

KİŞİSEL VERİLERİ KORUMA KURULU'NUN 20.4.2018 TARİHİNDE YAYINLAMIS OLDUĞU KARAR ÖZETLERİNE İLİŞKİN DEĞERLENDİRME

Doç. Dr. Murat Volkan Dülger*

Kişisel verilerin korunması alanına ilişkin olarak en çok merak edilen konulardan birini şüphesiz Kişisel Verileri Koruma Kurulu'nun vereceği kararlar teşkil etmekteydi. Kurulun karar verirken hangi hususlara dikkat edeceği ve önem vereceği, kararların hangi konular üzerinde yoğunlaşacağı, somut olay açısından ihlal değerlendirmesinin neye göre yapılacağı ve kararların yayınlanıp yayınlamayacağına ilişkin birçok soru işareti, uygulamanın yeni olması nedeniyle doğal olarak akılları karıştırmaktaydı.

Nihayet akıllara gelen bu tür soruları belli bir ölçüde cevaplandıracak nitelikte bir gelişme gerçekleşmiş ve Kurulun vermiş olduğu bazı kararların özetleri Kurul tarafından yayınlanmıştır. Kişisel verilere ilişkin farklı farklı ihlal kararlarının yayınlanmış olması özellikle konunun ilgilileri ve Kanun'un getirdiği yükümlülüklerle uyumlu hale gelmek zorunda olan veri sorumlusu ve veri işleyenleri açısından yol göstericidir.

Kurulun yayınlamış olduğu kararları; 6698 sayılı Kanun ile getirilen ve kararlara konu olan yükümlülük açısından ele alıp; somut olayda hangi noktalarda ve hangi nedenle ihlal kanaatine ulaşıldığına değineceğim. Böylece Kurulun konuya olan bakış açısının anlaşılabilir olarak Kanun'un verilen kararlar kapsamında ele alınmasını ve değerlendirilmesini sağlamaya çalışacağım.

Kişisel Verileri Koruma Kurulu Kararları

1. Kişisel veri güvenliği ihlalinin geç bildirimi

Veri sorumlusunun kişisel verilerin güvenliğini sağlamak ile ilgili görev ve yetkileri Kanun'un "veri güvenliğine ilişkin yükümlülükler" başlıklı 12. maddesinde düzenlenmiştir¹. Buna göre;

- Veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere erişilmesini önlemek ile verilerin muhafazasını sağlamak amacıyla gerekli her türlü teknik ve idari tedbiri almak zorundadır.
- Veri işleyen olması halinde bu tedbirlerin alınmasından veri sorumlusu ve veri işleyen müştereken sorumludur.
- Veri sorumlusu, Kanun'un uygulanmasını sağlamak üzere gerekli denetimi yapmak ve yaptırmak zorundadır.
- Veri sorumluları ve veri işleyenler görevden ayrıldıktan sonrası için de geçerli olmak üzere görevleri sırasında öğrendikleri kişisel verileri hukuka aykırı bir biçimde açıklayamaz ve kullanamazlar.
- İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirmelidir.

* Akademisyen/Avukat.

¹ Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) için bakınız: <https://kvkk.gov.tr/SharedFolder/Server/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf>.

Veri sorumlusunun veri güvenliğini sağlamak üzere yerine getirmesi gereken yükümlülüklerinden; işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirme gerekliliği dikkat çekicidir. Zira madde metninde geçen “*en kısa süre*” ibaresi belli bir süre zarfını ifade etmediğinden bu kavramdan ne anlaşılması gerektiği tam olarak anlaşılamamaktadır. Bununla beraber yasal düzenleme yapılırken kanun koyucu tarafından her somut olaya ilişkin en kısa sürenin öngörülmesi mümkün değildir. Nitekim öyle haller vardır ki, kanun ile belirlenen yükümlülüğü yerine getirebilmek için içerisinde bulunan şartlar dolayısıyla gereken süre birbirinden farklılık arz edebilmektedir. Bu tür belirsiz haller ve kavramların varlığı halinde yapılması gereken Kanunun uygulanmasını sağlamak üzere görevli kurum ve kuruluşlarca verilecek kararlarla belirsiz olan kavramı açıklığa kavuşturmaya çalışmaktır.

Konuyla ilgili Kurulun önüne gelen somut olayda gerçekleşen veri ihlali, veri sorumlusu tarafından ilgili kişilere 17 ay, Kurula ise 10 aylık süre sonra bildirilmiştir. Kurul, bu sürelerin Kanunda belirtilen en kısa süreyi aşan nitelikte olduğuna ve dolayısıyla veri güvenliği ihlalinin gerçekleştiğine kanaat getirmiştir. Bu kapsamda ilgili veri sorumlusu hakkında Kanun’un 18. maddesinin 1-b bendinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında verilecek idari yaptırım cezası gereğince yaptırım uygulanmasına karar verilmiştir.

