

KVKK Uygulamasında ve Uyum Sürecinde Ortaya Çıkan Soru ve Sorunlar

Doç. Dr. Murat Volkan Dülger*

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 24.03.2016 tarihinde Resmi Gazete’de yayımlanarak yürürlüğe girmesiyle birlikte Kişisel Verileri Koruma Hukuku günlük hayatımızın birçok noktasında karşımıza çıkmaya başladı. Ülkemizde Kişisel Verileri Koruma Hukukunun birincil kaynağı niteliğinde olan 6698 sayılı Kanun ve bunun yanı sıra yönetmelikler, tebliğler ve Kişisel Verileri Koruma Kurulu’nun kararları bulunmakla birlikte, uygulamada hala birçok sorun yaşanmakta ve çok sayıda soruya yanıt aranmaktadır. Bunlar özellikle özel sektör bakımından ticari hayatın hukuka uygun işlemesi ama bir yandan da ticaretin engellenmemesi açısından hayati önemi haizdir.

İşte bu yazıda “KVKK uygulamasında ve uyum sürecinde ortaya çıkan sorunları” ele almaya ve aslında bu işle ilgilenen hemen hemen herkesin kafasında olan soruları yüksek sesle dile getirmeye çalışacağım.

Her şeyden önce belirtmeliyim ki, 6698 sayılı Kanun, 2016 yılında yürürlüğe girmiş olup uygulama açısından henüz tam oturmamıştır. Kanun’un eleştirildiği ve uygulama açısından yetersiz kaldığı birçok husus bulunmaktadır. Bu hususların bir kısmı Kurul kararlarıyla netleştirilmiş olsa da uygulama açısından halen giderilmesi gereken birçok eksiklik bulunmaktadır. Aşağıda tespit ettiğim sorunlara ana başlıklar çerçevesinde değinecek ve bazılarını getirilebildiğim çözüm önerilerini açıklayacağım. Ancak bunlar kesin çözümler olmayıp, bu konudaki tartışmaların başlaması için birer öneri niteliğindedir.

1. VERBİS Sicil Yönetmeliği Kapsamında Uygulamadaki Soru ve Sorunlar

VERBİS Sicil Yönetmeliği’nin 13. maddesinde “*Veri sorumluları, sicilde kayıtlı bilgilerde değişiklik olması halinde meydana gelen değişiklikleri, VERBİS üzerinden yedi gün içerisinde Kurum’a bildirir.*” düzenlemesi yer almaktadır. Buna göre veri sorumlusu sıfatını haiz kişilere veya kurumlara kayıtlarda değişiklik olması halinde söz konusu değişikliği 7 gün içerisinde Kurum’a bildirme yükümlülüğü getirilmiştir. Ancak buradaki 7 günlük sürenin hangi andan itibaren başlayacağı belirsizdir.

VERBİS Sicil Yönetmeliği’nde düzenlenen 7 günlük sürenin, değişiklik olduğunun öğrenilmesinden itibaren mi yoksa değişikliğin oluştuğu andan itibaren mi işlemeye başlayacağı söz konusu düzenlemede belirtilmemiştir. Uygulamada gördüğüm örnekler göre kişisel verilerdeki olası değişikliklerin her zaman hemen ve kolayca tespit edilmesi mümkün değildir. Değişikliğin tespit edilmesi halinde ise 7 günlük sürenin değişikliğin meydana geldiği anda başlatılması halinde ise Kurul’a bildirim için 7 günlük sürenin kısa olduğunu

* Yeditepe Üniversitesi Hukuk Fakültesi, Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku öğretim üyesi / Avukat.

düşünmekteyim. Bu nedenle kişisel verilerin veri sorumlusu tarafından organizasyonel bir yapı içerisinde düzenli aralıklarla güncelliğinin, doğruluğunun kontrol edilmesi ve 7 günlük sürenin de bu kontroller sonucunda kişisel verideki değişikliğin tespit edilmesinden itibaren başlaması gerektiğini düşünmekteyim.

Bu husustaki değerlendirme, GDPR’da verilerin doğruluk ve güncelliğinin tespiti açısından yapılan değerlendirmeye kıyas yapılarak geliştirebilir. GDPR, “*Kişisel Verilerin Doğru ve Gerektiğinde Güncel Tutulma İlkesine*” yer verdiği 5/1-d maddesinde, güncel olmayan verileri işlediğini anlayan veri sorumlusunun ne yapması gerektiği hususunu da açıklamıştır. Buna göre, veri sorumlusu aslında güncel olmayan hatalı verileri işlediğini herhangi şekilde anlarsa bu gibi verilerin, işleneceği amaçlarla ilgili olarak bir gecikmeye mahal vermeksizin silinmesini veya düzeltilmesini sağlamak için gerekli her türlü makul adımı atmalıdır¹.

GDPR’da bu kapsamda yapılan yorumu VERBİS Sicil Yönetmeliği ile getirilen 7 günlük sürenin başlangıç aşaması açısından da kıyas yoluyla değerlendirebiliriz. Buna göre veri sorumlusunun 7 günlük süre zarfında değişikliği Kurul’a bildirmesi; bir gecikmeye mahal vermeksizin silinmesini veya düzeltilmesini sağlamak için gerekli bir adım olarak değerlendirilip, 7 günlük sürenin başlangıcı olarak da veri sorumlusunun üzerinde değişiklik meydana gelen verileri işlediğini herhangi şekilde öğrenme anını esas alabiliriz.

