildiğinde ilgili kişinin gizlilik bildirimlerinde yer alan koşulları kabul ettiği belirtilmektedir. İlgili kişilerin kişisel verilerinin aktarılması durumunda aktarım hakkında bilgilendirileceği ve vazgeçme hakkının saklı olacağı belirtilmiştir. Kurula göre, açık rıza, aydınlatma metni ile eş zamanlı temin edilemez ve opt-out yani bireyin önceden onayı almaksızın kişisel verilerinin işlenmesine otomatik onay verdiği sistemler geçerli değildir Bu nedenle, olayda geçerli bir açık rıza yoktur. Ek olarak, aydınlatma metninde yurtdışına veri aktarımı için herhangi bir bilgi verilmemiştir. Açık rızanın bilgilendirilmeye dayanması gerektiğinden, açık rızasını veren ilgili kişiye bilgi verilmeden alınan rıza geçerli kabul edilemez. Bu nedenlerle Kurul, yurtdışına veri aktarımı için açık rıza alınmadığına ve dolayısıyla aktarımın hukuka aykırı olduğuna hükmetmiştir.

Karar No: 2019/157
Sektör: N/A

Kurul, görüş talebi üzerine e-posta hizmetlerinin kullanımına ilişkin bir karar vermiştir. Kurul'a göre, (yurt dışı tabanlı bir e-posta hizmetinin altyapısının kullanılması, verilerin dünyanın her yerindeki veri merkezlerinde tutulmasına neden olacaktır. Bu durumda kişisel verilerin bu e-posta hizmetleri üzerinden aktarılabilmesi için yurtdışına veri aktarımına ilişkin esaslara uyulması gerekmektedir.

Karar No: 2020/26
Sektör: Hukuki hizmetler

Karara konu olan olayda, ilgili kişinin aleyhine başlatılan infaz işlemlerine ilişkin olarak ilgili kişinin yakınlarına gönderilen kısa mesajlar söz konusudur. Veri sorumlusu hukuk bürosu, bir müvekkili olan bankanın, ilgili kişiden alacağını tahsil etmek için bir icra takibi başlatmıştır. İlgili kişi, hukuk bürosu tarafından aranmış ve ilgili kişiye icra takibi konusunda bilgilendirmek için birkaç kısa mesaj gönderilmiştir. Mesajlar ayrıca ilgili kişilerin akrabalarına da gönderilmiştir. Veri aktarımı Kurul tarafından hukuka aykırı bulunmuş ve veri sorumlusu hukuk bürosuna idari para cezası verilmiştir.

Karar No: Kurul tarafından hazırlanan Rehberinde yer almakta olup Karar numarası belirtilmemiştir
Sektör: N/A

Karara konu olay, ilgili kişinin kişisel verilerini içeren bir belgenin aynı isim ve soyadına sahip bir başkasına gönderilmiş olmasıdır. Kurul'a göre, Birsöz konusu olay, ilgili kişilerin kimlik doğrulaması için veri sorumlusunun sisteminde bir kusur olduğunu göstermektedir. Ayrıca soruşturma sırasında ilgili kişinin kişisel verilerinin, ilgili kişinin herhangi bir talebi olmaksızın bir çalışan tarafından sistemde birkaç kez arandığı anlaşılmaktadır. Sonuçta veri sorumlusuna idari bir yaptırım uygulanmıştır.

Karar No: 2019/389
Sektör: Eğitim

Kurul, görüş talebi üzerine, başvuru sonuçlarının internet üzerinden açıklanmasına ilişkin bir karar vermiş ve yayınlamıştır. Bir üniversite tarafından akademik alanda çalışacak adaylara dair sonuçların resmi internet sitesinde ilan edilmesi talebi yapılmıştır. Kurul'a göre, sonuçların sadece adaya açık olması ve kimlik doğrulama ile ulaşılması gerekmektedir. Sonuçlar, kişisel bilgiler maskelenerek, yalnızca ad ve soyadlarının baş harfleri ile kimlik numaralarının ilk ve son iki rakamı belirtilmek suretiyle de üniversite internet sitesinde yayınlanabilir.