Veri sorumlusunun işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kurula bildirme yükümlülüğünü yerine getirebilmesi için bu sürenin belirlenmesi önemli olup; bu süreden tam olarak ne anlaşılması gerektiği veri sorumluları tarafından merak konusuydu. Böylelikle kişiler açısından 17 ayın, Kurula bildirim açısından ise 10 ayın uzun bir süre olduğunu anlamış bulunmaktayız. Konuyla ilgili verilmiş olan karar bu açıdan belirleyici ve yardımcı niteliktedir.

Ancak kararın hangi sektöre ait olduğunun açıklanmaması bu sürenin değerlendirilebilmesi açısından önemli bir eksiklik olduğu gibi, sektör açıklansa dahi bunun için Kurul tarafından en az sürenin ne olduğunun bildirilmemesi de önemli bir eksiklik olarak kalacak ve kafalardaki soru işaretleri giderilmemiş olarak kalacaktır. Dolayısıyla beklentim, Kurulun kararlarının tamamını yayınlaması, aleyhine karar verdiği gerçek ya da tüzel kişiyi açıklamasa dahi en azından sektörü hakkında bilgi vermesi ve mümkün olduğu kadar tavsiye niteliğinde alt süreler belirleyerek belirlilik ilkesine uygun davranması ve uygulayıcılara yol gösterici olmasıdır.

2. Açık rızanın hizmet şartına bağlanması

Açık rıza kavramı Kanun maddesi ile tanımlanmış olup; bu tanıma göre açık rızanın varlığından söz edilebilmek için şu şartların gerçekleşmesi gerekir:

- Belirli bir konuya ilişkin,
- Bilgilendirilmeye dayanan,
- Özgür iradeyle açıklanan

rıza beyanının varlığı, açık rıza anlamına gelir². Kanun'un "*kişisel verilerin işleme şartları*" başlıklı 5. maddesinin 1. fıkrası ile "*özel nitelikli kişisel verilerin işleme şartları*" başlıklı 6. maddesinin 2. fıkrasında kişisel verilerin ve özel nitelikli kişisel verilerin açık rıza olmaksızın işlenmesi yasaklanmıştır. İlgili maddelerin devamında ise açık rıza olmaksızın işlemenin istisnaları belirtilmiştir.

Bu noktada özellikle açıklamak istediğim husus açık rıza ve diğer istisna hallerinin birbirlerine karşı herhangi bir üstünlüğünün bulunup bulunmadığıdır. Kanun lafzına göre yapılacak yorumda; açık rızanın esas olup; diğer istisna hallerine karşı öncelik teşkil ettiği gibi bir anlam çıkmaktadır. Bu husus ile ilgili Kurula yönelttiğimiz sorulara karşılık, Kurul tarafından yapılan açıklamayla ise Kurulun bakış açısının Kanun lafzına göre yapılan yorumdan tamamen farklı olduğu anlaşıldı. Kurulun açıklamasına göre; ilgili kişiden açık rıza alınması hali de 95/46/EC sayılı Direktif düzenlemeleriyle paralel olarak diğer istisna halleriyle aynı düzeydedir. Dolayısıyla kişisel verilerin işlenmesi faaliyetlerinde birbirlerine karşı herhangi bir üstünlük durumu söz konusu değildir.

Altını önemle çizmek istediğim diğer bir husus ise; Kanun'un 5. maddesinin 2. fıkrası ile 6. maddesinin 3. fıkrasında sayılan kişisel verilerin ve özel nitelikli kişisel verilerin işlenmesinde istisna hallerinin varlığı halinde ilgili kişiden açık rızanın alınmasının gerekip gerekmediğidir. Alınması halinde bu açık rızanın herhangi bir geçerliliği var mıdır? Ayrıca istisna hallerinin varlığı halinde dahi açık rıza alınması durumu hukuka uygun mudur?