Bununla birlikte veri sorumlusunun olumsuz sonuçlarla karşılaşmaması ve ilgili kişinin hak ihlali iddialarına maruz kalmaması için veri sorumlusunun organizasyonel bir yapıda verileri kontrol etmesi gerektiğini tekrar belirtmeliyim. Bu kapsamda yeni veri işleme süreçlerinin ortaya çıkması halinde nasıl hareket edileceğine, kimin hangi sürede nasıl bildirimde bulunacağına dair politikalar ve prosedürler oluşturulmalı, bu konuda görevlendirmeler yapılmalı ve bir ihlal durumunun olmaması için bu yapılanlar doğrultusunda ilgili kişilerin işlemde bulunması sağlanmalıdır.

2. Açık Rıza Alınırken Rıza Karşılığı Ek Avantajlar Sağlanabilir mi?

GDPR, Direktif ve 6698 sayılı Kanun’da açıkça belirtildiği üzere açık rıza beyanı ilgili kişinin özgür iradesinin ürünü olmalıdır. Özgür iradeyle açıklanmış olan bir beyan, kişinin kendi kararını özgürce verebilmesi ve bunu dışarıya özgür bir şekilde açıklayabilmesi anlamına gelir. Veri sorumlusunun “*açık rıza verilmesi halinde hizmetin yerine getirileceği dayatması*” yapması açık rızanın özgür iradeyle açıklanmış olma özelliğini zedelediği için bu şekilde alınan rızaların hukuka uygun olmadığı kabul edilmektedir. Ancak tam tersi yönde, söz konusu işlemin yerine getirilmesi hususunda bir dayatma olarak değil de kişinin açık rıza vermesiyle kendisine artı bir menfaat kazandırılacağı yönünde bir uygulamayla alınan açık rızanın geçerli olup olmadığı tartışmalıdır.

Kanaatimce rıza karşılığı ek avantaj getirilmesi kişinin özgür iradesini zedelemeyiz. İşlemin gerçekleştirilmesi hususunda dayatmada bulunulması kişinin açık rıza vermezse yapmak istediği işin yapılmayacağını, söz konusu işlemin yapılması için kişisel verilerinin işlenmesine açık rıza vermesini zorunlu kılar niteliktedir. Bu nedenle kişinin özgür iradesinin ortadan

¹ **Murat Volkan Dülger**, Kişisel Verilerin Korunması Hukuku, İstanbul, Hukuk Akademisi, 2018, s. 132.

kalkması sonucu doğmaktadır. Ancak ek avantaj getirilmesi söz konusu işlemi etkilememekte sadece kişinin rızasını almak üzere teşvik edilmesini sağlamaktadır. Veri sorumlusunun yerine getirdiği faaliyet çerçevesinde veri ilgisini zorlamaya varmayacak derecede etkilemeye çalışması gibi durumların özgür iradeyi sakatlayan durumlar olarak algılanmaması gerektiğini düşünüyorum. Zira böyle bir kabulde özgür iradeyle açıklanmış olma kavramı çok geniş yorumlanmış ve ticaret faaliyetler de kötü etkilenmiş olacaktır. Üstelik yalnızca ticari faaliyet yürüten veri sorumlusu için değil bundan faydalanacak olan veri ilgisi üzerinde de olumsuz etkilerinin olması mümkündür².

Bu soru en çok sadakat kart (loyalty card) özelinde gündeme gelmektedir. Ticaret şirketleri, müşterilerini kendilerine çekebilmek ve bağlı kalmalarını sağlamak için müşterilerinin bazı kişisel verilerini almakta ve bunun karşılığında müşterilerine indirim yaparak ya da çeşitli hediyeler vererek avantajlar sağlamaktadır. İşte tam da bu noktada yukarıda ifade etmiş olduğum görüş devreye girmektedir. Sadakat kartı çıkaran şirket, kişisel verilerini vermek ve kartı almak istemeyen müşterilerine ürün ya da hizmet satmaktan kaçınmamakta, yalnızca bunlara avantaj sağlamamaktadır. Dolayısıyla aslında burada iradenin etkilenmesi değil, karşılıklı bir sözleşme söz konusudur ve bu sözleşmenin ifası gereği karşılıklı edimler yerine getirilmektedir. Bence burada dikkat edilmesi gereken husus, müşteriye dilediği zaman bu sözleşmeyi kolayca sona erdirmeye hakkının verilmesi ve bu irade beyanı gerçekleştiğinde veri sorumlusunun müşterinin bu kapsamda alınan kişisel verilerini gerçekten silmesidir.