[5]https://www.kvkk.gov.tr/Icerik/5416/Kisisel-Veri-Guvenliginin-Saglanmasi-Amaciyla-Uygun-Guvenlik-Duzeyini-Temin-Etmeye-Yonelik-Gerekli-Idari-ve-Teknik-Tedbirlerin-Alinmamasi

3. Özel Nitelikli Kişisel Veriler

Karar No: 2020/649
Sektör: N/A

Kurul, görüş talebi üzerine biyometrik imzaya ilişkin bir karar vermiştir. Kişilerin yürüyüş biçimi, klavyeye basış şekli, akıllı cihazları kullanırken uyguladığı basınç ve basış şekli, araba sürüş biçimi gibi veriler davranışsal nitelikte biyometrik verileri oluşturur. Açık rızanın olmadığı durumlarda, biyometrik veriler ancak kanunla öngörüldüğü takdirde işlenebilir. Şayet biyometrik veri işleme kanunla öngörülmüşse, söz konusu hüküm şüpheye yer bırakmayacak kadar açık olmalıdır. Biyometrik imza, imzalarını belirli biyometrik verileri kullanarak özel bir tablet/ped üzerinde oluşturan hizmet sağlayıcıları tarafından elde edilir ve bu veriler genellikle imzalanan belgeye ayrılmaz bir şekilde bağlanır. Biyometrik imza çözümleri belirli bir standart çerçevesinde tanımlanmadığından, farklı kurgusal özelliklere sahiptirler ve ıslak imza ile denk kabul edilmezler.

TBK'de imzaya ilişkin hükümler, klasik imza ve elektronik imzaya ilişkin düzenlemelerden oluşur. Bu hükümlerin biyometrik imzayı içerecek şekilde yorumlanması, "kanunda öngörülen" istisnasının geniş yorumlanmasına yol açacak ve orantılılık ilkesine aykırı olacaktır. Kurul, bu değerlendirmeler ışığında, biyometrik imzanın özel nitelikli kişisel veri olarak değerlendirilebileceğine, ancak kişinin açık rızası varsa veya kanunda açıkça belirtilmişse işlenebileceğine karar vermiştir. TBK'de yer alan sözleşmelerin şekline ilişkin hükümler, "kanunda açıkça öngörülme" şartını yerine getirmemektedir.

Karar No: 2019/81
Sektör: Sağlık

Karara konu olay, tesis girişleri için iki spor salonunun kimlik doğrulama yöntemi uygulamasıdır. Veri sorumluları, tesislere girişlerde kimlik belirleme amacıyla el-avuç okutma sistemi kullanmaktadırlar. Avuç içi izi, biyometrik bir veri olması sebebiyle Kurul tarafından özel nitelikli kişisel veri olarak kabul edilmektedir. Veri sorumluları el-avuç okutma sistemine yönelik ilgili kişilerden açık rıza almış olsa da, Kurul avuç içi izi bilgilerinin alınmasına rıza göstermemeleri halinde ilgili kişilerin söz konusu hizmetten yararlanamayacakları dikkate alındığında, üyeler tarafından verilen açık rızaların özgür iradeye dayalı olduğunu söylemenin mümkün bulunmadığını vurgulamış, spor salonu girişlerinde biyometrik veri işlemesinin "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi ile bağdaşmadığını belirtmiş, bu nedenle, veri sorumluları tarafından biyometrik verilerin işlenmesine yönelik alınan açık rızanın hukuka aykırı ve geçersiz olduğuna ve biyometrik verilerin silinmesine karar vermiş; ayrıca veri sorumluları hakkında idari para cezası uygulamıştır.

4. Açık Rıza ve Aydınlatma Yükümlülüğü

Karar No: 2018/90
Sektör: N/A

Karar, internet sitesinden iş başvuruları alan bir veri sorumlusu hakkındadır. Veri sorumlusuna özgeçmiş göndermek ve pozisyona başvurmak için kayıt zorunludur. Başvuru sahipleri, açık rızalarını vermek ve aydınlatma metnini okuduklarını kabul etmek için tek bir kutucuğu işaretlemektedirler. Kurul'a göre, aydınlatma metni ilgili kişinin herhangi bir onayına tabi değildir ve kişisel verilerin her işleme faaliyeti için ilgili kişilerin ayrıca bilgilendirilmesi gerekir. Bu itibarla Kurul, aydınlatma metninin okunduğuna ilişkin geri bildirim alınması ile ilgili kişilerin kişisel verilerinin işlenmesi hususunda gerekli seçimlik haklarının da tanındığı açık rıza metninin onaylandığının ispatını sağlayacak mekanizmaların birbirinden ayrıştırılması gerektiğini vurgulayarak, veri sorumlusunu bu gerekliliklere uyması için talimat vermiştir.