Konuyla ilgili Kanun'un yorumlanmasıyla ulaşılan sonuç istisna hallerinin varlığı halinde açık rıza alınmasının gereksiz olduğuydu. Ancak bu durumun hukuka aykırılık oluşturup oluşturmadığı belirsizdi. Yine Kurulun bu sorularımıza karşı yaptığı açıklamaya göre; istisna hallerinin varlığı halinde açık rızanın alınması ilgili kişiyi yanıltacak ve yanlış yönlendirecek nitelikte olduğundan; veri sorumlusu açısından Kanun ile belirtilen veri işlemeye yönelik istisna hallerinden herhangi birinin var olması halinde açık rıza alınması yalnızca gereksiz değil; yasak ve hukuka aykırıdır. Zira böyle bir durumda ilgili kişi nezdinde, açık rızasını geri aldığı takdirde veri sorumlusunun veri işleme faaliyetine son vermesi gerektiği algısı oluşmaktadır. Oysa veri sorumlusu Kanun ile kendisine getirilen yükümlülükleri yerine getirebilmek için söz konusu veri işleme faaliyetine devam etmelidir. Bu nedenle de istisna halinin varlığı halinde; veri işleme faaliyeti veri sorumlusu tarafından bu istisnaya dayandırılacak ve ilgili kişiden açık rıza alınamayacaktır.

Kurulun vermiş olduğu karara konu olan somut olayda, veri sorumlusunun kişisel veri işleme faaliyeti Kanun'un 5. maddesinin 2-c bendinde belirtilen; "*Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olma*" istisna haline dayanmaktadır. Ancak bu istisna halinin varlığına rağmen ilgili kişiden açık rıza alınmış ve bu açık rıza üyeliğin ve hizmetin, dolayısıyla sözleşmenin bir koşulu olarak dayatılmıştır. Böylece olayda iki farklı hukuka aykırılık söz konusu olmuştur:

² Açık Rıza Rehberi için bkz: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf>.

- Veri sorumlusu, tarafı olduğu sözleşme kapsamında Kanun ile kendisine getirilen yükümlülükleri yerine getirmek için kişisel veri işleme faaliyetini zaten gerçekleştirmek mecburiyetinde olmasına rağmen ilgili kişiden açık rıza almıştır.
- İlgili kişiden alınan açık rıza şarta bağlanmış ve ancak açık rıza verilmesi halinde hizmetin yerine getirileceği dayatması yapılmıştır. Oysaki Kanun tanımına göre açık rıza özgür iradeyle açıklanmalı ve dolayısıyla herhangi bir şarta bağlanmamalıdır.

Belirtilen hukuka aykırı durumlar neticesinde veri sorumlusu tarafından Kanun'un "*Genel ilkeler*" başlıklı 4. maddesinin 2-a bendi; "*hukuka ve dürüstlük kurallarına uygun olma*" ile aynı maddenin 2-ç bendi olan "*işlenme amacı ile bağlı, sınırlı ve ölçülü olma*" ilkelerine aykırılık gerçekleştirilmiştir. Dolayısıyla veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri yerine getirmediğine kanaat getirilmiş ve Kanun'un 18. maddesinin 1-b bendi gereğince idari yaptırım uygulanmasına karar verilmiştir.

Bu durum bize açık bir şekilde, Kanunun 5/2. maddesinde belirtilen kişisel veri işleme nedenlerinden birisinin bulunması halinde, açık rıza alınmaması gerektiğini göstermektedir. Böylelikle "rıza kirliliğinin" önüne geçilmek istenmektedir ve "ne olur, ne olmaz, ben alayım da bulunsun" mantığıyla hareket edilmesinin hukuka aykırı olduğu, ihlale neden olacağı ve yaptırımla karşılanacağı açık bir biçimde ifade edilmektedir.

3. İşlenme amacının gerektirdiğinden fazla kişisel veri işlenmesi/aktarılması³ (Veri minimizasyonu ilkesine aykırılık)

Kanun'un kişisel verilerin işlenmesi sırasında uyulması gereken usul ve esasların belirtildiği "*Genel ilkeler*" başlıklı 4. maddesinin 1-ç bendine göre; kişisel veriler ancak işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenebilir. Bu ilke, Kanun gerekçesinde de açıklandığı üzere işlenen verilerin, belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir. Böylece kişisel veriler üzerinde gerçekleştirilecek her türlü işleme ve aktarma faaliyetleri yalnızca gereği kadar kişisel veri faaliyeti üzerinde gerçekleştirilmelidir.