3. 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ve 6698 sayılı Kişisel Verilerin Korunması Kanun’u Arasındaki Eksikler ve Çelişkiler

2015 yılında yürürlüğe giren 6563 sayılı Elektronik Ticaret Kanunu ile 6698 sayılı Kanun arasında Kişisel Verilerin Korunması Hukuku açısından birtakım çelişkiler bulunmaktadır. Bu çelişkiler başlıca şunlardır:

- 6563 sayılı Elektronik Ticaret Kanunu esas itibarıyla kişisel verilerin aktarılması ve işlenmesi hususunda zımni rızayı kabul etmektedir. Ancak 6698 sayılı Kanun ve GDPR’daki düzenlemelerde açıkça belirtildiği üzere Kişisel Verilerin Korunması Hukuku açısından zımni rıza söz konusu olamaz. Bu durumda ülkemizdeki uygulama açısından Elektronik Ticaret Kanunu kapsamında alınan kişisel veriler için zımni rızanın geçerli olup olmayacağına yönelik bir soru işareti oluşmaktadır. Bu konudaki görüşüm Elektronik Ticaret Kanunu kapsamında işlenen kişisel veriler için 6563 sayılı Elektronik Ticaret Kanunu’nun uygulanması yönündedir. Bu görüşümün iki gerekçesi bulunmaktadır.

Bunlardan ilki kanunların uygulanması bakımından temel bir kural olan genel kanun – özel kanun çatışmasında özel kanunların uygulanacağına yönelik kuraldır. Bu kurala göre; bir hususa ilişkin olarak genel kanundaki bir düzenleme ile özel kanundaki bir düzenleme çatışıyorsa genel kanun değil özel kanun uygulama alanı bulur. Bizim değerlendirmemiz açısından ise 6698 sayılı Kişisel Verilerin Korunması Kanunu genel kanun niteliğinde olup 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

² Ayrıntılı bilgi için bkz: **Dülger**, Kişisel Verilerin Korunması Hukuku, s. 25.

ise özel kanun niteliğindedir. Bu nedenle iki düzenleme arasında çatışma olması durumunda 6563 sayılı Kanun kapsamında işlenen kişisel veriler için 6563 sayılı Kanun uygulanmalıdır.

İkincisi ise, 6698 sayılı Kanunun 6. maddesinin 3. fıkrasında ve 5. maddesinin 2. fıkrasının (a) bendinde “*Kanun’da Öngörülmiş Olma*” kişisel verilerin işlenmesine ilişkin hukuka uygunluk nedenleri arasında düzenlenmiştir. Bu açıdan bakıldığında Elektronik Ticaret kapsamında işlenen kişisel veriler için 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun’da açıkça bir düzenleme bulunmaktadır. Bu nedenle bu kanun kapsamında işlenen veriler için 6698 sayılı Kanunun 6. maddesinin 3. fıkrasına ve 5. maddesinin 2. fıkrasının (a) bendine giren hallerde istisna söz konusu olup bu hallerde açık rıza alınmaması gerekir.

Ancak söz konusu yorum özel nitelikli kişisel veriler açısından, 6. maddenin 3. fıkrası dışında kalan haller için işe yaramayacak olup bu tür veriler için her durumda açık rıza alınması gerekir.

- Yukarıda 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun’da Elektronik Ortamda alınan kişisel verilerin işlenebilmesi için onay alınması gerektiğinden bahsetmiştik. Buna ek olarak söz konusu kanundaki bir başka düzenlemeyle veri sorumlusuna, kişi istenilen onaya ret cevabını vermiş olsa bile, yılda iki kere ilgili kişiye onaylayıp onaylamadığını sorma hakkı verilmiştir. 6563 sayılı Kanun’da böyle bir düzenleme getirilmiş olmasına rağmen bu konuyla ilgili 6698 sayılı Kanun’da bir sınırlama bulunmamaktadır. Bu hususla ilgili 6698 sayılı Kanun ile bir sınırlama getirilmelidir. Aksi taktirde ilgili kişilerle onay olmak amacıyla çok sık aralıklarla iletişime geçilmesi söz konusu olabilir.

Bu şekilde alınacak olan rızanın hukuka uygunluğu ise ayrı bir tartışma konusudur. İlgili kişilerden her gün telefon, e-mail vb. yollarla iletişime geçilerek rıza alınması kişinin özgür iradesinin ürünü olması gereken açık rızayı hukuka aykırı hale getirecektir. Bu nedenle bu hakkın kullanılmasına bir sınırlama getirilmelidir.

- Ayrıca 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun kapsamında yapılacak bilgilendirme ile 6698 sayılı Kanun kapsamında yapılacak aydınlatma birlikte yapılabilir mi? Bilgilendirme metni aydınlatma metnini de kapsayabilir mi yoksa ayrı ayrı mı yapılmalı gerekmektedir? Uygulamada birçok soru işareti ve tereddüde yol açan bu soruya da bir açıklama getirilmesi gerekir.

Bu kapsamda Kişisel Verilerin Korunması Kurumu tarafından 10 Mart 2018 tarihinde yayınlanan “*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*”in 5. maddesinin 1. fıkrasının “f” bendi uyarınca aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekir. Söz konusu sorun bu tebliğ kapsamında değerlendirildiğinde *Elektronik Ticaretin Düzenlenmesi Hakkında Kanun* kapsamında yapılacak bilgilendirme işleminin de ayrıca yapılması gerektiğini düşünmekteyim. Ancak bu ikisinin birlikte tek metinde yapılabilmesinin daha kolay ve işlevsel bir yöntem olduğunu da belirtmeliyim.

