

**KİŞİSEL VERİLERİ KORUMA KURULU’NUN 2018/10 SAYILI KARARI İLE
AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİ VE VERİ
SORUMLUSUNA BAŞVURU KONULU TEBLİĞLERE İLİŞKİN
DEĞERLENDİRME**

Doç. Dr. Murat Volkan Dülger*

Kişisel verilerin korunması hakkının her geçen gün daha fazla ilgi çektiği ülkemizde buna paralel olarak, 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun ardından kişisel verilerin korunması alanına ilişkin yönetmelik, tebliğ ve karar yayınlanması yoluna gidilerek konu, yetkililer tarafından yasal düzenlemeler ile kapsamlı bir biçimde açıklanmak istenmektedir.

Kişisel verilerin korunması hakkının konu edildiği çalışmalar uzun zaman öncesine dayansa da konuya ilişkin ilk somut adım, söz konusu hakkın 2010 yılında yapılan Anayasa değişikliği sonucu Anayasanın 20. maddesine eklenen 3. fıkrasıyla Anayasal güvence altına alınması ile atılmıştır. Bu husus kişisel verilerin Anayasal düzeyde korunmaya değer görülmesi ve özel hayatın gizliliği başlığı altında düzenlenmiş bulunsu da özel hayat kavramından ayrı olarak zikredilmesi oldukça önemli olmuştur.

Anayasada yapılan değişikliğin ardından zaman içerisinde kişisel verilerin korunması hakkının kapsamlı bir şekilde düzenlenmesi ihtiyacının artması ile nihayet 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde yürürlüğe girerek; söz konusu ihtiyaç büyük ölçüde giderilmeye çalışılmıştır.

Kişisel verilerin korunması hakkı, konuyla ilgili daha önceki yazılarımda da belirttiğim gibi birçok hak ile bağlantılı olup; oldukça geniş bir kavramı ifade eder. Özellikle teknolojinin geldiği nokta ile bağlantılı olarak hangi faaliyet içerisinde bulunursa bulunulsun, kişisel veriler alınmadan, tutulmadan veya herhangi bir biçimde işlenmeden bu işlemlerin yapılması mümkün değildir. Üstelik bu yalnızca ekonomik ve mesleki faaliyetlerle sınırlı olmayıp; gündelik ihtiyaçlarımızda dahi sıklıkla karşılaştığımız ve ihtiyaç duyduğumuz bir husus haline gelmiştir.

Günlük hayatımızın bu denli içerisine girerek, her anımızla ilişkili olan kişisel verilerin korunması hakkının yalnızca Kanun ile hüküm altına alınan düzenlemelerle yeterli bir korumaya sahip olması beklenemez. Bu nedenle Kanun’un genel olarak düzenlediği hususları açıklamak ve eksik kalan noktaları tamamlamak amaçlarıyla başta yönetmelik olmak üzere diğer hukuki araçların kullanılması zorunludur.

Nitekim 6698 sayılı Kanun tarafından hüküm altına alınmış bulunan birtakım konulara ilişkin usul ve esasları belirlemek amacıyla yönetmelikler yayınlanacağı öngörülmüş ve Kanun’dan sonra birçok farklı kırılım noktasında yayınlanan yönetmelikler ile konunun daha iyi anlaşılması sağlanmaya çalışılmıştır.

Kişisel verilerin korunması alanında yaşanan gelişmeleri son olarak tarafımızca da beklendiği üzere Kişisel Verileri Koruma Kurulu tarafından yayınlanan karar ve tebliğler takip etmiştir.

* Akademisyen/Avukat

Bu yazımda da söz konusu karar ve tebliğleri ayrı başlıklar halinde detaylı bir biçimde inceleyip, düzenlemelerin hangi konularda faydalı olup hangi eksik yönleri tamamlayıcı nitelikte olduğunu konuya ilişkin daha önce de yapılan düzenlemeler doğrultusunda değerlendirmede bulunacağım. Ayrıca metin ifadelerinden çıkarılabilecek muhtemel yanlış anlaşılımları ve tartışma yaratabilecek noktalara değinip; kendi düşüncelerimi de belirteceğim.

I. Kişisel Verileri Koruma Kurulu’nun 2018/10 Sayılı Kararı ve Özel Nitelikli Kişisel Veriler Açısından Alınması Gereken Yeterli Önlemler

Kişisel Verileri Koruma Kurulu’nun “*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*” konulu, 31/01/2018 tarihli ve 2018/10 sayılı kararı, 7 Mart 2018 tarihli ve 30353 sayılı Resmi Gazete’de yayınlandı¹. Karar, Kurulun yaptığı görüşmeler sonucu belirlenmiş ve yayımlanmış olup; dayanağını KVKK’nın özel nitelikli kişisel verilerin işleme şartları başlıklı 6. maddesinin 4. fıkrası ile kurulun görev ve yetkileri başlıklı 22. maddesinden almıştır. Zira söz konusu hükümlerde özel nitelikli verilerin işlenmesinde kanun ile belirtilenler dışında ayrıca Kurul tarafından yeterli önlemlerin belirlenmesi zorunlu kılınmıştı.

Kararla ilgili ilk olarak Kurul’un 6698 sayılı Kanun’un uygulanmasını sağlamak amacıyla yayınladığı ilk karar olması noktasına dikkat çekmek istiyorum. Kurulun özellikle tartışmalı noktalara ilişkin olarak bu şekilde çalışmalar yapmasını, hem Kanun’un uygulanması ve anlaşılması açısından hem de Kanun’a uyumluluk süreçlerinde oldukça faydalı buluyorum.

Kararda belirlenen yeterli önlemler şunlardır:

1. *Kişisel verilerin korunması, saklanması ve işlenmesi politika ve prosedürüne ilişkin önlemler*

Kişisel verilerin korunmasına ilişkin politika oluşturulması Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’in 5. maddesiyle zaten zorunlu kılınmıştı. Buna göre veri sorumluları siciline kayıt olmakla yükümlü olan veri sorumluları, oluşturdukları kişisel veri envanterine uygun olarak kişisel veri saklama ve imha politikası oluşturmak zorundadır. Kurul tarafından yayınlanan karar ile özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi ilk kez öngörülmüştür. Bu tedbirle:

- Veri sorumlularının Kanun’a uyumluluk süreçlerinde özel nitelikli kişisel verilere yönelik faaliyetleri konusunda ayrıca çalışma yapması ve bu verilere ilişkin ayrı prosedürler belirleyip politika oluşturması,
- Ayrıca bu politika ve prosedürlerin belirtildiği gibi sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir şartlarına sahip olması,

gerekecektir.

¹ Kararın tamamı için bakınız: <http://www.resmigazete.gov.tr/eskiler/2018/03/20180307-7.pdf>

Bu zorunluluk ile veri sorumlularına esasen daha sıkı yükümlölükler getirilmiş olmakla beraber; özel nitelikli verilerin önemi ve bu veriler üzerinde gerçekleşebilecek olası ihlallerin doğuracağı tehlikeli sonuçlar düşünüldüğünde, bu verilerin saklanması ve işlenmesinin farklı şartlara bağlanması ve bu şartların belirli olması zaten olması gerektir.