Karar No: 2019/82
Sektör: Market zinciri

Karar, bir market zincirinin sadakat programı hakkındadır. İlgili kişinin sadakat programına üye olabilmesi için açık rıza zorunlu tutulmuştur. Kurul'a göre sadakat programı üyelerine özel indirimler gibi çeşitli faydalar sunmakta ise de ilgili kişi sadakat programına üye olmadan da ürünleri satın alabilmektedir. Bu nedenle, hizmetlerin sunumu için açık rıza zorunlu değildir. Açık rızalarının verilmesi ilgili kişilere daha avantajlı satın alma fırsatları sunsa da ilgili kişiler için isteğe bağlı niteliktedir. Bu nedenle hizmet veya ürün için açık rıza zorunlu olmadığından Kurul tarafından veri işlemenin hukuka uygun olduğu tespit edilmiştir.

Karar No: 2019/206
Sektör: N/A

Karar, çevrimiçi hizmetler sağlayan bir veri sorumlusu hakkındadır. Veri sorumlusunun internet sitesinin ana sayfasına erişmek için, bir e-posta adresiyle kayıt yapılması gerekmektedir. Kurul'a göre, ilgili hizmet için açık rıza zorunlu tutulmuştur ve bu nedenle olaydaki açık rıza geçersizdir. Ayrıca veri sorumlusu tarafından hazırlanan aydınlatma metninde kişisel verilerin işlenmesinin tek hukuki dayanağı açık rıza olarak ifade edildiği vurgulanmış, açık rıza dışındaki işleme şartlarının da aydınlatma metnine açıkça eklenmesi gerektiği belirtilerek, veri sorumlusuna aydınlatma metni ve açık rızayı hukuka uygun hale getirilmesine yönelik talimat verilmiştir.

Karar No: 2019/122
Sektör: Bankacılık ve finans

Karar, bir veri sorumlusunun aydınlatma metni hakkındadır. Aydınlatma metinlerinde, kişisel verilerin işlenmesinin KVKK'nin 5. ve 6. maddelerinde öngörülen işleme şartlarına dayandırıldığı belirtilmektedir. Ancak somut olayda veri sorumlusunun kişisel verilerin işlenmesi için hangi işleme şartına dayandığı açıkça belirtilmemiştir. Kurul'a göre, aydınlatma metninde veri sorumlusunun kişisel verileri hangi hukuki sebeple işlediği açık bir şekilde ilgili kişiye bildirilmek zorundadır.

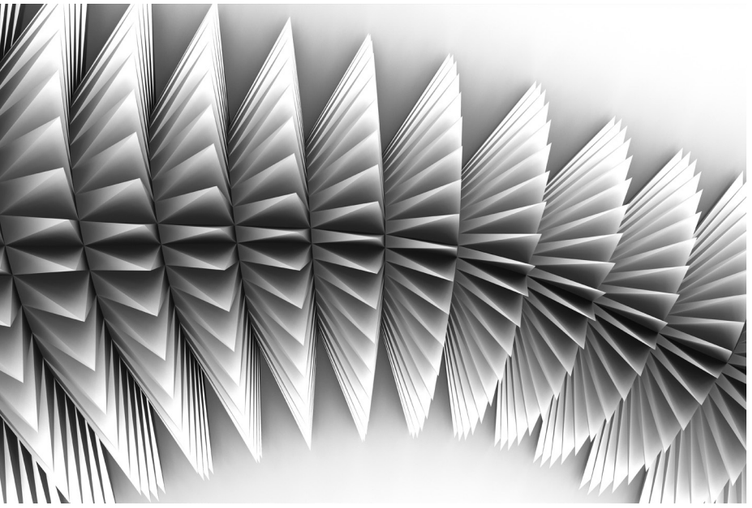
5. Veri Sorumlusuna Başvuru

Karar No: 2019/296
Sektör: Telekomünikasyon

Karar, bir ilgili kişinin kimlik doğrulamasının yapılamaması nedeniyle veri sorumlusunun internet sitesi üzerinden yaptığı başvurunun reddiyle ilgilidir. Veri sorumlusu, ilgili kişiyi, kimlik doğrulama amacıyla formu doldurup noter veya kayıtlı e-posta yoluyla göndererek başvurusunu yapmaya yönlendirmiştir. Kurul'a göre, Tebliğ ile ilgili kişilere sağlanan başvuru yöntemleri veri sorumluları tarafından sınırlandırılamaz veya sadece belirli yöntemlerle kısıtlanamaz.