Kanaatimce, söz konusu iki kanun arasında yukarıda belirtmiş olduğumuz çelişkiler ve soru işaretlerinin giderilmesi ve bu hususlarla ilgili olarak Kurul ve Ticaret Bakanlığı'nın ortak bir tebliğ yayınlaması yerinde ve faydalı olur.

4. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Yürürlük Tarihinden Önce Hukuka Uygun Rıza ile Alınmış Veriler Geçerli midir?

6698 sayılı Kanun'un Geçici 1. maddesinin 3. fıkrası gereğince *"Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir"*. Buna göre 6698 sayılı Kanun'un yürürlüğe girdiği tarih olan 7 Nisan 2016'dan önce alınan veriler 6698 sayılı Kanun'un Geçici 1. maddesine göre hukuka uygun bir rıza ile alınmışsa, "1 yıl içinde aksine bir irade beyanında bulunulmaması halinde" bu Kanun'a uygun kabul edilir.

Öncelikle belirtmek gerekir ki Kanun'daki bu düzenlemede bahsedilen "hukuka uygun alınmış rızalar" ifadesi genel bir kavram olup bu maddenin tüm rıza türleri için mi geçerli olacağı yoksa sadece açık rıza hallerini mi kapsayacağı açık değildir. Yani önceden hukuka uygun olarak alınmış zımni rızalar geçerli olacak mıdır? Bu belirsizliğin giderilmesi gerekir.

Ayrıca açık rıza her ne şekilde alınmış olursa olsun 6698 sayılı Kanun kapsamında açık rıza alınması gereken hallerde açık rızayla birlikte bir aydınlatma da yapılması gerekir. Geçici 1. maddenin 3. fıkrası kapsamındaki hukuka uygun şekilde alınmış açık rızalarla işlenen veriler için geriye dönük olarak aydınlatma yapma gerekliliği söz konusu olacak mıdır? Bana göre söz konusu veri sayısının fazlalığı ve hepsi için geriye dönük aydınlatma yapılması uygulama açısından pek mümkün gözükmemektedir ancak yine de bu hususun da çıkarılacak tebliğler ya da Kurul kararıyla açıklığa kavuşturulması gerekir.

Diğer yandan Geçici 1'inci maddede aksine bir irade beyanında bulunulması için 1 yıllık bir süre verilmiştir ancak bu irade beyanının ne şekilde verileceğine ilişkin bir açıklık bulunmamaktadır. İlgili kişilerin 1 yıl içerisinde veri sorumlularıyla iletişime geçip aksi bir irade beyanında mı bulunması gerekir yoksa veri sorumlusunun 1 yıl içerisinde tüm ilgili kişileri arayıp verdikleri hukuka uygun rızanın geçerli olup olmadığını sorması mı gerekir?

Kanaatimce ilgili kişilerin veri sorumlusuyla iletişime geçip aksi yöndeki irade beyanlarını ortaya koymaları daha makul olacaktır. Zira bu görüşün aksinin kabulü halinde, veri sorumlusunun 1 yıl içerisinde verilerini işlediği tüm ilgili kişilerle bu husus kapsamında iletişime geçmesi zaman ve maliyet açısından veri sorumlusuna oldukça orantısız bir yükümlülük yükleyecektir. Bu ihtimalde de bu olumsuz irade beyanlarının ne şekilde bildirilebileceği konusu akla gelmektedir. Bu durumda ilgili kişiler her türlü yöntemle iradelerinin belirtmeli midir? Yoksa veri sorumlusuna başvuru yöntemleri kullanılarak mı bu bildirimler yapılacaktır? Bu konu da ayrıca bir uygulama problemidir. Zaten kanunun yayım tarihi ile veri sorumlusuna başvuru usullerinin belirlenmesi arasında 1 yıldan fazla süre bulunmaktadır. Bu sebeple ilgili kişinin hak kaybına uğramaması için her türlü yöntemlerle iradesini belirtmesi yerinde olabilecektir. Ancak bu durum veri sorumluları açısından da sistemin yönetilmesindeki problemleri beraberinde getirecektir. Sonuç olarak bu konuda her iki

tarafında da menfaatleri dikkate alınarak Kurum tarafından bir yönlendirme yapılması gerektiğini düşünmekteyim.

5. 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Kurul Kararlarının Yayınlandığı Süre Arasında İşlenen Verilerin Hukuka Uygunluğu Ne Olacaktır?

6698 sayılı Kanun, 7 Nisan 2016 tarihinde Resmi Gazete’de yayımlanarak yürürlüğe girmiş olup veri sorumlularına bu tarihi takiben 2 yıl içerisinde bu zamana dek işlediği tüm verileri Kanun’a uygun hale getirmeleri için süre verilmiştir. Bazı veri sorumluları 7 Nisan 2016 tarihinden itibaren 6698 sayılı Kanun’a uyum süreci altında çalışmalar yapmaya başlamışlardır. Ancak söz konusu Kanun genel düzenlemeler içermekte olup uygulama açısından eksiklikler Kurul Kararları ile giderilmeye çalışılmakta ve bu süreç hala devam etmektedir.