2. Özel nitelikli kişisel verilerin işlenmesi süreçlerinde çalışanlara yönelik alınacak tedbirler

Kurul'un, özel nitelikli verilerin işlenme süreçlerinde çalışanlara yönelik olarak alınacak teknik ve idari tedbirler bakımından da ayrıma gittiğini görüyoruz. Buna göre çalışanlara yönelik alınması gereken tedbirler şunlardır:

- *Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi:*

Bu noktada öncelikle belirtmek istediğim en önemli husus Kanun'a uyumluluk süreçlerinde konuyla ilgili eğitimin olmazsa olmaz nitelikte olduğudur. Kanun'a uyumlu hale gelmek zorunda bulunan veri sorumluları ve bu veri işleme faaliyetleri içerisinde yer alan veri işleyenlerin veya faaliyet içerisinde bulunsun veya bulunmasın olası risklere karşı bu faaliyetler esnasında veri sorumluları bünyesinde bulunan tüm kişilerin, kişisel verilerin korunması hakkında teknik ve idari bakımından eğitilmesi şarttır. Eğitim yapılmaksızın veri sorumlularını Kanun'a uyumlu hale getirmek ne mümkün ne de doğru bir yaklaşımdır. Böyle bir bakış açısıyla yürütülen uyumluluk süreçlerinin sonucunda, o an için Kanun'a uyumlu bir görünüm elde edilmiş olsa bile bu yalnızca görünümünden ibaret olup ileride büyük sorunlarla karşılaşılmasından kaçınılamaz. Bunun nedeni ülkemizde kişisel veri ve bu verilerin korunmasına yönelik mantığın değişmesi gerektiğidir. Ayrıca veri sorumluları faaliyetleri çerçevesinde sürekli olarak veri tutmaya ve veri işlemeye devam etmektedir. Dolayısıyla bu konu esasında devam eden ve yaşayan bir süreçtir. Bu nedenle kişisel verilerin korunması alanına ilişkin eğitimler şart olup; bu eğitimlerin belli aralıklarla güncel konular doğrultusunda tekrar edilmesi gereklidir.

Özel nitelikli verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik bu verilerin güvenliği konusunda düzenli eğitim verilmesini öngören kararı veri sorumluları ve veri işleyenlerin kişisel verilerin korunması bilincini geliştirmesi adına zorunlu ve olumlu bir gelişme olarak değerlendiriyorum.

- *Gizlilik sözleşmelerinin yapılması:*

Gizlilik sözleşmesi taraflar arasında yürütülen iş konusu hakkında, ilgili kişinin onayı alınmaksızın herhangi bir üçüncü gerçek veya tüzel kişiye bilgi verilmemesini ve gizliliğin sınırlarını belirlemeyi sağlar. Karar ile özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlarla gizlilik sözleşmesi yapılması zorunlu hale getirilmiştir. Buradan özel nitelikte olmayan verilerde henüz böyle bir yükümlölüğün getirilmediği anlaşılabılır. Hali hazırda zaten gizlilik sözleşmesi yapan veri sorumlularının ise bu sözleşmeleri, özel nitelikleri kişisel verileri de kapsamı altına aldığını açıkça gösterecek biçimde düzenlemeleri gerektiğini düşünüyorum.

- *Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması:*

Veri sorumluları, faaliyetleri çerçevesinde özel veya özel nitelikte veri ayrımı olmaksızın ihtiyaç duydukları kişisel verilerin alınması, işlenmesi ve işleme süresini net bir biçimde belirlemek durumundadır. Bunun doğal sonucu olarak söz konusu verilere erişmeye yetkili kişilerin de bu yetki kapsamlarının ve sürelerinin belirli olması gerekir. Dolayısıyla belirlenen bu tedbirin, zaten mevcut şartlarda alınması gerekmektedir. Nitekim Kanun'un veri güvenliğine ilişkin yükümlülüklerin düzenlendiği 12. maddesinde de verilere hukuka aykırı olarak erişilmesini önlemek veri sorumlusunun yükümlülükleri altında sayılmıştır.

Bununla birlikte bu hususun özel nitelikli kişisel veriler açısından açıkça belirtilmesi yerindedir. Ayrıca erişime yetkili kişiler bulunsun da bu yetkinin kapsam ve sınırının çizilmesi ve yetkinin ne kadar süreyle devam edeceğinin tanımlanması gerektiğinden, kapsam ve sürenin belirlenmesi noktasında dikkatli olunması gerekir.

- *Periyodik olarak yetki kontrollerinin gerçekleştirilmesi:*
Buna göre özel nitelikte kişisel verilerin işlenmesinde yer alan çalışanların yetkisinin hukuka uygunluğu belli periyotlarla denetlenmelidir. Denetimlerin yapılacağı zaman aralıkları belirli olmalıdır.
- *Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması ve bu kapsamda veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması:*
İşten ayrılan çalışanların sebep olacağı kişisel veri ihlalleri büyük bir tehlike konusudur. Zira çalıştığı sırada kişisel verileri hukuka uygun bir biçimde tutan veya işleyen çalışanların, işten ayrılmalarda halinde özellikle veri sorumlusu tarafından gerekli tedbirlerin alınması gerekir. Bu karar ile görev değişikliği veya işten ayrılan çalışanların pozisyonları doğrultusunda sahip oldukları yetkilerin derhal kaldırılması gerektiği belirtilerek, bu kapsamda kişisel veri envanterinin de geri alınması gerektiğinin altı çizilmiştir.

3. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamların elektronik ortam olmasına ilişkin açıklamalar

İşlenen, muhafaza edilen veya erişilen kişisel verilerin tutulduğu ortamın elektronik ortam olması halinde aşağıda belirtilen tedbirlerin alınması zorunludur:

- *Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi:*
Özel nitelikli kişisel verilerin muhafazası için kriptografik yöntemlerin kullanılması gerektiği tedbirini belirleyen Kurul, bu yöntemlerden herhangi birini işaret etmemiş ve bu konuyu veri sorumlusunun takdir yetkisine bırakmıştır. Ancak bu takdir yetkisinin sınırını yine Kurul tarafından yakın zamanda yayınlanan Kişisel Veri Güvenliği Rehberi'nde görüyoruz². Rehber'e göre kişisel verilerin tam olarak korunduğundan emin olunması için uluslararası kabul gören şifreleme programlarının kullanımı tercih edilmelidir. Öyleyse veri sorumlusu verilerin muhafaza edilmesinde uluslararası kabul gören şifreleme programlarında kendisine en uygun olan yöntemi belirleyebilecektir.