Kurulun karar vermiş olduğu olayda; mahkeme tarafından veri sorumlusundan ilgili kişi hakkında bazı kişisel veriler talep edilmiştir. Veri sorumlusu mahkemenin bu talebini Kanunun "*kişisel verilerin aktarılması*" başlıklı 8. maddesinin 2. fıkrasında atıfta bulunulan Kanunun 5. maddesinin 2-ç bendinde yer verilen "*Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması*" gereğince yerine getirmek durumundadır. Ancak veri sorumlusu hukuka uygun olarak gerçekleştireceği kişisel verileri aktarma faaliyetini mahkeme tarafından talep edilen kişisel verilerle sınırlı olarak yerine getirmeli ve istenilen kişisel verilerden fazlasını aktarmamalıdır. Ancak olayda veri sorumlusunun mahkemenin istediğinden dolayısıyla gereğinden fazla kişisel veri aktardığı anlaşılmıştır. Böylece kişisel verilerin işlenmesinde uyulması gereken genel ilkelere aykırılık meydana gelmiştir. Sonuç olarak veri sorumlusu hakkında veri güvenliğine ilişkin yükümlülükleri yerine getirmeme

³ Kişisel Verilerin İşlenme Şartları Rehberi için bkz: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/8c90423f-97ea-4d81-a7c1-ace74295c2b8.pdf>

gereğince yine Kanun'un 18. maddesinin 1-b bendi gereğince idari yaptırım cezasının uygulanmasına karar verilmiştir.

Bu durum uygulamada, çeşitli uyuşmazlıkların soruşturma ve kovuşturmalarında (yargılamalarında) sıklıkla karşılaştım ve eleştirdiğim bir hukuka aykırılık halidir. Özel hukuk yargılamasında taraflar, ceza muhakemesinde ise özellikle soruşturma makamının yardımcısı olan kolluk ya da katılan taraf, mahkeme gözünde diğer tarafı ya da sanığı bir şekilde küçük düşürmek, durumunu daha iyi ispat edebilmek ya da muhakemeyi fiil değil, fail yargılamasına çevirebilmek için bu yola başvurmaktadırlar. Kurul vermiş olduğu bu kararlar, sessiz bir biçimde aslında çok büyük bir değişikliğe adım atmıştır. Bu bir zihniyet değişikliğidir ve herkesin bunu benimsemesi ve buna uyması gerekir. Böylece hem gereksiz ve hukuka aykırı biçimde birçok kişisel verinin kamuya yayılması önlenerek hem de mahkemeler önünde, uyuşmazlık konusu ile ilgili olmayan konuların tartışılmasının önüne geçilecek ve son olarak usul ekonomisine de katkı sağlayacaktır. Dolayısıyla bu karar, neresinden bakılırsa bakılsın son derece olumlu ve faydalıdır.

4. Veri sorumlusu tarafından Kanunda belirlenen süre içerisinde ilgili kişiye cevap verilmemesi

İlgili kişi, Kanunun uygulanmasıyla ilgili olarak Kanun'un "veri sorumlusuna başvuru" başlıklı 13. maddesi gereğince veri sorumlusuna başvurma hakkına sahiptir. Bu başvuruyu Kanun'un "ilgili kişinin hakları" başlıklı 11. maddesinde sayılan hakları çerçevesinde yapılacaktır. Maddeyle ilgili kişinin kişisel verisi üzerinde her türlü iş ve eylemi öğrenme, talep etme ve verisi hakkında bilgi edinme hakkı düzenlenmiştir.

Veri sorumlusu ilgili kişinin başvurusunda yer alan talepleri, Kanun'un 13. maddesi gereğince; talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmalıdır. Ayrıca Kanun'un 15. maddesinin 5. fıkrası gereğince; Kurulun şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlal kanaatine varması hâlinde; Kurul tarafından, tespit edilen hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar verilerek ilgililere tebliğ edilir.

Kurul tarafından verilen kararda veri sorumlusu tarafından, Kanunun 15. maddesinin 5. fıkrası gereğince tebliğ edilen kararın tebliğinden itibaren ilgili kişiye 30 gün içinde cevap verilmesi gerektiği, aksi takdirde Kanunun 18. maddesi uyarınca hakkında idari yaptırım uygulanacağı hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

Bu karar, veri sahibine cevap verilmesi gerektiğini, verilmemesine ilişkin şikâyet olması halinde şartları gerçekleşmişse bunun ihlal olarak nitelendirileceğini; bu şikâyetlerin dikkate alındığı ve veri sorumluları tarafından kanun ve yönetmelikte bulunan yükümlülüklerle uyulması konusunda Kurum'un hassas davrandığını bizlere göstermesi açısından son derece önemlidir.