Bu süreçte karşımıza çıkan en önemli sorunlardan biri 7 Nisan 2016 tarihi ile konuyla ilgili Kurul kararı çıkana kadarki süreçte alınan verilerin akıbetinin ne olacağıdır. Somut bir örnek vermek gerekirse; açık rıza alınırken ve aydınlatma yapılırken dikkat edilecek hususlarla ilgili tebliğ 10 Mart 2018 (Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ) tarihinde yayımlanmıştır. 7 Nisan 2016 tarihinden 10 Mart 2018 tarihine kadar geçen süreçte şirketler Kanun’daki hususlara göre ilgili kişilerden açık rıza almışlardır. Bu süreçte alınan rızalar ve yapılan aydınlatmalar yayınlanan tebliğdeki şartları taşıyorsa bu verilerin akıbeti ne olacaktır? 6698 sayılı Kanun’a uygun işlenmişse hukuka uygun mu kabul edilecektir yoksa tebliğlerdeki usul ve esaslara uygun olması mı beklenecektir? Tebliğdeki esaslara uygun olmasının beklenmesi ihtimalinde geriye dönük olarak açık rıza alınabilecek midir?

Kanaatimce geçen süre zarfında 6698 sayılı Kanun’a uygun olarak işlenen ancak 10/03/2018 tarihindeki tebliğdeki usullere uyulmadan alınan açık rızalar söz konusu süreyle sınırlı olmak koşuluyla hukuka uygun kabul edilmelidir. Aksi taktirde Kurul Kararlarından önce Kanun’a uygun olarak uyum süreci kapsamında yapılan işlemleri sırf Kurul Kararı’na uymadığı için hukuka aykırı kabul edersek, 6698 sayılı Kanun’a uyum süreci asla sonlanmayacak ve bir kısır döngü oluşacaktır. Zira halen Kurul kararları yayınlanmaya ve kişisel verilerin korunması hukuku dönüşmeye ve gelişmeye devam etmektedir. Kaldı ki söz konusu işlemleri hukuka aykırı saymak kanunların zaman bakımından uygulanması yönünde benimsenen temel kurallara da aykırı olacaktır.

Üstelik tebliğlerde belirlenen hususlara uygun olmasının beklenmesi halinde geriye dönük açık rıza alınması gerekliliği ortaya çıkacaktır. Ancak açık rızanın şartları ve doğası göz önünde bulundurulduğunda geriye dönük açık rıza alınması mümkün olmamalıdır.

6. 6698 sayılı Kişisel Verilerin Korunması Kanunundaki Hukuka Uygunluk Nedenlerinden Sözleşmenin İfasının Kapsamının Belirsizliği

6698 sayılı Kanun’un 5. maddesinin 2. fıkrasının (c) bendinde; *“Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması”* şeklinde belirtilmek suretiyle bir sözleşmenin kurulması

veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin açık rıza alınmaksızın işlenmesi mümkün kılınmıştır.

Uygulamada özellikle web siteleri aracılığıyla alınan veriler kapsamında “sözleşmenin ifası” kavramının kapsamı oldukça önem taşımaktadır. Somut bir örnek vermek gerekirse; internet üzerinden alışveriş için üye olduğumuz bazı sitelerde üyelik aşamasında birçok kişisel veri işlenmektedir. Ancak üyelik aşamasından sonra bir ürün satın alınmaya karar verilirse üyelik aşamasında alınan kişisel veriler kapsamında da bu veriler işlenmektedir. Burada üyelik aşamasında alınan ve daha sonra ek bir onay verilmeden doğrudan mesafeli satım sözleşmesinde de kullanılan veriler için üyelik aşamasında açık rıza alınması gerekli midir? Bu sorunun yanıtlanabilmesi için sözleşmenin ifasının kapsamında değerlendirilebilecek veya değerlendirilemeyecek hususların açıklanması gerekmektedir.

Gerçekten web sitesi üzerinden bir üyelik sözleşmesi yapılıyor ise üyelik sözleşmesinin kuruluşu için zorunlu olduğu kadar veri alınmalı ve bu veriler hem amaca uygun kullanılmalı, hem hedeflenen amacı sağlamaya yetecek kadar veri alınmalı hem de veri ilgilisi bu konuda açık bir şekilde aydınlatılmalıdır. Ancak bu şartların varlığı halinde bu tür sitelere üye olunurken alınan rızalar geçerli olabilir. Ayrıca kişi üye yapılırken alınan veriler satım işlemi esnasında da kullanılacaksa, veri ilgilisi bu konuda da aydınlatılması gerekli ve yeterlidir. Zira sözleşmenin ifası hukuka uygunluk nedeni bu durumda geçerli olacaktır. Bu işlemi yapan şirket ilgili politika ve prosedürleri de buna uygun olarak yapılandırmalıdır.