² **Kişisel Veri Güvenliği Rehberi tam metnine ulaşmak için bakınız:**
http://kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

- *Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması:*
Özel nitelikli kişisel veriler kriptografik yöntemler kullanılarak muhafaza edildikten sonra bu şifre anahtarı da güvenli ve farklı ortamlarda tutulmalıdır. Bu kapsamda şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda saklanmalı ve yetkisiz olarak erişim de önlenmelidir.
- *Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması:*
Bir sistemin ve sistemdeki kullanıcıların hareketlerini kaydeden yapı anlamına gelen ve aygıtın geriye dönük yaptığı işlemlerin kayıt altına alınmasını sağlayan loglama işlemi, özel nitelikteki kişisel veriler üzerinde gerçekleştirilen hareketler için de zorunlu hale getirilmiştir.
- *Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması:*
Burada dikkati çekmek istediğim esas husus; veri güvenliğinin sağlanmasına yönelik çözümler üretilmesinin yeterli görülmeyip; ayrıca bu çözümlerin güncel olması gerektiğinin aranmasıdır. Belirlenen çözümlerin güncel olup olmadığı takip edilmeli, güvenlik açıklarının tespitini sağlayan güvenlik testleri düzenli olarak yapılmalı ve bu test sonuçları kaydedilmelidir. Uygulamada veri kaybı ve sızıntısını önlemek amacıyla DLP güvenlik yöntemleri yaygın olarak kullanılmaktadır.
- *Verilere bir yazılım aracılığıyla erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması:*
Kişisel verilerin bulunduğu ortamların güvenliğinin sağlanmasının yanı sıra; özel nitelikte kişisel verilere erişilmesini sağlayan yazılımların da aynı şekilde güvenlik testlerinden geçirilmesi ve bu test sonuçlarının kaydedilmesi gerekir. Ayrıca yazılıma erişme yetkisine sahip kullanıcıların açıkça belirlenmesi gerekir.
- *Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması:*
Bu ifadede yer alan uzaktan erişim kavramıyla kastedilenin bilgisayar ortamında bulunan bir dosyaya network üzerinden ulaşılması olduğunu düşünüyorum. Örneğin, iki bilgisayar aynı odada olsa bile bir bilgisayara diğer bilgisayar aracılığıyla ulaşıyorsa böyle bir erişim uzaktan erişim olarak adlandırılır. Karar ile böyle bir erişimde en az iki kademeli kimlik doğrulama sisteminin sağlanması tedbiri getirilmiştir. Veri sorumlusunun bu tedbiri alabilmek için kendiliğinden iki kademeli olan yazılımları da kullanabilmesinde sakınca görülmemektedir.

4. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamların fiziksel ortam olmasına ilişkin

İşlenen, muhafaza edilen veya erişilen kişisel verilerin tutulduğu ortamın fiziksel ortam olması halinde aşağıda belirtilen tedbirlerin alınması zorunludur:

- *Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması:*

Öncelikle fiziksel olarak bulunan özel nitelikte kişisel veriler hangi ortamda bulunursa bulunsun belirtilen önlemlerin alınması gerektiğini belirtmeliyim. Bu noktada veri sorumlusu, söz konusu kişisel verileri yalnızca fiziksel olarak işyerinde değil; her yerde olursa olsun korumalı ve bunun için gerekli önlemleri almalıdır. Özel nitelikte kişisel verilerin bulunduğu fiziksel ortamların kilit altında tutulması, yetkili kişilerin erişebileceği ve yetkisiz erişimlerin önlenmesi bu kapsamda alınması gereken önemli tedbirlerdir.

- *Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi:*
Buna göre özel nitelikli kişisel verilerin bulunduğu fiziksel ortamlara giriş çıkışların kontrol altına alınması gerekir. Bu ortamlara girişlerin şifrelenmesi veya kartlı sistem oluşturulması ve bu şifre ve kartların yalnızca yetkili kişilerde bulunması en yaygın kullanılan güvenlik yöntemlerindedir.

5. Özel nitelikli kişisel verilerin aktarımına ilişkin

Özel nitelikli kişisel verilerin aktarılması sırasında belirtilen güvenlik tedbirlerine uyulması zorunludur:

- *Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması:*
Burada özel nitelikli kişisel verinin aktarımını gerçekleştirecek kişiye iki farklı seçenek tanınmıştır. Buna göre; ilk yol olarak yöntemi belirli olmaksızın şifreli olarak kurumsal e-posta adresi kullanılacaktır. Kurul, bu tür bir aktarımda hangi şifreleme yöntemi kullanılacağını belirtmemiş, bu noktada takdir yetkisi tanınmıştır. Öyleyse veri sorumlusu veya veri işleyen kendisine en uygun yöntemi belirlemelidir. Kurul, ikinci olarak özel nitelikli veri aktarımının elektronik postanın nitelikli halini oluşturan KEP hesabı aracılığıyla gerçekleştirileceğini öngörmüştür.
- *Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması:*
Özel nitelikli kişisel verilerin belirtilen yollarla aktarılması halinde de yine bu aktarım kriptografik yöntemlerle gerçekleştirilecek ve şifre anahtarı farklı ortamda tutulacaktır. Kurul, burada da yöntemini belirlememiştir.
- *Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi:*
Güvenli dosya taşıma protokolü anlamına gelen sFTP dosya transferi yapılırken kullanılan ftp yönteminin şifrelenmiş halini oluşturur. VPN ise bilgisayarın fiziksel olarak bulunduğu yerden başka bir ağa şifreli tünel açarak dışardan görünümü engeller. Veri akışı görülebilse de bu akışın içeriğini görebilmek mümkün değildir. Veri sorumlusunun alması gereken söz konusu tedbirle amaçları aynı olsa da birbirinden çok farklı çalışan iki farklı şifreleme yönteminden bahsedilmiştir.

- *Verilerin kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi:*

Burada evrak yoluyla gerçekleştirilen aktarımlarda evrakın olası risklerden korunması ve yetkisiz kişiler tarafından görülmemesi için her türlü tedbirin alınması gerektiği belirtilmiştir. Ayrıca bu evrakın gizlilik dereceli belgeler formatında gönderilmesi gerektiği ancak format hakkında bilgi verilmemesi akıllara yeni soru işaretlerini beraberinde getirmiştir. Bu sorulara cevap verebilmek adına 2016 tarihli “*Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması*”na³ bakmak gerekir. Zira bu düzenlemede güvenlik dereceleri sınıflandırılmış, yeni dereceler belirlenmiş ve uygulamada yeni açılım sağlanması amaçlanmıştır.

Öncelikle gizlilik derecesi, bilgi varlığının bilmesi gereken kişiler dışındakilere açıklanmasının veya verilmesinin millî güvenlik veya kişisel güvenlik açısından sakıncalı görülen hallerde, muhtemel zararların önlenmesi amacıyla önem derecesine göre sınıflandırılması ve adlandırılması anlamına gelir. Söz konusu düzenlemede gizlilik derecesi sekiz başlık altında toplanmış ve Kişisel Verilerin Korunması Kanunu çerçevesinde özel nitelikli kişisel veri kapsamına giren bilgi için ise “KİŞİYE GİZLİ” sınıflandırılması öngörülmüştür.

6. *Belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurulu’nun internet sitesinde yayımlanan Kişisel Veri Güvenliğine İlişkin Rehber’inde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirlerin de dikkate alınması gerekliliği*

Kurul tarafından özel nitelikli verilere ilişkin olarak alınacak tedbirlerin belirlendiği kararda esasen söz konusu Rehber büyük ölçüde dikkate alınmıştır. Bu nedenle kararda eksik veya belirsiz olduğu düşünülen noktalarda Karar ile Rehberin birlikte değerlendirilerek sonuca ulaşılması faydalı olacaktır.

