

Veri İhlali Bildiriminde Bulunması Gereken Unsurlar ve Bildirim Esas ve Usulleri: KVK Kurulu’nun 18 Eylül 2019 Tarihli, 2019/271 Sayılı ve 24 Ocak 2019 Tarihli, 2019/10 Sayılı Kararlarının Değerlendirilmesi

Doç. Dr. Murat Volkan Dülger*

Giriş

Veri ihlalleri kadar veri ihlali bildirimleri de son dönemde önem kazandı. Gerçekten de veri sorumlusunun yalnızca veri ihlaliinde bulunması değil, bu ihlalleri bildirmemesi de Kişisel Verilerin Korunması Kanunu’nda (KVKK) 12. maddede düzenlenen veri güvenliğine ilişkin yükümlülükleri ihlal ettiği anlamına gelmekte. Bu yükümlülüğün ihlal edilip edilmediği de oldukça açık olduğundan (Kişisel Verileri Koruma Kurulu’nun veri sorumlusunca herhangi bir bildirim olmadan, re’sen ya da şikâyet üzerine vermiş olduğu kararlar), veri ihlali ile birlikte, ihlal bildiriminin yapılmamış olması nedeniyle idari para cezalarına hükmedildiği pek çok karara rastlamaktayız.

Açıkçası bildirim ihlali için hükmedilen para cezaları da azımsanacak düzeyde değil. Facebook hakkında 450.000 TL (18.09.2019 tarih ve 2019/269 sayılı karar) ve 550.000 TL (11.04.2019 tarih ve 2019/104 sayılı karar), Marriott hakkında 350.000 TL (16.05.2019 tarih ve 2019/143 sayılı karar), Cathay Pasific Airway ve Clickbus Seyahat hakkında 100.000 TL’lik (16.05.2019 tarih ve 2019/144 sayılı karar ve 16.05.2019 tarih ve 2019/141 sayılı karar) meblağlara yalnızca ihlal bildiriminde bulunulmadığından hükmedilmesi, zannediyorum bir önceki cümlemde ifade ettiğim hususu ve Kişisel Verileri Koruma Kurulu’nun (Kurul) bu konudaki kararlılığını ortaya koyuyor. Bu etki, son dönemde pek çok veri ihlal bildiriminin de Kurula iletilmesini sağladı ve bir kısmı Kurum web sitesi aracılığıyla kamuoyuna duyuruldu. Microsoft, İş Bankası, Denizbank, TEB, ING Bank ve Zynga Games bir çırpıda aklıma gelen veri ihlal bildiriminde bulunan veri sorumluları. Kurulun veri ihlal bildiriminin yapılmaması durumunda 18. maddeyi işletmesi ve idari para cezalarına hükmetmesindeki kararlılığı yapılacak veri ihlali bildirimlerinin sayısını arttıracaktır.

Öte yandan, veri ihlali bildiri Kurulun üzerinde durmuş olduğu bir yükümlülük olmasına rağmen maalesef yasanın üzerinde pek durduğu bir kavram değil. Yasa m. 12/5 ile *“İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.”* hükmüne yer vermiş. Ancak bunun dışında, herhangi açıklayıcı bir düzenlemeye yer vermemiştir. Bu durum, detaylarına aşağıda değineceğim üzere, önemli bir

* Akademisyen / Avukat.

eksiklik. Kurul ise verdiği kararlar ile veri ihlal bildirimi yükümlülüğünü açıklamaya ve belirsizlikleri gidermeye çalışmakta. Bu kısa makalemde de Kurulun bu konuda verdiği ve 15 Ekim 2019 tarihinde yayınladığı kararı konu edeceğim. Bunun yanında, tamamlayıcısı olarak görülebilecek, 24 Ocak 2019 tarihli karara da değinmeye çalışacağım.

Kurulun 18 Eylül 2019 tarihinde yayınlamış olduğu kararında, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri ilgisine ve Kurula yapılacak bildirimde olması gereken asgari unsurlar konu edilmiştir. Kararda veri ihlali bildiriminin önemi üzerinde durulmuş, KVKK'nın mevcut düzenlemesine yer verilerek bildirimde bulunacak asgari unsurlar belirtilmiştir.