7. Kişisel Verilerin İlgili Kişiden Alınmadığı Durumlarda Uygulamada Oluşan Soru ve Sorunlar

10/03/2018 tarihinde Kurul tarafından yayımlanan “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”in “Kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğü” başlıklı 6. maddesine göre; “Kişisel verilerin ilgili kişiden elde edilmemesi halinde; Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında, kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerekir.”

Buna göre kişisel verinin ilgili kişiden alınmaması durumu için de veri sorumlusuna, veri ilgisini makul bir süre içerisinde aydınlatma yükümlülüğü yüklenmiştir. Ancak bu düzenleme uygulama açısından yeterli olmamakla birlikte çoğu zaman veri ilgililerinin hepsine ulaşma imkânı da bulunmamaktadır.

Somut örnek vermek gerekir ise işçinin işe başlamak üzere verdiği ailesi ve çocuklarına ilişkin kişisel verilerde veya iş başvurularında başvuru tarafından verilen referans kişilere ait kişisel verilerde ve hatta kamu otoriteleri tarafından düzenlenen belgelerde bulunan (örneğin icra ödeme emirleri, trafik ceza tutanağı, bilirkişi raporları vb.) üçüncü kişilere ait kişisel verilerde veri sahibi kişilerin aydınlatılması imkânı oldukça güçtür. Bu durumda söz konusu örneklerdeki üçüncü kişilerin aydınlatılması veri sorumluları için altından kalkılamaz bir yük olacaktır diye düşünüyorum.

Tebliğ ile getirilen bu düzenleme teorik olarak mümkün gözükse de uygulamada sorunlara neden olmaktadır. Bu nedenle veri sorumlusuna gerekenden fazla yükümlülük yüklenmemeli ve veri sorumlularının bu hususta uğrayacakları mağduriyetler engellenmelidir.

8. Özel Nitelikli Kişisel Verilerin Kapsamı, Çift Katmanlı Doğrulama Sistemi ve Özel Nitelikli Kişisel Veriler İçin Ayrı Politika ve Prosedürler Hazırlanması Hususunda Uygulamadaki Soru İşaretleri

“Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı Karar’ında; *“Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,...”* şeklinde belirtildiği üzere özel nitelikli kişisel verilerin güvenliğine yönelik ayrı bir politika ve prosedürün oluşturulması öngörülmüştür.

Burada ayrı politika ve prosedürden kasıt ayrı ayrı metinler midir yoksa tek bir politika ve prosedürün içerisinde ayrı bir başlık altında da özel nitelikli kişisel veriler için politika ve prosedürlere de yer verilebilir mi?

6698 sayılı Kanun’da açıkça tanımlandığı üzere 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 veridir. Özel nitelikli kişisel verilerle ilgili önemli bir husus ise; söz konusu kategorilerin kapsamıdır. Örneğin; kılık kıyafet görüntüleri kişinin etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi gibi birçok hususta bilgi verebilecek niteliktedir. Bu durumda kılık kıyafet görüntüleri özel nitelikli kişisel veri sayılabilir mi? Eğer bu verileri özel nitelikli kişisel veri sayarsak bu durumda bu verilerin veri sorumlusu bünyesinde tutulmaya devam edilebilmesi için kriptolanması gerekliliği gündeme gelecektir. Ancak belirtmek gerekir ki kamera görüntülerini kriptolamak mümkün değildir. Aynı şekilde İş Sağlığı ve Güvenliği Mevzuatı’nda³ bu kayıtların belirli bir süre saklanması gerekli kılan bir düzenleme bulunmaktadır. Bu gibi kişisel verilerin özel nitelikli kişisel veri sayılıp sayılamayacağı açıklığa kavuşturulmalı ve sayılması durumunda bu duruma bir çözüm getirilmelidir.

Bana göre, tek başına kılık kıyafet görüntüleri özel nitelikli kişisel veri sayılmamalıdır. Bu veriler ancak belli bir sistematikte kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançlarını tespit etmek için analiz ediliyorsa bu durumda özel nitelikli kişisel veri özelliğini kazanır ve bu durumdan sonra özel nitelikli kişisel verilerin korunmasına ilişkin hususlar bu veriler için de uygulama alanı bulur.

Aynı zamanda 2018/10 sayılı Kurul Kararı’nda özel nitelikli kişisel verilere uzaktan erişilmesi durumunda *“çift katmanlı doğrulama sistemi”* öngörülmüştür. Ancak çift katmanlı doğrulama sisteminin ne olduğu ve nasıl sağlanacağı hususunda bir açıklama yapılmamıştır. Bilgi

³ İşyeri Açma ve Çalışma Ruhsatlarına İlişkin Yönetmelik m.5. Tehlikeli Madde Taşıyan Araç ve Üst Yapıların Teknik Muayeneleri Hakkında Yönetmelik’ m.6.

güvenliği kapsamında çift katmanlı doğrulama sistemi “*bilinen ve sahip olunan bilgi*” olmak üzere iki katmanlı doğrulamayla oluşturulan bir güvenlik sistemidir. Ancak söz konusu Kurul Kararı kapsamında bu sistemin ne olduğu ve nasıl uygulanacağı hakkında bir açıklama yapılmamıştır. Bu noktanın da açıklığa kavuşturulması gerekir.