Sonuç

Kişisel Verileri Koruma Kurulu tarafından yayınlanan kararla, özel nitelikli kişisel verilerin önemi, yaygınlığı ve bu veriler üzerinde gerçekleştirilebilecek hukuka aykırı eylemlerin sebep olacağı tehlikeler dikkate alınarak özel nitelikli kişisel verilere ilişkin birçok farklı noktada ayrıma gidilmiştir. Kurul, yukarıda tek tek açıkladığım üzere; özel nitelikli kişisel veriler konusunda, ayrı prosedür ve politikaların belirlenmesi, çalışanlara yönelik ayrıca tedbirlerin alınması, bu verilerin fiziksel veya elektronik ortamda saklanmasına göre buna ilişkin teknik ve idari tedbirlerin alınması ve bu verilerin aktarılması faaliyetlerini haklı bir biçimde ayrı esaslara tabi tutmuştur.

Burada değinmek istediğim bir diğer husus, Kurul tarafından belirlenen önlemler isimden de anlaşılabilceği gibi “yeterli önlemler” niteliğindedir. Dolayısıyla bu önlemler asgari düzeyde olup; eksiksiz alınması halinde yeterli olacaktır. Bununla beraber veri sorumlusu tarafından alınan teknik ve idari tedbirlerin gerçekleştirilen faaliyet göz önüne alındığında eksik ve yetersiz kalması halinde; veri sorumlusu, Karar ile belirtilen önlemleri aldığından bahisle

³ **Tam metin için bakınız:** <http://www.udhb.gov.tr/doc/siberg/siberbilgi.pdf>

Kanun'un 12. maddesi ile kendisine verilen veri güvenliğine ilişkin yükümlülüklerden kurtulamaz.

Kurul'un yayınladığı Karar, özel nitelikli verilere ilişkin faaliyetlerde alınması gereken teknik ve idari tedbirlerin belirlenmesi açısından oldukça önemli ve yardımcı niteliktedir. Ayrıca tedbirlerin belirlenmesi noktasında Karar ile Veri Güvenliğine İlişkin Rehberin birlikte değerlendirilmesi gerektiği de atlanmamalıdır.

II. Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

Veri sorumlusuna başvuru, Kanun'un 13. maddesiyle ilgili kişiye tanınan bir haktır. Buna göre; ilgili kişi, Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna bildirebilir. Veri sorumlusu ise başvuruda yer alan talepleri en kısa sürede ve en geç otuz gün içinde yerine getirmelidir. Taleplerin yerine getirilmesinin ücretsiz olması esas olmakla beraber; işlemin ayrıca bir ücret gerektirmesi halinde ilgili kişiden ücret talep edilebileceği de hüküm altına alınmıştır.

Kanun tarafından veri sorumlusuna başvuru hakkının genel çerçevesi çizilmiş olsa da bu başvurunun nasıl ve ne şekilde yapılacağı ile hangi hallerde ücret talep edilebileceği noktasında akıllarda soru işaretleri bulunmaktaydı. Bu soru işaretlerini gidermesi ve veri sorumlusuna başvuru işlemi ile ilgili usul ve esasları belirlemek amacıyla Kişisel Verileri Koruma Kurumu tarafından düzenlenen "*Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ*" 10 Mart 2018 tarihli 30356 sayılı Resmi Gazete'de yayınlandı ve yayımı tarihinde yürürlüğe girdi⁴.

Tebliğin ilk dayanağını Kanun'un "*veri sorumlusuna başvuru*" başlıklı 13. maddesi oluşturmaktadır. Zira bu madde ile ilk kez veri sorumlusundan bahsedilmiş ancak bu başvurunun detaylandırılmaması ve ücret hususunun belirsiz olması daha sonra Kurum tarafından konuyla ilgili düzenlemeler yapılacağını göstermektedir. Ayrıca Kanun'un "*kurulun görev ve yetkileri*" başlıklı 22. maddesi de Tebliğe dayanak olmuştur. Buna göre Kurulun görev alanı ile ilgili ve veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak Kurul'un görev ve yetkileri arasındadır.

1. Başvuru Hakkı ve Usulü

Tebliğin "*başvuru hakkı*" başlıklı 4. maddesinde kişisel verisi işlenen gerçek kişilerin veri sorumlusuna başvuru hakkına sahip olduğunu ve ilgili kişilerin bu haktan faydalanabileceği belirtilmiştir. Maddede yer alan esas önemli nokta ise veri sorumlusuna yapılacak başvuruların Türkçe yapılması gerektiğinin hüküm altına alınmış olmasıdır. Bu husus veri sorumlusuna başvuru hakkının bir şartı olarak dile getirilmiştir. Öyleyse Türkçe yapılmayan başvurular dikkate alınmayacaktır.

Kişisel verisi işlenen gerçek kişilerin veri sorumlusuna başvuru hakkını kullanırken uyması gereken usul kuralları tebliğin "*başvuru usulü*" başlıklı 5. maddesiyle hüküm altına alınmıştır.

⁴ Tebliğ için bakınız: <http://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm>

Başvuru hakkının nasıl kullanılacağına belirsizliğinin giderilmesi açısından söz konusu madde oldukça önemlidir.

İlgili kişinin, Kanunun 11. maddesinde belirtilen hakları kapsamındaki taleplerini veri sorumlusuna nasıl iletmesi gerektiği konuyla ilgili en büyük soru işaretlerinden birini oluşturmaktaydı. Tebliğle bu soru işareti giderilmeye çalışılmış ve kullanılacak araçlar sayılmıştır. Buna göre ilgili kişi talebini;

- Yazılı olarak veya
- Kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle, başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama

vasıtasıyla veri sorumlusuna iletir.

Taleplerin hangi araçlar kullanılarak veri sorumlusuna iletileceği esasen tahmin edilmekle beraber bu araçların Kurum tarafından tek tek belirtilmesi özellikle ilgili kişinin hakkını etkin bir biçimde kullanması ve başvuru hakkının belirli olması açısından önemli ve yerindedir. Bu noktada en uygun yöntemin veri sorumlusunun başvuru hakkının amacına yönelik olarak yazılım veya uygulama geliştirilmesi olduğunu düşünmekteyim. Veri sorumlusunun web sitesinde konuya ilişkin ayrı bir sekme oluşturması başvuru hakkına ilişkin ihtiyaçları gidermek açısından en elverişli yöntem olarak görünmektedir, ancak ilgisiz kişilerin başvuru yapmasını önlemek için önceden elektronik posta adresleri kayıtlı olan, dolayısıyla kişisel verilerinin de kayıtlı olduğu ihtimal dahilinde olan kişilerle bu işlemin sınırlandırılması yerinde olacaktır. Aksi hali veri sorumlusu için altından kalkılması son derece güç bir yük oluşturur.

İlgili kişinin veri sorumlusuna başvuru hakkını hangi araçlarla kullanacağı tespit edildikten sonra bu başvurunun nasıl oluşturacağı ve başvuruda nelerin yer alacağı sayılmıştır. Buna göre başvuruda:

- Ad, soyad ve başvuru yazılı ise imza,
- Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası,
- Tebligata esas yerleşim yeri veya iş yeri adresi,
- Varsa bildirim esas elektronik posta adresi, telefon ve faks numarası,
- Talep konusu,

bulunmak zorundadır. Ayrıca konuya ilişkin bilgi ve belgeler varsa bunların da başvuruya eklenmesi gerekir.