Karar No: 2019/294
Sektör: Havayolu taşımacılığı

Karar, veri sorumlusuna kullanıcı adı ve parola bilgisini değiştirmek için başvuran bir ilgili kişinin kimlik fotokopisini talep eden havayolu şirketi hakkındadır. Kurul'a göre, başvuru sahibinin kimlik doğrulaması için ek bilgi talep etmek hukuka uygun olmakla birlikte, kimlik kartı kopyaları kan grubu ve din gibi özel nitelikli kişisel verileri de içermektedir. Bu nedenle, yalnızca kanunda açıkça belirtilmişse işlenebilirler. Kimlik kartlarının kopyalanmasında açık rıza alınmamasının ve kimlik kopyalama sisteminin veri işleme ilkelerine aykırı olduğu sonucuna ulaşılmıştır.



D.Veri İhlali Bildirimleri

KVKK'nin 12. maddesinde düzenlenen veri ihlallerini bildirme yükümlülüğü konusunda kamuoyunu bilgilendirmek adına, Kurul tarafından 2 Ağustos 2018 tarihinden bu güne kadar yaklaşık 60 adet veri ihlali bildirimi yayınlanmıştır. Öte yandan, 4 adet veri sorumlusuna veri ihlal bildiriminin yanı sıra Kurul tarafından kesilen idari para cezası da duyurulmuştur.

Kurul tarafından 2018 yılında veri ihlaline ilişkin verilen ilk kararda sadece veri sorumlusuna verilen idari para cezasının nedeni açıklanmıştır. Veri sorumlusunun adı/unvanı, ne kadar idari para cezası verildiği veya kaç kişinin ve hangi veri kategorilerinin veri ihlalinden etkilendiği gibi veri ihlaline ilişkin başkaca hususlarda bir açıklamada bulunulmamıştır. 2 Ağustos 2018 tarihinde yayınlanan ilk veri ihlal bildiriminin ardından Kurul, veri ihlali ile ilgili daha detaylı bilgileri kamuya açıklamaya başlamıştır.

Kurul tarafından yayınlanan veri ihlali bildirimleri yer alan bilgi seti aşağıdaki gibidir;

- Veri sorumlusu tarafından veri ihlalinin nasıl ve ne zaman tespit edildiğinin, veri ihlalinin nasıl meydana geldiğinin ve hangi sistemlerin etkilendiğinin özeti,
- Kurul'a bildirimin ne zaman yapıldığı,
- Veri ihlalinden Türkiye'de kaç kişinin etkilendiği ve hangi veri kategorileri ve veri öznesi gruplarının etkilendiği,
- Veri ihlali sonrasında veri sorumlusu tarafından hangi önlemlerin alındığı,
- İlgili Kişilerin verilerinin etkilenip etkilenmediğini hangi yollarla öğrenebileceği ve veri ihlaline maruz kaldıkları durumda kişisel verileri hakkında nasıl daha fazla bilgi edinebileceği.

Önemli Veri İhlali Bildirimleri

- Kurul tarafından 8 veri sorumlusuna yaklaşık 7.000.000 TL tutarında idari para cezası verilmiştir.
- Kurul Facebook'a veri ihlali nedeniyle 1.650.000 TL'lik şimdiye kadarki en yüksek idari para cezasını uygulamıştır. Facebook'a uygulanan para cezasının ardından benzer gerekçelerle Marriott International Inc.'e de1.450.000 TL idari para cezası verilmiştir.
- Kurul, yurt dışında yerleşik 7 veri sorumlusunun veri ihlali bildirimlerini yayımlamıştır.

Aşağıdaki tablo, Kurul tarafından yayımlanan veri ihlali bildiriminin sektör bazında dağılımını göstermektedir.