9. 6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Veri İşleyenlerin Durumu

6698 sayılı Kanun’a baktığımızda GDPR ve Direktif’ten farklı olarak veri işleyenlerin tam bir standardının olmadığı görülür. 6698 sayılı Kanun’da veri işleyen; “*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi...*” şeklinde tanımlanmıştır.

Uygulamada veri işleyen sıfatına haiz olmamakla birlikte çok fazla sayıda kişisel veri aktarımı olan gerçek veya tüzel kişiler mevcuttur. Örneğin; şirketlere sağlık tetkiki yapmak için gelen kurumlar ve yoğun veri aktarımı yapılan şirketler bulunmakta, ancak bunlar veri sorumlusu adına veri işlememektedir.

Veri işleyen sıfatına sahip olmamakla birlikte söz konusu kurum/şirketlerle veri işleyen sözleşmesi standartlarında bir sözleşme yapılması mümkün müdür? Bu konuda risklerin azaltılması için yukarıda belirttiğimiz şekilde yoğun veri aktarımının olduğu veya özel nitelikli verilerin yoğun olarak aktarıldığı ancak veri işleyen niteliğinde olmayan gerçek veya tüzel kişiler ile de veri işleyenler ile yapılan sözleşmelere benzer bir sözleşme yapılmalı ve bu kişiler tarafından da kişisel verilerin korunması taahhüdünü sağlayacak mekanizmalar oluşturulmalıdır.

10. Kişisel Verilerin Yurtdışına Aktarımı ve Bulut Hizmet Sağlayıcılar Konusundaki Belirsizlik

Son olarak da kişisel verilerin yurtdışına aktarımı kapsamında uygulamada karşımıza çıkan soru ve sorunlara değinilmesi yerinde olacaktır.

Kişisel verilerin yurtdışına aktarılması hususunda en önemli sorunlardan biri yeterli korumanın bulunduğu “güvenli ülkelerin” henüz ilan edilmemiş olmasıdır. Bu listenin ne zaman açıklanacağını halihazırda varsayılabilir olmadığından hareketle, listenin ilanına kadar yurtdışına aktarım için uygulamada rıza alınması yoluna başvurulmaktadır. Doğru uygulamanın gelişmesi açısından da yeterli korumanın bulunduğu ülkelerin ilan edilmesi, bunun yanı sıra Kurul’un bulut hizmet sunucularında tutulan kişisel veriler yönünden görüşlerini bildirmesi önemlidir.

Kişisel verilerin yurtdışına aktarılması başlığı altında, yeterli korumanın bulunduğu ülkeler henüz ilan edilmemekle birlikte, Kurul’un bu konuda sözlü olarak karşılıklılık ilkesini uygulayacağına dair açıklamaları bulunmaktadır. Bununla birlikte, yapılan tartışmalarla listenin ne zaman açıklanacağını halihazırda varsayılabilir olmadığı ve bu nedenle listenin ilanına kadar, yurtdışına aktarım için rıza yoluna başvurulması gerektiği konularında hemfikir olunmuştur.

Bu kapsamda, hangi işlemlerin yurtdışına veri aktarımı olarak kabul edileceği/edilmesi gerekeceği de önemli bir konudur. Uluslararası şirketlerin çeşitli birimlerinin yurtdışından yönetildiği ve ilgili birimlere ilişkin tüm verilerin yurtdışında tutulduğu veya şirket sunucularının yurtdışında bulunduğu uygulamalar günümüzde oldukça fazladır Uluslararası otel zincirleri bu hususta yerinde bir örnek olacaktır. Hâlihazırda, uygulamada şirketlere yurtdışına aktardıkları tüm veriler için rıza almaları veya serverlarını yurt içinde tutmalarını önermek tercih edilse de, bu tür önerilerin uygulamada pratik, hızlı ve tam olarak gerçekleştirilebilir olmayacağı veya kişilerden rıza alınmasındaki ve rızanın geri çekilmesi halindeki sorunlarla karşılaşılacağı açıktır. Uygulamada karşılaşılabilecek zorlukları düşünerek, uluslararası şirketlerin burada belirtilen şekildeki veri aktarımları için farklı bir yaklaşım getirmek faydalı olacaktır.

Öte yandan, yeterli korumanın bulunduğu ülkeler listesi yayınlansa dahi, bulut hizmet sunucularının genellikle verileri birden çok ülkede tuttukları ve verilerinin yedeklemesini çeşitli ülkelerde yaptıkları göz önünde bulundurulursa, yayımlanan listenin bu noktada yetersiz kalma ihtimali bulunmaktadır. Buna karşılık, sorunun, şirketlerin hizmet sunucularıyla yapacakları sözleşmelere koyacakları hükümler aracılığıyla, verilerin yedekleneceği ülkeleri kısıtlamaları yoluyla çözülebilecekleri düşünülebilir. Ancak bu şekilde bir çözüm veri sorumluları açısından ciddi maliyetler doğurabilir. Kaldı ki bulut hizmet sunucularının çoğu kendi standartları ile hareket etmektedir ve bunlardan bazılarının sözleşmelerinin müzakere etmeye kapalı olması da uygulamada sorunlara yol açabilir. Kurul'un bulut çözümlerine ilişkin yaklaşımı henüz belli değildir. Ancak şu ana kadar çeşitli konularda uygulamaya vermiş olduğu yön dikkate alınacak olursa, Kurul'un, büyük olasılıkla bulut hizmet sağlayıcıları aracılığıyla işlenen verileri yurtdışına aktarım kapsamında değerlendireceği şaşırtıcı olmayacaktır⁴.