Başvuru hakkının kullanılması ile ilgili diğer bir önemli nokta, veri sorumlusunun talepleri yerine getirmede bir süreye tabi olması sebebiyle bu başvurunun hangi tarihte yapılmış sayılacağına ilişkindir. Tebliğin 5. maddesi bu konuda da açıklama getirmiş ve yazılı başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarihin; diğer

yöntemlerle yapılan başvurularda ise başvurunun veri sorumlusuna ulaştığı tarihin başvuru tarihi olarak sayılacağı öngörülmüştür.

2. Başvuruya Cevap

Tebliğin 6. maddesi ilgili kişinin başvurusuna karşılık veri sorumlusunun bu başvuruya vereceği cevaba ilişkin olup; cevabın nasıl ve ne şekilde verileceğini düzenlemektedir. Kanun, başvuru hakkının usulünde olduğu gibi başvuruya cevap noktasında da daha genel kurallar belirtmiştir.

Tebliğin başvuruya cevap noktasında en dikkat çeken kısmı, veri sorumlusunun Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbiri almakla yükümlü olmasıdır. Burada ifade edilmek istenen; veri sorumlusunun verisi işlenen gerçek kişinin başvuru hakkını en etkin biçimde kullanmasını sağlayacak her türlü tedbiri alması ve bu hakkın kullanımını engelleyecek herhangi bir faaliyette bulunmaması gerektiğidir. Bu kapsamda veri sorumlusu, ilgili kişinin taleplerini kendisine ileteceği araçları bu hakkın kullanılmasını engelleyecek kadar zorlaştırmamak ve ilgili kişinin taleplerini bildirmede sıkıntı ve zorluk yaşamamasını sağlamak durumundadır.

Bununla birlikte cümlede geçen “*hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak*” ifadesinden veri sorumlusunun, ilgili kişi tarafından başvuru hakkının kullanılıp bu başvuruya kendisi tarafından cevap verilmesine kadarki süreç içerisinde de gerekli bütün tedbirleri almakla yükümlü olduğu anlaşılmaktadır. İlgili kişinin yalnızca taleplerini iletmesiyle veri sorumlusunun yükümlülüğü sona ermeyecektir.

Veri sorumlusu kendisine gelen başvuruyu kabul veya reddetme hakkına sahiptir. Ancak başvuruyu reddeden veri sorumlusu red kararının gerekçesini açıklamak zorundadır. Bu husus aynı şekilde Kanun’da da yer almaktaydı.

Veri sorumlusu, başvuruya vereceği cevabı ilgili kişiye yazılı veya elektronik ortamda bildirebilir. Burada başvuru ve cevabın aynı yolla yapılması gibi bir gereklilikten söz edilmediğinden bu konuda bir ayırım olduğunu düşünmüyorum. Örneğin, veri sorumlusu kendisine elektronik ortamda yapılan bir başvuruyu, hakkın kullanılmasını engellemek ve gerekli bütün teknik ve idari tedbirleri almak kaydıyla ilgili kişinin adresine yapacağı yazılı bir bildirimle cevaplayabilecektir.

Veri sorumlusunun vereceği cevap yazısı;

- Veri sorumlusu veya temsilcisine ait bilgileri,
- Başvuru sahibinin; adı ve soyadını, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarasını, yabancılar için uyruğunu, pasaport numarasını veya varsa kimlik numarasını, tebligata esas yerleşim yeri veya iş yeri adresini, varsa bildirim esas elektronik posta adresini, telefon ve faks numarasını,
- Talep konusunu,
- Veri sorumlusunun başvuruya ilişkin açıklamalarını,

içermek zorundadır.

Cevap yazısında bulunması gereken ifadelerin maddede tek tek sayılması ve bunun bir zorunluluk olarak işaret edilmesinden, veri sorumlusunun belirtilen hususlardan herhangi birini içermeyen cevap yazısının hiç cevap verilmemiş sayılacağına anlaşılmaması gerektiğini düşünüyorum. Ayrıca cevap yazısında, ilgili kişiye başvuru hakkının ruhuna ve amacına uygun cevap verebilmek için maddede sayılanlardan başka bilgilerin de yer alması gerektiği takdirde, veri sorumlusunun gerekli olan diğer bilgi veya bilgilerin de eklenmesi noktasında yükümlü olduğu açıktır.

Veri sorumlusunun başvuruya cevap verebilmek ve talepleri yerine getirmek için tabi olduğu süre Kanun ile paralel bir biçimde talebin niteliğine göre en kısa süre ve en geç otuz gün olarak belirlenmiştir. Veri sorumlusu bu süreler içerisinde ilgili kişinin taleplerini sonuçlandırmalıdır. Veri sorumlusunun bu yükümlülüğünü ücretsiz olarak yerine getirmesi esas olmakla beraber; işlemin ayrıca maliyet gerektirmesi halinde ilgili kişiden ücret talep edilebilecektir. Ancak işlem ayrıca bir maliyet gerektirmiş olsa dahi, ilgili kişinin başvurusu veri sorumlusunun hatasından kaynaklanmışsa talep edilen ücret kendisine geri verilecektir. Böylece veri sorumlusunun hatasından kaynaklanan başvuruların maliyetine de kendisinin katlanması sağlanmıştır.

3. Ücret

Kanunda ilgili kişinin başvuru hakkını kullanması sonucu veri sorumlusunun cevap vermesi işleminin ayrıca bir maliyet gerektirmesi halinde ilgili kişiden ücret talep edilebileceği hüküm altına alınmıştır. Ancak bu ücretin nasıl ve neye göre belirleneceği bilinmemekteydi. Tebliğin ücret başlıklı 7. maddesiyle bu konuda yaşanan belirsizlikler giderilmeye çalışılmıştır. Cevabın ücretlendirilmesinde yazılı veya kayıt ortamında verilmesine göre ikili bir ayırım yapılmıştır. Buna göre;

- Yazılı olarak verilen cevaplarda; on sayfaya kadar ücret alınmayacak ancak on sayfanın üzerindeki her bir sayfa için 1 TL işlem ücreti alınabilecektir.
- CD, flash bellek gibi bir kayıt ortamında verilen cevaplarda ise; veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemeyecektir.

Kurum tarafından belirlenen ücretler oldukça makul olup; esasen cevabın yazılacağı veya bulunacağı ortamın maliyetine göre yapılmıştır. Ancak veri sorumlusunun ilgili kişinin taleplerini yerine getirebilmek için gerçekleştirmek zorunda olduğu faaliyetler kapsamında ücret talep edip edemeyeceği, edecekse bunun nasıl belirleneceği hala açıklanmış değildir. Bu konuya da açıklık getirilmesi gerektiğini düşünüyorum.