Sektör	Karar sayısı
Araç Kiralama	15
Teknoloji-Medya	9
Bankacılık	5
Turizm	5
Seyahat	2
Satış	2
Telekomünikasyon	1
Kamu Kurum	1
Ecza	1
Sigorta	1
Diğer	5

III. KURUL'UN GÜNDEMİ

A. 11. Kalkınma Planı

11. Kalkınma Planı'nda KVKK'nin GDPR baz alınarak güncellenmesinin beklendiği açıklanmış olup; KVKK'de yer alan bazı kavramların GDPR dikkate alınarak değiştirilmesi ve/veya genişletilmesinin söz konusu olabileceği belirtilmiştir.

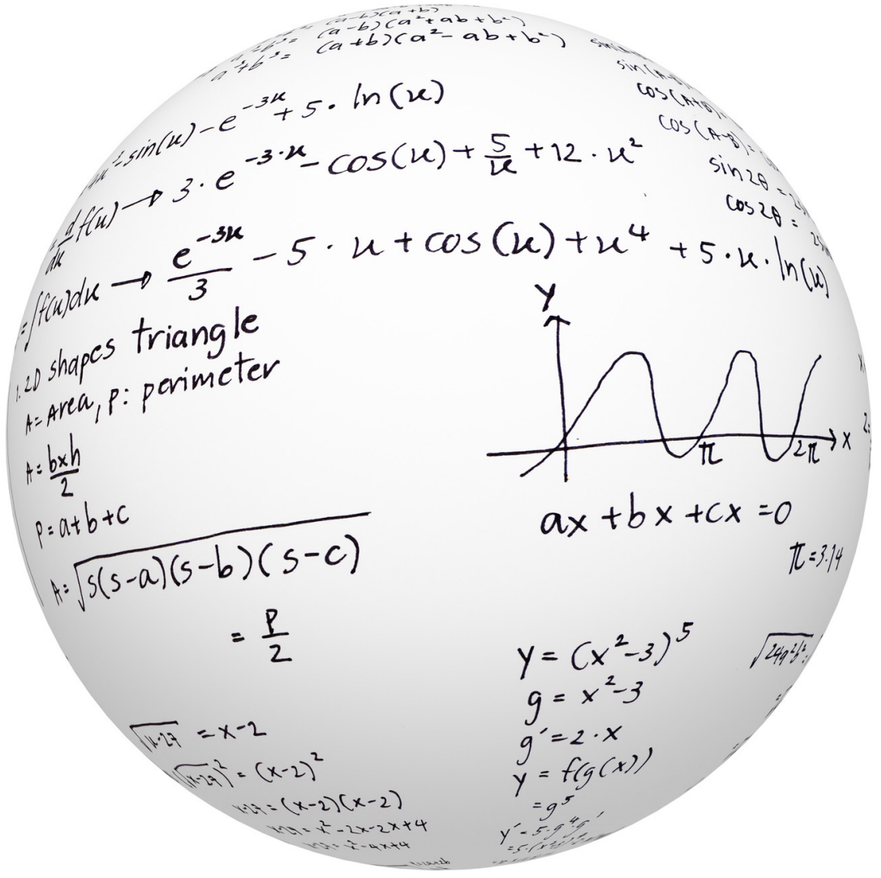
GDPR'de olduğu gibi, KVKK'nin uygulama kapsamı, Türkiye'de yerleşik gerçek kişileri hedefleyen veya Türkiye'de yerleşik gerçek kişilerin davranışlarının izlenmesini içeren tüm veri işleme faaliyetlerini kapsayacak şekilde belirlenebilir. Kısıtlama hakkı ve veri taşınabilirliği gibi ilgili kişilere yeni haklar tanınması gündeme gelebilir. İdari para cezasının hesaplanma yönteminde de değişiklik olabileceği değerlendirilmektedir. İdari para cezalarında belirli üst – alt sınırlar yerine, veri sorumlusunun cirosuna dayalı bir hesaplama yöntemi benimsenebilir. Bunların yanı sıra, KVKK'ye "veri koruma görevlisi", "veri işleme kayıtları" ve "veri koruma denetimleri", "özel ve olağan veri koruması ("data protection by design and by default") ve "müşterek veri sorumluları" gibi kavramların eklenmesi söz konusu olabilir.