Burada önemli olan bir diğer husus ise güvenli ülkeler belirlendiğinde bulut hizmet sunucuları açısından verilerin tutulduğu ülke kapsamında mı yoksa bulut hizmet sunucularını bağlı olduğu şirketin menşei ülke kapsamında mı güvenli ülke olup olmadığının değerlendirileceğidir. Verilerin bulundurulduğu ülke kapsamında güvenli olacağının belirlenmesi ihtimalinde ise çoğu zaman bulut hizmet sunucularının verileri nerede tuttukları tam olarak bilinmemekte ve tespiti de oldukça güç olmaktadır.

Bu başlık altında değineceğim son husus ise; güvenli ülkeler listesinin yayınlanması durumunda dahi şirketlerin günlük işleyişinde yapması gereken ani aktarımlar için nasıl bir yol izlemesi gerektiğinin düzenlenmediğidir. Mevzuattaki bu boşluk şirket işleyişleri göz önünde bulundurulduğunda giderilmesi zaruri olan bir eksikliktir. Bana göre, güvenli olmayan ülkelere veri aktarım prosedürünün ani durumlara uyumluluk gösterecek şekilde düzenlenmesi gerekir.

Yukarıda açıkladığım tüm hususlar ışığında kişisel verilerin yurtdışına aktarımı konusunda esas ve usul açısından uygulamaya yönelik düzenlemeler yapılması ve bazı kavramların açıklığa kavuşturulması gerekir.

Sonuç

⁴ **Kişisel Veriler Platformu Çalışma Notları**, Amaç Tartışılan Konular Toplantı Notları, Tespit ve Öneriler, Ocak – Haziran 2018, s.7 vd.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun uygulamasında ve uyum sürecinde ortaya çıkan soru ve sorunların yukarıda açıklanan hususlar çerçevesinde değerlendirilmesi sonucunda varmış olduğum sonuçlar şu şekildedir:

- VERBİS Sicil Yönetmeliği'nin 13. maddesinde düzenlenen 7 günlük sürenin başlayacağı zamanın açıkça düzenlenmesi gerekir. Bana göre bu sürenin değişikliğin tespit edilmesinden itibaren başlaması gerekir.
- Açık rıza alınırken rıza karşılığı ek avantaj getirilmesinde bir engel bulunmaz. Ayrıca bu husus açık rızanın kişinin özgür iradesinin ürünü olması şartının oluşmasına engel teşkil etmez.
- Kurul ve Ticaret Bakanlığı Elektronik ortamda işlenen veriler açısından 6563 sayılı Kanun ile 6698 sayılı Kanun arasından çelişkiler ve soru işaretlerinin giderileceği ortak bir tebliğ yayınlamalıdır. Bu konu bakımından; hem özel kanun - genel kanun ilişkisinden hem de 6698 sayılı Kanun'un 5. maddesinde "*kanunda öngörülmüş olma*" halinin istisna olarak sayılmasından dolayı elektronik ortamda işlenen kişisel veriler için 6563 sayılı Kanun'un uygulanması gerekir.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlük tarihinden önce hukuka uygun rıza ile alınmış verilerin akıbetinin ve hukuka uygun alınmış rıza kavramının açıklığa kavuşturulması gerekir. Özellikle bu dönemde alınan zımni rızaların akıbetinin belirlenmesi önemlidir.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Kurul Kararlarının yayınlandığı süre arasında işlenen verilerin hukuka uygunluğu bakımından, 6698 sayılı Kanun'a uygun olarak işlenmişse bu verilerin hukuka uygun kabul edilmesi gerekir.
- Uygulamada sorun yaratmaması ve kişisel verilere sunulan korumada, koruma altına alınmayan bir husus bırakılmaması amacıyla veri işleyen kavramı açısından belirli bir standart getirilmelidir. Bu durum özellikle şu anki düzenleme kapsamında veri işleyen kategorisine girmeyen ancak kişisel verilere ulaşımı çok fazla olan oluşumlarda, söz konusu verilerin korumasının sağlanabilmesi için oldukça önemlidir.
- Kişisel verilerin yurtdışına aktarımı hususunda önemli düzenlemeler yapılması gerekmektedir. Bulut hizmeti sunan sistemlere Kurul'un bakış açısı ortaya konmalı ve hatta bu sistemler için ayrıca düzenlemeler getirilmelidir.
- Ayrıca şirketlerin yurtdışına veri aktarırken uygulamaları gereken prosedür günlük hayatta şirketlerin işleyiş hızı dikkate alındığında işleyişte aksaklığa sebebiyet verebilecek kadar yavaş işleyen bir prosedürdür. Bu nedenle bu prosedürler de revize edilmelidir.