5. İlgili kişinin kişisel verilerinin silinmesi talebinin yerine getirilmemesi⁴

Kurulun bu kararına konu olay açısından ilgili madde, Kanun'un kişisel verilerin işlenmesinde uyulacak usul ve esasların sayıldığı 4. maddesinin 2-d bendidir. Buna göre kişisel verilerin işlenmesinde; “İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” ilkesi söz konusudur. Bu ilke kişisel verilerin işlenmesinde oldukça önemli olup; esasen yerine getirmede en çok zorlanılan konulardan birini oluşturmaktadır. Ülkemizde ne yazık ki kişisel verilerin korunmasının öneminin henüz yeterince farkına varılmamış olması nedeniyle işleme faaliyetlerinin gerçekleştirildiği kişisel verilere artık ihtiyaç duyulmasa bile veri sorumluları tarafından söz konusu verilerin silinmesinden imtina edilmektedir. Böylece “veri çöplüğü” dediğimiz kavram meydana gelmektedir. Ancak Kanun ve ilgili diğer yasal düzenlemeler ile beraber bu alışkanlıklardan vazgeçilmeli ve kişisel verilerin işlendikleri amaç için gerekli olan süre kadar saklanması gerektiği bilinci yerleşmelidir.

Veri sorumlusu tarafından hukuka uygun bir biçimde işlenen kişisel veriler, ilgili mevzuatta öngörülen; yoksa işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Bu sürenin geçmesi halinde “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik”in 7. maddesi gereğince; işlenen kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir⁵.

İşlenen kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi hususuyla ilgili olarak özellikle Kanun'a uyumluluk süreçleri noktasında da dikkat edilmelidir. Nitekim yukarıda anılan Yönetmeliğin kişisel veri envanteri tanımına göre; kişisel verilerin işlendikleri amaçlar için gerekli olan azami süre kişisel veri envanterinde yer almalıdır.

Kurulun kararına konu olan olayda veri sorumlusunun tabi olduğu mevzuat uyarınca işlediği kişisel verileri 10 yıl boyunca muhafaza etmesi zorunluluğu bulunmaktadır. Bu nedenle, Kurul tarafından aktif olmayan müşterilerin kişisel verilerinin, Kanunun 4. maddesinde yer verilen genel ilkelere uygun olarak saklama amacı dışında işlenmemesi gerektiği yönünde veri sorumlusunun talimatlandırılmasına karar verilmiştir.

Dolayısıyla veri sorumlusunun geçerli bir hukuki nedeni ve veri işlemek için nedeni bulunsa dahi bunu veriyi işlemek için veri envanterinde gösterdiği işleme gerekçesi yani haklı neden doğrultusunda gerçekleştirmelidir. Diğer hususlar bulunsa dahi, haklı bir nedenin bulunmaması ve buna rağmen veriyi işlemesi halinde Kanun ihlal edilmiş olacaktır.

6. Kişisel veri güvenliğinin sağlanması amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli idari ve teknik tedbirlerin alınmaması

⁴ İlgili kişinin hak arama yöntemleri rehberi için bkz: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/7226b55d-b1e7-4e78-a3c4-0b1ba82ce542.pdf>.

⁵ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi için bkz: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf>.

Veri sorumlusunun veri güvenliğine ilişkin yükümlölükleri yukarıda Kurulun birinci kararını deęerlendirdiđim kısımda detaylı olarak açıkladıđım üzere Kanun'un 12. maddesinde düzenlenmiştir. Buna göre; veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere erişilmesini önlemek ile verilerin muhafazasını sağlamak amacıyla gerekli her türlü teknik ve idari tedbiri almak zorundadır.

Karara konu olan olayda;

- Veri sorumlusu tarafından aynı zamanda müşterisi olan ilgili kişinin kişisel verilerinin yer aldığı bir belgenin, aynı isme sahip başka bir kişiye gönderilmesi,
- Veri sorumlusunun bir çalışanın, talebi olmamasına rağmen aynı zamanda müşterisi olan ilgili kişinin kişisel verilerini, kendisine yetki tanımlaması yapılan sistemler aracılığıyla kişisel amaçları için sorgulaması

söz konusu olmuştur.

Müşterinin kişisel verilerinin yer aldığı belgenin aynı isimdeki başka bir kişiye gönderilmesi Kurul tarafından, veri sorumlusu açısından sistemselsel bir açığa işaret olarak deęerlendirilmiştir. Böylece veri sorumlusunun veri güvenliğinin sağlanması hususunda gerekli teknik ve idari tedbirleri almadığı sonucuna ulaşılmıştır.