Bu noktada değinmek istediğim bir diğer husus veri sorumlusunun kötü niyetli başvurulara karşı ücret kapsamında önlem alıp alamayacağına ilişkindir. Başvuru hakkına sahip ilgili kişi, her ne kadar veri sorumlusu tarafından verisi işleniyor da olsa bu hakkını kötü niyetli bir biçimde kullanabilecektir. Dolayısıyla ilgili kişinin kişisel verilerini korumak ve kişisel verileri üzerinde hakimiyetini sağlamak amacıyla öngörülen başvuru hakkının suiistimal edilmesi de

muhtemeldir. Böyle bir tehlike karşısında veri sorumlusunun kendisine yapılacak başvurularda ilgili kişiden makul bir ücret talep edilmesinin çözüm olabileceğini düşünüyorum. Ancak bu ücret ilgili kişinin hakkını kullanmasını zorlaştıracak oranda olmamalı ve makul olmalıdır. Ayrıca veri sorumlusunun başvuruya cevap verdikten sonra ilgili kişinin başvuru hakkını kullanmada gerçekten menfaati olduğu anlaşılıyorsa alınan ücret geri verilebilir. İlgili kişinin hangi durumlarda menfaatinin olduğunun kabul edileceği de ayrı bir soru olarak düşünülmelidir. Zira ilgili kişinin başvuru hakkını sağlamak adına veri sorumlusunun zor durumda bırakılması da hukuka uygun bir yaklaşım olmayacaktır. Dolayısıyla veri sorumlusu ve ilgili kişinin başvuru hakkını kullanmasında menfaat dengeleri gözetilmeli ve en uygun çözümler aranmalıdır.

Sonuç

İlgili kişinin veri sorumlusuna başvuru hakkına ilişkin usul ve esasları belirlemek amacıyla düzenlenen “*Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ*” hükümleri, başvuru hakkı ile ilgili akıllarda yer alan birçok soruya cevap vermiştir. İlgili kişinin başvuru hakkını kullanırken ve veri sorumlusunun başvuruya cevap verirken uyacağı kurallar detaylı bir biçimde belirtilmiştir. Ayrıca ücret konusu da başvuru hakkı ile ilgili oldukça konuşulan ve merak edilen bir konuydu. Tebliğ, bu konuda da bazı noktalara açıklık getirmiş olsa da yukarıda da belirttiğim üzere birtakım soru işaretleri devam etmektedir. Bu belirsizliklerin de zamanla yapılacak düzenlemelerle giderileceğini umuyorum.

III. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul Ve Esaslar Hakkında Tebliğ

Veri sorumlusunun aydınlatma yükümlülüğü kişisel verilerin etkin bir biçimde korunması adına oldukça önemli bir noktadır, nitekim bu husus Kanun’un 10. maddesi ile de veri sorumlusunun yükümlülükleri altında düzenlenmiş bulunmaktaydı.

Kanun’un bu yükümlülüğü genel hatlarıyla düzenlemiş olması sebebiyle birçok noktada belirsizlikler bulunmaktaydı. Bu belirsizlikleri gidermek ve Kanununun 10. maddesi uyarınca veri sorumluları veya yetkilendirdiği kişilerce yerine getirilmesi gereken aydınlatma yükümlülüğü kapsamında uyulacak usul ve esasları belirlemek amacıyla Kişisel Verilerin Korunması Kurumu tarafından düzenlenen “*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*” 10 Mart 2018 tarihli 30356 sayılı Resmi Gazete’de yayınlandı⁵. Bu tebliğ de yukarıda açıkladığım veri sorumlusuna başvuru konulu Tebliğ ile aynı günde yayınlandı ve yine yayımı tarihinde yürürlüğe girecek şekilde belirlendi.

Tebliğin düzenleme konusunun Kanun’un 10. maddesine ilişkin ve söz konusu maddenin uygulanmasını sağlayacak ve kolaylaştıracak nitelikte olması sebebiyle Tebliğin ilk dayanağını Kanun’un 10. maddesinden aldığını söylemek mümkündür. Ayrıca Kanun’un 22. maddesinde Kurulun görev alanı ile ilgili ve veri sorumlusunun ve temsilcisinin görev, yetki ve

⁵ **Tebliğ için bakınız:** <http://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm>

sorumluluklarına ilişkin düzenleyici işlem yapmak Kurul'un görev ve yetkileri arasında sayılmıştır.

1. Aydınlatma Yükümlülüğünün Kapsamı

Tebliğin “*aydınlatma yükümlülüğünün kapsamı*” başlıklı 4. maddesiyle Kanun ile veri sorumlusu tarafından ilgili kişiye yönelik olarak yapılması öngörülen aydınlatma yükümlülüğü açıklanmaya çalışılmıştır. Maddeyle ilk olarak Kanun ile de paralel biçimde; kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce, ilgili kişilerin bilgilendirilmesi gerektiği belirtilmiştir. Veri sorumluları veya yetkilendirdiği kişilerce yapılacak bilgilendirmenin asgari olarak aşağıdaki konuları içermesi gerekir:

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- İlgili kişinin Kanunun 11 inci maddesinde sayılan diğer hakları.

Tebliğin söz konusu maddesi esasen büyük ölçüde Kanun'un 10. maddesini tekrar niteliğindedir. Aydınlatma yükümlülüğünün ne anlama geldiği, yükümlülüğü kimlerin yerine getireceği, bildirimin hangi konuları içermesi gerektiği noktasında hiçbir fark görünmemektedir. Ancak Tebliğde Kanun'dan farklı olarak aydınlatma yükümlülüğü kapsamında yapılacak bildirimin “*asgari*” olarak sayılan konuları içermesi gerektiği belirtilmiştir. Buradan anlaşılması gereken maddede sayılan hususlardan herhangi birini içermeyen bildirimin geçersiz olacaktır. Ayrıca aydınlatma yükümlülüğünün yerine getirilmiş olmasının sayılması için ilgili kişinin, maddede sayılan konulardan başka konularda da bilgilendirilmesi gerekiyorsa bu kapsamda da bilgilendirilmesi gerekecektir. Bu kurallara uygun olarak yapılmayan bilgilendirme aydınlatma yükümlülüğünün yerine getirilmemesinin sonuçlarını doğurmalıdır.

2. Aydınlatma Yükümlülüğüne İlişkin Usul ve Esaslar

Tebliğin “*usul ve esaslar*” başlıklı 5. maddesi aydınlatma yükümlülüğü konusunda yenilikler getirmekte ve özel hükümler içermektedir. Bu açıdan oldukça önemli olan madde, detaylı olarak incelenmeli ve eksik veya tartışmalı noktalar net bir biçimde ifade edilmelidir.

Maddeyle ilk olarak aydınlatma yükümlülüğünü yerine getirmekle sorumlu kişiler tarafından bu yükümlülüğün hangi vasıtalarla yerine getirileceği açıklanmıştır. Buna göre; veri sorumlusu ya da yetkilendirdiği kişi tarafından bilgilendirme yapılırken sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortamlardan duruma uygun olanlardan herhangi bir yol tercih edilebilir. Bu bilgilendirme yerine getirilirken uyulacak usul ve esaslar ise aşağıdaki gibidir:

- *İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir:*

Aydınlatma yükümlülüğünün yerine getirilmesinde kişisel verilerin işlenme şartları bakımından herhangi bir ayrıma gidilmemiştir. Kişisel verilerin işlenmesi ilgili kişinin açık rızasına dayansa veya Kanunda belirtilen diğer işleme şartlarından biri mevcut bulunsada her durumda veri sahibi her veri işleme faaliyeti ile ilgili olarak bilgilendirilmelidir. Bir faaliyet kapsamında birden fazla kere veri işlenmesi gerektiği takdirde bilgilendirmenin sadece faaliyet kapsamında yapılmasının yeterli olduğu her veri işleme öncesinde aydınlatma yükümlülüğünün bulunmadığı açıktır.