Son olarak, veri işleme faaliyetleri başlamadan önce veri korumasına ilişkin alınacak önlemlerin, veri koruma etki değerlendirmeleri ve GDPR kapsamında öngörüldüğü üzere Kurul'a önceden danışılması suretiyle detaylıca düzenlenmesi de söz konusu olabilecektir.

B. AB İlerleme Raporu

2020 AB İlerleme Raporu'nda , kişisel verilerin korunmasına ilişkin temel beklentiler, KVKK'nin AB mevzuatı olan GDPR ile uyumlu hale getirilmesi ve Kurum'un bağımsızlığının sağlanması olarak açıklanmaktadır. Rapor'da, AB'nin Kurum'un bağımsızlığına ve KVKK tahtında düzenlenmekte olan muafiyetler kapsamında devletin yurtdışından Türkiye'ye gönderilen kişisel verilere istihbarat gerekçesi ile erişim yetkisi olmasına dair endişeleri yer almaktadır. Rapor'da ayrıca 2018 tarihli 108 sayılı Sözleşme'de yapılan değişiklik protokolünün Türkiye tarafından imzalanmamış olmasına da değinilmiştir.

KVKK ve GDPR'ın uyumlaştırılması ile bu endişelerin belirli bir düzeyde çözülmesi beklenmektedir. 11. Kalkınma Planı'nda da düzenlendiği üzere, KVKK'nin GDPR esas alınarak değiştirilmesi planlanmaktadır. Bu durumda AB ile kişisel verilerin korunmasına ilişkin daha benzer bir rejim ve muafiyetler uygulama alanı bulacaktır.



IV. VERİ KORUMA ALANINDA BEKLENEN GELİŞMELER

A. Yurt Dışı Veri Aktarımı

Bölüm I.D.4'te açıklandığı gibi, yurtdışına veri aktarımının hukuka uygun olarak gerçekleştirilmesi için mevcut aşamada uygulanan öncelikli yöntem ilgili kişinin açık rızasının aranmasıdır. Bununla birlikte, KVKK uyarınca yurtdışına veri aktarımında açık rıza şartının istisnalarından birinin varlığı halinde; (i) aktarım yapılan tarafın Kurul tarafından belirlenen yeterli korumaya sahip ülkelerden birinde bulunması veya (ii) veri aktarıcısı ile veri alıcısı arasında Kurul tarafından asgari içeriğe uygun bir taahhütname imzalanması ve Kurul'un izninin alınması halinde, ilgili kişinin açık rızası aranmaksızın yurtdışına kişisel veri aktarılması mümkündür. Grup şirketler açısından BŞK'ler yurt dışı aktarım süreçlerinin yönetilmesinde alternatif bir yöntem teşkil etmektedir.

Yurt dışı aktarımlara yönelik olarak,

- Kurul tarafından yeterli koruma sahip ülkelerin açıklanması ve
- Kurul'a halihazırda sunulmuş yurt dışı aktarım taahhütleri ile BŞK'lerin Kurul tarafından onaylanması

beklenmektedir.

B. Çocukların Kişisel Verilerinin Korunması

KVKK çocukların kişisel verilerinin korunmasına yönelik özel bir düzenleme öngörmemektedir.

GDPR ile uyum sürecinde, KVKK'ye reşit olmayan bireylere ait kişisel verilerin işlenmesine dair düzenlemelerin de eklenmesi beklenmektedir.