Veri sorumlusunun çalışanı tarafından, müşterinin kişisel verilerinin kendi kişisel amaçları için sorgulanması esasen sıklıkla karşılaşılan bir kişisel verilerin korunması ihlali durumudur. Örneğin veri sorumlusu olan şirketlerin çalışanları veri işleyen konumundadır ve mesleki faaliyetlerinden kaynaklanan yükümlölükleri yerine getirebilmek için kendilerine yetki tanımlaması yapılan sistemler mevcuttur. Ancak veri işleyen konumundaki çalışanlar, bu sistemleri sadece bulundukları pozisyon nedeniyle yerine getirmekle yükümlü oldukları faaliyetler kapsamında kullanılmalıdır. Oysaki günümüzde sıklıkla bu durum ihlal edilmekte ve kişilerin verilerine ulaşabilen kişiler tarafından kendi kişisel çıkarları doğrultusunda bu verilere ulaşım sağlanmaktadır. Esasen bu durum kişilerin kişisel verilerin korunmasına olan bakış açısıyla ilgili olup; konuyla ilgili bir kültürün oluşması meselesidir. Veri işleyenlerle beraber müşterek sorumlu konumunda bulunan veri sorumluları bu konuyla ilgili oldukça dikkatli olmalıdır. Zira her ne kadar konuya ilişkin gerekli idari ve teknik tedbirlerin alınmasını sağlamış olsa da; bu tedbirler kapsamında ayrıca çalışan konumundaki veri işleyen kişilerde de kişisel verilerin korunması alanında verilecek eğitimlerle gerekli bilincin oluşmasını sağlamalıdır. Aksi takdirde veri işleyenin yanında veri sorumlusunun kendisi de sorumlu tutulacaktır.

Kararda da veri işleyen çalışanın kendisine tanımlaması yapılan sistemler aracılığıyla kendi kişisel çıkarları doğrultusunda müşterinin kişisel verilerini sorgulaması sonucunda veri sorumlusunun veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirlerin alınmadığı sonucuna ulaşılmıştır. Her iki hukuka aykırı fiil için de Kanunun 18. maddesi uyarınca idari işlem tesis edilmesine karar verilmiştir.

7. Kanunda yer alan genel ilkelere aykırı şekilde kişisel verilerin işlenmesi

Kişisel veriler üzerinde gerçekleştirilecek her türlü işleme faaliyeti esnasında Kanun'un 4. maddesinde sayılan genel ilkelere uyulmalıdır⁶. Bu ilkelere aykırı bir biçimde kişisel verilerin işlenmesi halinde hukuka aykırılık söz konusu olacaktır.

Kurulun incelemesine konu olan olayda; veri sorumlusu tarafından ilgili kişinin talebi üzerine gerçekleştirilen işlemde; veri sorumlusu tarafından müşteriden işlemin gerektirmediği kişisel veri içeren bir belge istenilmiştir. Ancak bu belgenin istenilmesi herhangi bir mevzuat hükmüne dayanmadığı gibi ulaşılmak istenen amaç ile de bağdaşmamaktadır. Bu sebeplerle de veri sorumlusu tarafından gerçekleştirilen belge istemi fiilinin; Kanunun 4. maddesinin 2-a bendinde yer verilen; “*hukuka ve dürüstlük kurallarına uygun olma*” ilkesi ile 2-c bendinde yer verilen; “*belirli, açık ve meşru amaçlar için işlenme*” ilkesine aykırılık teşkil ettiğine kanaat getirilmiştir. Bu kanaatin sonucunda kişisel veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18. maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

Uygulamada sıklıkla gördüğümüz, basit bir işlem için bile gereksiz çok sayıda ve özel nitelikte kişisel verinin istenmesi eylemlerinden birisi bu kararının konusunu oluşturmuştur. Bu karardan sonra veri sorumlularının, iş süreçlerini gözden geçirmeleri ve kişisel veri koruma ve işleme politikalarında gerekli düzeltme ve değişiklikleri yapmaları, eğer bu politikaları yoksa da bir an önce oluşturmaları gerekir.

8. Kanuna aykırı şekilde kişisel verilerin paylaşılması

Kişisel verilerin işlenmesi kapsamında gerçekleştirilen paylaşım ve aktarım faaliyetleri Kanun'un işleme şartlarının belirtildiği ilgili Kanun hükümlerine dayanmalıdır. Veri sorumlusunun bu şartlara dayanmaksızın kişisel verileri üçüncü kişilerle paylaşması halinde hukuka aykırılık meydana gelecektir.