- *Kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir:*

Bu husus esasen Kanun'un aydınlatma yükümlülüğünün kişisel verilerin hangi amaçla işleneceği veya aktarılacağı konularını içermesi gerektiğini düzenleyen maddesinden de anlaşılmaktadır. Ancak Tebliğ ile açıkça belirtilmesi yerindedir. Buna göre daha önce belli bir amaç için aydınlatma yükümlülüğünü yerine getiren veri sorumlusu, işleme veya aktarma faaliyetlerini aynı veri üzerinde gerçekleştirecek dahi olsa ilgili kişiyi değişen amaç kapsamında da bilgilendirmelidir. Bireyin, kişisel verisi üzerinde hakimiyet sahibi olması ilkesi gereğince kişisel verisinin hangi amaçla işlendiği veya aktarıldığını bilmeye hakkı vardır.

- *Veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa, aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir:*

Öncelikle bu hükmün oldukça belirsiz olduğunu ve sözünden çıkarılan anlamı kastediyor olması halinde ciddi yükümlülükler içerdiğini belirtmeliyim.

İlk olarak birim kavramından ne anlaşılması gerektiği açıklığa kavuşturulmalıdır. Zira bu kavramın kişisel verilerin korunması mevzuatı ile gündeme gelmiş olması sebebiyle net bir tanımı da bulunmamaktadır. Kavramdan genel olarak tüzel kişiliği haiz şirketlerin organizasyonel yapısı içerisindeki insan kaynakları, satış ve pazarlama, üretim, maliye gibi farklı farklı departmanların anlaşılması gerektiği en doğru çözüm olarak görünmektedir.

Hüküm ile veri sorumlusu konumunda bulunan tüzel kişiliğin, dolayısıyla şirketlerin yukarıda belirttiğim farklı birimlerinde kişisel verilerin işlenmesi halinde aydınlatma yükümlülüğünün nasıl yerine getirileceği belirlenmeye çalışılmıştır. Hükümün dilbilgisi olarak anlamı tespit edilmeye çalışıldığında özellikle “nezdinde” ifadesinden dolayı her birimin aydınlatma yükümlülüğünü ayrı ayrı yerine getirileceği gibi bir anlam da çıkabilmektedir. Ancak burada kastedilenin, tüzel kişilik bünyesinde bulunan farklı birimlerin kişisel verileri ancak farklı amaçlarla işlemesi halinde birbirlerinden ayrı olarak ilgili kişiyi bilgilendirmeleri gerektiği olduğunu düşünüyorum. Örneğin, işçinin kişisel verilerini İş Kanunu'ndan doğan yükümlülüklerini yerine getirebilmek amacıyla işleyecek olan insan kaynakları biriminin, işçiyi bu kapsamda bilgilendirmesi yeterli olacaktır. Ancak bu bilgilendirme, işçinin verileri kendisine reklam yapılması amacıyla kullanılması için geçerli bir aydınlatma anlamına gelemez. İşçinin verileri reklam yapılması amacıyla işlenecekse bu noktada aydınlatma yükümlülüğünün pazarlama birimi tarafından da ayrıca yapılması gerekecektir. Böylece farklı amaçlarla kişisel veri işleyen farklı birimler aynı kişiyi ayrı ayrı bilgilendirmek durumundadır. Bu şekilde anlaşılması halinde Kanun'un ve kişisel verilerin korunmasının özüne uygun bir

aydınlatma yükümlülüğü söz konusudur. Aksi takdirde bir yükümlülük, ticaret hayatını işlemez hale getirecek kadar olumsuz sonuçlar doğurabilecektir.

Kanun ve kişisel verilerin korunmasına ilişkin diğer düzenlemeler beraber değerlendirildiğinde böyle bir sonuç çıkarılabilecekse de cümlenin ifadesi belirsizlik içerdiğinden tartışmalara açıktır. Bu sebeple Kurul tarafından bu yükümlülüğe ilişkin açıklama getirilmesi gerektiği kanaatindeyim.

- *Sicile kayıt yükümlülüğünün bulunması durumunda, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır:*

Kanun ve Veri Sorumluları Sicili Hakkında Yönetmelik ile veri sorumluları siciline kayıt olmakla yükümlü bulunan veri sorumlularının, kayıt yükümlülüğünü yerine getirirken kayıt bildiriminin hangi bilgileri içermesi gerektiği belirlenmiştir. Kişisel verinin hangi amaçla işleneceği, alınan tedbirler, işlenmesi gereken azami süre gibi bilgiler kayıt bildiriminde yer almak zorundadır. Veri sorumlusu aydınlatma yükümlülüğünü yerine getirirken ilgili kişiye yapacağı bildirimde de verinin işleme amacını açıklamak durumundadır. Hüküm ile sicile bildirilen bilgilerle ilgili kişiye yapılan bildirim çerçevesinde veri sahibine verilen bilgilerin birbiriyle çelişmemesi ve uyumlu olması gerektiği belirtilmiştir.

- *Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir:*
Bu husus, veri sorumlusunun, ilgili kişinin talebi olmadığı bahanesine dayanarak aydınlatma yükümlülüğünden kurtulmasını engelleyecek nitelikte olduğundan oldukça önemlidir. Kişisel verisi işlenen gerçek kişinin veri sorumlusu tarafından bilgilendirilmesi için bunu ayrıca ve açıkça talep etmek zorunda değildir, veriyi işleyecek olan veri sorumlusu bu işleme faaliyeti öncesinde aydınlatma yükümlülüğünü kendiliğinden yerine getirmelidir.
- *Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir:*
Aydınlatma yükümlülüğünü kendiliğinden yerine getirmekle yükümlü olan veri sorumlusu bu bilgilendirmeyi yaptığını da yine kendisi ispat etmelidir. Bu noktada veri sorumlusu kötü niyetli ilgili kişilere karşı kendisini korumak amacıyla gerekli tedbirleri almalıdır. Örneğin ilgili kişinin aydınlatma yükümlülüğünün yerine getirildiğine dair beyanının yazılı veya elektronik ortamda herhangi bir biçimde alınması veri sorumlusu açısından ispat kolaylığı yaratacaktır. Sadece sözlü olarak yapılan bilgilendirmenin, daha sonradan ilgili kişi tarafından inkâr edilmesi ve ispatının gerekmesi ihtimalinde veri sorumlusu büyük tehlikelerle karşı karşıya kalacaktır.
- *Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir:*

Bu hüküm ile esas belirtilmek istenen açık rıza şartının aydınlatma yükümlülüğünün yerine getirilmesi noktasında herhangi bir istisna teşkil etmediğidir. Kişisel verisi işlenen ilgili kişinin bu işleme faaliyetine yönelik olarak Kanun'a uygun açık rızası bulunsa dahi veri sorumlusunun aydınlatma yükümlülüğü devam etmektedir. Veri sorumlusu açık rıza alınması ve bilgilendirme yapılması yükümlülüklerini birbirinden bağımsız bir biçimde yerine getirmelidir.