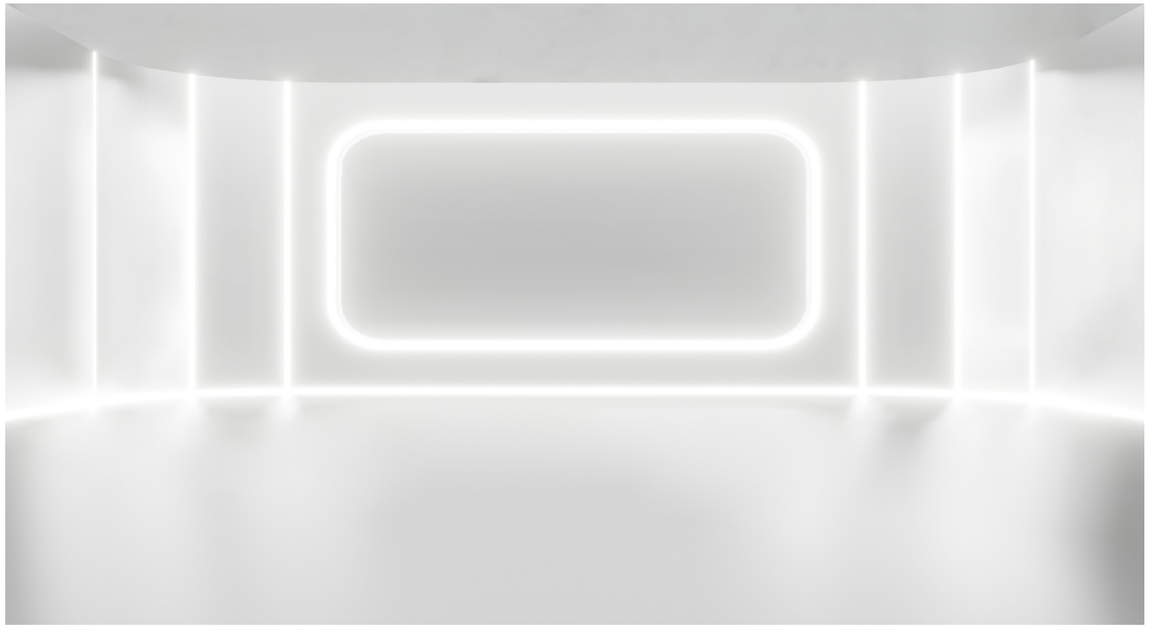
C. Çerezler

KVKK'de çerezlere yönelik özel bir düzenleme bulunmamakla birlikte; çerezler vasıtasıyla işlenmekte olan veriler gerçek bir kişiyi tanımlamaya imkân veriyorsa çerezler kişisel veri olarak kabul edilecektir.

Çerezlere ve çerezlerin onay süreçlerine yönelik AB'nin e-Privacy Direktifi'ne benzer bir düzenlemenin getirilmesi beklenmektedir.

D. Veri Lokalizasyonu

Türk Hukuku'nda bankacılık, ödeme sistemleri, sermaye piyasaları ve telekomünikasyon dahil olmak üzere çeşitli sektörlere özgü düzenlemeler ile veri lokalizasyonu zorunluluğu getirilmiş ve piyasa aktörlerinin verilerini Türkiye'de tutması zaruri kılınmıştır. Veri lokalizasyonuna yönelik yükümlülüklerin yakın zamanda daha detaylı şekilde düzenlenmesi beklenmektedir.



Kısaltmalar

11. Kalkınma Planı	T.C. Cumhurbaşkanlığı 11. Kalkınma Planı (2019-2023)
108 Sayılı Sözleşme	Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
AB	Avrupa Birliği
Aydınlatma Tebliği	Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
Başvuru Tebliği	Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
BŞK	Bağlayıcı Şirket Kuralları
GDPR	Genel Veri Koruma Tüzüğü
KEP	Kayıtlı Elektronik Posta
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
Sağlık Verileri Yönetmeliği	Kişisel Sağlık Verileri Hakkında Yönetmelik
TBK	6098 sayılı Türk Borçlar Kanunu
TBMM	Türkiye Büyük Millet Meclisi
TCK	5237 sayılı Türk Ceza Kanunu
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi

MOROĞLU ARSEVEN

MOROĞLU ARSEVEN

Yazarlar

BURCU TUZCU ERSİN, LL.M.
Ortak Avukat
btuzcu@morogluarseven.com
D: +90 (212) 377 47 50
T: +90 (212) 377 47 00

BURCU GÜRAY
Avukat
bguray@morogluarseven.com
D: +90 (212) 377 47 25
T: +90 (212) 377 47 00

CEYLAN NECİPOĞLU, PH.D, LL.M.
Avukat
cnecipoglu@morogluarseven.com
D: +90 (212) 377 47 35
T: +90 (212) 377 47 00

MOROĞLU ARSEVEN

www.morogluarseven.com

Abdi İpekçi Caddesi 19-1
Nişantaşı, İstanbul, 34367

T: +90 212 377 4700
F: +90 212 377 4799
info@morogluarseven.com