Kurul kararına konu olan olayda veri sorumlusu tarafından bir şirketin çalışanlarına e-posta yoluyla sözleşme örnekleri gönderilmiştir. Sözleşmelerde yer alan işveren e-posta adresi kısmına şirketin adresinin yazılması gerekirken veri sorumlusu tarafından herhangi bir işleme şartına dayanmaksızın şirket adına sürecin yönetiminden sorumlu kişi olan ilgili kişinin ev adresi yazılmıştır. Veri sorumlusunun şirket adına sürecin yönetiminden sorumlu ilgili kişinin kişisel verisinin herhangi bir gerekçe olmadan üçüncü kişilerle paylaşılması Kanunun 12. maddesi kapsamında veri güvenliğini sağlayamayan veri sorumlusu hakkında Kanunun 18. maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

Bu karar, Kurulun taksirle gerçekleştirilen eylemlerde dahi hassas olduğunu göstermesi bakımından önemlidir. Şirketin kendi çalışanı dahi olsa, açık adresinin hatalı bir şekilde paylaşılması, veri sorumlusunun yükümlülüklerinin ihlali anlamına gelir. Tabi bu kararda

⁶ Kişisel verilerin işlenmesine ilişkin temel ilkeler rehberi için bkz: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/d0fbca08-30af-41fe-a7c9-65663b9c5231.pdf>.

göremediğimiz husus, şirket çalışanın bu başvurusunun işçi – işveren ilişkisini nasıl etkilediğidir.

Sonuç

Kişisel Verileri Koruma Kurulu’nun kendisine yapılan şikayetleri değerlendirerek; incelemesi sonucunda yayınladığı kararların değerlendirilmesi sonucu dikkat edilmesi gerektiğini düşündüğüm hususlar aşağıdaki gibidir:

- İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde veri sorumlusu tarafından en kısa sürede ilgisine ve Kurula bildirim yapılmalıdır. En kısa süre somut olayın şartlarına göre belirlenmelidir. Kurul kararına konu olan olayda söz konusu olan 10 ve 17 aylık süreler bu sürelerin belirlenmesi açısından yardımcı olabilecek niteliktedir. Ancak kararın hangi sektöre ait olduğunun ve sektör açıklansa dahi söz konusu sektör için Kurul tarafından öngörülen en az sürenin ne olduğunun kararda yer almamış olmasını bir eksiklik olarak değerlendirdiğimi belirtmeliyim. Bundan sonraki yayınlanacak kararlar için beklentim, Kurulun kararlarının tamamını yayınlaması, aleyhine karar verdiği sektör hakkında bilgi vermesi ve mümkün olduğu kadar tavsiye niteliğinde alt süreler belirleyerek belirlilik ilkesine uygun davranması ve uygulayıcılara yol gösterici olmasıdır.
- Kişisel verilerin işlenmesi için ilgili kişiden açık rızanın alınması gerektiği durumlarda veri sorumlusunun bu açık rızayı şarta bağlaması mümkün değildir. Ayrıca Kanun’un 5/2. maddesiyle belirtilen istisna hallerinin varlığı halinde açık rızanın alınması ilgili kişiyi yanıltacak nitelik taşıdığından; bu hallerde açık rızanın alınması hukuka aykırıdır. Böylelikle “rıza kirliliğinin” önüne geçilmek istenmektedir ve istisna hallerinin varlığına rağmen “ne olur, ne olmaz, ben alayım da bulunsun” mantığıyla hareket edilmesinin hukuka aykırı olduğu, ihlale neden olacağı ve yaptırımla karşılanacağı açık bir biçimde ifade edilmektedir.
- Kişisel verilerin ancak işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenmesi ilkesi gereğince işlenen veriler, belirlenen amaçların gerçekleştirilebilmesine elverişli olmalı ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmalıdır. Uygulamada, çeşitli uyuşmazlıkların soruşturma ve kovuşturmalarda (yargılamalarında) sıklıkla karşılaştığım bu durum karşısında Kurulun vermiş olduğu karar, esasen çok büyük bir değişikliğe gitmek üzere atılan ilk adım olmuştur. Her açıdan son derece faydalı olacağını düşündüğüm bu kararla hem gereksiz ve hukuka aykırı biçimde birçok kişisel verinin kamuya yayılması önlenecek hem de mahkemeler önünde, uyuşmazlık konusu ile ilgili olmayan konuların tartışılmasının önüne geçilecek ve son olarak usul ekonomisine de katkı sağlanacaktır.
- Veri sorumlusu, ilgili kişiye Kanunun 11. maddesi kapsamında talep ettiği hususlarla ilgili olarak, Kanunun 15. maddesinin 5. fıkrası gereğince Kurul kararının tebliğinden itibaren 30 gün içerisinde cevap vermelidir. Bu karar, veri sahibine cevap verilmesi gerektiğini, verilmemesine ilişkin şikâyet olması halinde şartları gerçekleşmişse bunun ihlal olarak nitelendirileceğini; bu şikayetlerin dikkate alındığı ve veri sorumluları tarafından kanun ve yönetmelikte bulunan yükümlülüklerle uyulması konusunda Kurum’un hassas davrandığını bizlere göstermesi açısından son derece önemlidir.