- *Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelerle yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır.*
- *Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirimin anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir:*

Burada veri sorumlusunun dikkatli olması gerekir. Zira kasıtlı ve kötü niyetli bir biçimde yapmamış olsa da kişilerin anlayamayacağı kadar karmaşık bir dil kullanmak aydınlatma yükümlülüğünün yerine getirilmemesinin sonuçlarını doğurabilir. Bilgilendirme olabildiğince açık ve sade bir dille yapılmalıdır.

- *Kanunun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan “hukuki sebep” ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanunun 5 ve 6ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir:*

Tartışmaların yoğunlaştığı bir diğer nokta da bu hükümde yer almaktadır. Akıllarda oluşabilecek soru işaretlerine cevap verebilmek adına hükmün detaylı incelemesinde bulunacağım.

Kanun’un aydınlatma yükümlülüğünün düzenlendiği 10. maddesinde, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişinin, ilgili kişilere hangi konularda bilgilendirme yapması gerektiği tek tek sayılmış ve (ç) bendinde, “*kişisel veri toplamanın yöntemi ve hukuki sebebi*” de ilgili kişilere verilmesi gereken bilgiler arasında sayılmıştır.

Söz konusu hükümde Kanun’un yukarıda belirttiğim bendinde yer alan “*hukuki sebep*” kavramından anlaşılması gerekenin, kişisel verilerin Kanun’un 5. ve 6. maddelerinde belirtilen kişisel verilerin işleme şartlarından hangisine dayanılarak işlendiği olduğu belirtilmiştir. Aydınlatma yükümlülüğü kapsamında yapılacak bilgilendirmede Kanun’un 5. ve 6. maddelerinde yer alan kişisel veri işleme şartlarından hangisine dayanılarak kişisel veri işlendiği açıkça belirtilecek ve böylece ilgili kişi, kişisel verisinin işlenmesindeki hukuki sebep konusunda bilgilendirilmiş olacaktır.

Burada akıllara, Kanun’un açık rıza aranmaksızın kişisel verilerin işlenebileceği istisnaları düzenleyen 5. maddesinin 2. fıkrasında yer alan (a) bendi gelmektedir. İlgili bentte “*kanunlarda açıkça öngörülmesi*” istisna hali olarak sayıldığına göre sadece bu bendin belirtilmesi aydınlatma yükümlülüğünde ilgili kişiye hukuki sebep bilgisinin verilmiş olduğu anlamına gelip gelemeyeceği noktasında belirsizlik söz konusudur.

Kanun’un ilgili hükümleri ve Tebliğ hükmünün dilbilgisi olarak anlamı dikkate alındığında böyle bir anlam çıkarılabilecekse de yalnızca “*kanunlarda açıkça öngörülmesi*” kavramının kişisel verilerin işlenmesinde yerine getirilmesi gereken aydınlatma yükümlülüğünde yer alması gereken hukuki sebep bilgisi niteliğinde olamayacağı kanaatindeyim. Söz konusu kavram hukuki sebepten çok; hukuki sebebin dayanağı niteliğinde değerlendirilmelidir. Dolayısıyla hukuki sebep olarak Kanun’un 5. maddesinin 2-a bendinde yer alan ifade değil; kanunda açıkça öngörülen hüküm hangisiyse, o hüküm kişisel verinin işlenmesinin hukuki sebebi olarak belirlenmeli ve

ilgili kişiye o hükmün bilgisi verilmelidir. Nitekim tebliğ hükmünün son cümlesinde de hangi hukuki sebebe dayanıldığına açıkça belirtilmesinin aranması bu düşünceyi kuvvetlendirmektedir. Aksi yönde bir yaklaşım halinde Kanun'un özü ve amacı dikkate alınmadan sadece belirli kavramların dikkate alınarak yapılan bir yorum söz konusu olacaktır.

- *Aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları belirtilmelidir:*

Burada Kanun'un veri sorumlusunun ilgili kişiye vermesi gereken bilgilerin düzenlendiği hükmü tekrar edilmiştir.

- *Aydınlatma yükümlülüğü kapsamında kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği açık bir şekilde belirtilmelidir:*

Aydınlatma yükümlülüğünün kişisel verilerin hangi amaçlarla işleneceği ve aktarılacağından başka veri sorumlusu tarafından hangi yollarla elde edildiği bilgisini de içermesi gerekir.

- *Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir:*

Veri sorumlusu bilgilendirmeyi yaparken ilgili kişiye belirtmesi gereken hususların yanı sıra olmayan yanlış veya yanıltıcı bilgilere yer vermemesi gerekir. Ayrıca belirtmesi gereken bilgilerde eksiklik ve yanlışlık olmamalıdır. Bu husus aydınlatma yükümlülüğüne ilişkin hükümlerden zaten anlaşılmaktadır.

3. Kişisel Verilerin İlgili Kişiden Elde Edilmemesi Halinde Aydınlatma Yükümlülüğü

Tebliğin 6. maddesinde aydınlatma yükümlülüğüne konu olan kişisel verilerin ilgili kişi haricinde üçüncü bir kişiden elde edilmesi halinde bilgilendirmenin nasıl yapılacağı düzenlenmiştir. Buna göre:

- İlk olarak veri sorumlusu, elde edilen kişisel verinin sahibini elde edildiği andan itibaren makul bir süre içerisinde bilgilendirmekle yükümlüdür.
- Kişisel verisi kendisi dışında elde edilen ilgili kişiyle iletişim kurulabilmesi halinde; veri sorumlusu, bu kişiyle ilk iletişim kurduğu esnada aydınlatma yükümlülüğünü yerine getirmelidir.
- İlgili kişi haricinde üçüncü bir kişi tarafından elde edilen kişisel verinin aktarımı yapılacaksa; bu aktarıma ilişkin aydınlatma yükümlülüğü en geç aktarımın yapılacağı esnada yerine getirilmelidir. Hükümden ilgili kişiyle iletişim kurulamaması halinde aktarımın hiçbir şekilde yapılamayacağı anlaşılmaktadır.

Sonuç

Kanun'un 10. maddesiyle veri sorumlusuna yükletilen aydınlatma yükümlülüğü kişisel verilerin korunması açısından büyük önem arz etmektedir. İlgili kişinin kişisel verilerinin hukuka uygun olarak işlendiği veya aktarıldığından bahsedebilmek için bilgilendirme yapılması olmazsa olmaz niteliktedir. Aksi takdirde veri sahibinin verisi üzerinde herhangi bir hakimiyetinden bahsetmek de mümkün olmayacaktır.

“Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ” maddeleri, aydınlatma yükümlülüğünü bütün hatlarıyla belirlemesi bakımından konuya büyük ölçüde açıklık getirmiş ve birçok soruyu gidermiştir. Bununla birlikte yukarıda detaylı bir biçimde açıkladığım üzere cümle ifadelerinden çıkarılabilecek Kanun’un ve kişisel verilerin özüne aykırı ve amacını aşan anlamların bulunduğu noktalarda açıklama getirilmesi gerektiğini düşünüyorum.