- Veri sorumlusu, halihazırda aktif olmayan müşterisinin kişisel verilerinin silinmesi hususundaki talebini tabi olduğu mevzuat uyarınca muhafaza etmesi zorunluluğunun bulunduğu gerekçesiyle yerine getirmemesi halinde; kişisel veriler silinmese de söz konusu kişisel veriler genel ilkelere uygun olarak saklama amacı dışında işlenmemelidir. Dolayısıyla veri sorumlusunun geçerli bir hukuki nedeni ve veri işlemek için nedeni bulursa dahi bunu veriyi işlemek için veri envanterinde gösterdiği işleme gerekçesi yani haklı neden doğrultusunda gerçekleştirmelidir. Diğer hususlar bulursa dahi, haklı bir nedenin bulunmaması ve buna rağmen veriyi işlemesi halinde Kanun ihlal edilmiş olacaktır.
- Veri sorumlusunun kişisel verilerin yer aldığı bir belgeyi, bir hata sonucu başka bir kişiye göndermesi ve bir çalışanı tarafından kendisine yetki tanımlaması yapılan sistemler aracılığıyla kendi kişisel çıkarları doğrultusunda ilgili kişinin kişisel verilerini sorgulaması, sistemsal bir açığa işaret ettiğinden veri sorumlusunun veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı anlamına gelmektedir.
- Kişisel veriler üzerinde gerçekleştirilen her türlü işleme faaliyetinde Kanun ile belirlenen genel ilkelere uygun hareket edilmelidir. Uygulamada da sıklıkla gördüğümüz, basit bir işlem için bile gereksiz sayıda kişisel verinin istenmesi karşısında verilen bu karardan sonra veri sorumlularının, iş süreçlerini gözden geçirmeleri ve kişisel veri koruma ve işleme politikalarında gerekli düzeltme ve değişiklikleri yapmaları, eğer bu politikaları yoksa bir an önce oluşturmaları gerekir.
- Kişisel verilerin işlenmesi kapsamında gerçekleştirilen paylaşım ve aktarım faaliyetleri Kanun ile belirlenmiş olan kişisel verilerin işleme şartlarına dayanmalıdır. Bu kararın esas önemi ise, Kurulun, şirketin kendi çalışanı dahi olsa, açık adresinin hatalı bir şekilde paylaşılması suretiyle gerçekleştirilen taksirli eylemlerde dahi hassas olduğunu göstermesi noktasındadır.

Kurul tarafından kişisel verilerin korunması alanına ilişkin temel noktaları oluşturan hususlar konusunda verilen kararların yayınlanmış olmasının veri sorumluları açısından oldukça faydalı olacağını düşünüyorum.

Bu noktada altını önemle çizmek istediğim diğer bir husus; Kanun'a uyumlu hale gelmek ile yükümlü olan veri sorumlularının Kanun'un yayınlandığı 7 Nisan 2016 tarihinden sonra kaydettikleri yeni kişisel veriler için 6 ay; bu tarihten önce kaydedilen arşiv verileri dediğimiz veriler için ise 2 yıl içinde Kanun'a uyumlu hale gelmek zorunda olduğudur. Dolayısıyla şu an eski ve yeni fark etmeksizin tutulmuş veya tutulan her türlü kişisel verilerin işlenmesinde Kanun'un getirdiği yükümlülöklere uyulmalıdır. Kanun ile öngörölen süreler halihazırda geçmiş bulunmaktadır. Bu nedenle Kurul tarafından resen veya ilgili kişinin başvurusu üzerinde yapılacak incelemeler yoğunluk gösterecek ve birçok farklı noktada karar verilecektir. Ayrıca sürelerin geçmiş bulunmasına rağmen veri sorumlularının Kanuna uyumlu hale gelmemiş bulunması Kurul tarafından verilecek ihlal kararlarında artış meydana getirecektir. Bu nedenle de veri sorumlularına Kurul tarafından verilmiş söz konusu kararların da dikkate alınarak bir an önce Kanun'a uyumlu hale gelmeleri gerektiği konusunda uyarıda bulunuyor; Kanun'a uyumluluk projelerinde bulunmaları gerektiğini tavsiye ediyorum.