Kişisel verilerin ihlali bildiriminin önemi ve kararda açıklanan bu bildirimin sağlaması gereken asgari unsurların incelenmesi amacıyla, öncelikle KVKK ve sonrasında GDPR düzenlemeleri üzerinde durarak, konuyu açıklamaya çalışacağım. Kurulun 2019/271 ve 2019/10 sayılı söz konusu kararlarını bu bilgiler ışığında değerlendireceğim.

I. KVKK Uyarınca Yapılacak Veri İhlal Bildirimi ve Şartları

KVKK'nın 12/1 maddesine göre veri sorumlusu; kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak zorundadır. Teknik tedbirler, siber güvenliğin sağlanması, kişisel veri güvenliğinin takibi, kişisel veri içeren ortamların güvenliğinin sağlanması, kişisel verilerin bulutta depolanması, bilgi teknolojileri sistemleri tedarigi, geliştirme ve bakımı kişisel verilerin yedeklenmesidir. İdari tedbirler ise, mevcut risk ve tehditlerin belirlenmesi, çalışanların eğitilmesi ve farkındalık çalışmaları, kişisel veri güvenliği politikalarının ve prosedürlerinin belirlenmesi, kişisel verilerin mümkün olduğunca azaltılması ve veri işleyenler ile ilişkilerin yönetimini kapsayan tedbirlerdir.

İhlallere ilişkin olarak tedbir alınmasının yanında yeri sorumlusunun diğer bir yükümlülüğü veri ihlalinin gerçekleşmesi durumunda Kurula ve veri ilgisine ihlalin bildirilmesidir. 6698 sayılı Kanun'da işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildirilmesi gerektiği düzenlenmiştir. Hatta Kurul, bir kararında veri sorumlusunun gerçekleşen veri ihlalinin **ilgili kişilere 17 ay, Kurula ise 10 aylık gecikmeyle** bildirmesinin Kanunda belirtilen ***“en kısa süre”*** yi aşan bir süre olduğuna karar vermiştir.

Ancak veri ihlalinin nasıl yapılacağı ve içeriğinin ne olacağı gibi önemli ve yüksek miktarlarda idari para cezası öngörülen bir konu hakkında yasada düzenleme olmadığı gibi Kurul'un da 24.01.2019 tarih ve 2019/10 sayılı ve 18.09.2019 tarih ve 2019/271 sayılı kararlarına kadar bir açıklık yoktu.

Kanun yalnızca yükümlülüğün bulunduğu (m. 12/5) ve yükümlülüğe aykırılığın yaptırımını (m. 18/1-b) düzenlemekte ancak veri ihlali bildirimine ilişkin müstakil bir hükme yer vermemektedir. Kurul, 2019/10 sayılı kararında “en kısa sürede” ifadesinin 72 saat olarak yorumlanmasına karar vermiş; veri ihlali bildiriminin şekline, bu bildirimin yapılacağı forma ve veri ihlali müdahale planı kavramına yer vermiştir. Bu makalenin konusunu oluşturan 2019/271 sayılı kararında ise veri ihlali bildiriminde bulunması gereken asgari unsurları açıklığa kavuşturmuştur.

II. GDPR Uyarınca Yapılacak Veri İhlal Bildirimi ve Şartları

Kişisel veri ihlalinin, gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir risk oluşturduğu hallerde, veri sorumlusu kişisel veri ihlalinin ivedilikle veri ilgisine iletmekle yükümlüdür (GDPR, m. 34/1). Bir kişisel veri ihlali olması durumunda, veri kontrolörü ihlalden haberdar olduğu andan itibaren en geç 72 saat içinde, kişisel veri ihlalinin denetim makamına bildirmekle yükümlüdür (GDPR, m. 33/1). Yapılan veri ihlali bildiriminde aşağıda sayılan unsurlar yer almalıdır (GDPR, m. 33/3):

- Veri ilgilisi, veri kategorileri ve sayısına ilişkin açıklamaların yer aldığı veri ihlalinin niteliği açıklanmalıdır.
- Veri koruma görevlisi (Data Protection Officer) veya daha fazla bilginin elde edilebileceği diğer irtibat noktasına ilişkin isim ve gerekli bilgiler sağlanmalıdır.
- Kişisel veri ihlalinin olası sonuçları açıklanmalıdır.
- Veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik alınan/önerilen tedbirler açıklanmalıdır.

Bu bilgilerin aynı zamanda sağlanmasının mümkün olmadığı durumlarda, bilgiler ek bir gecikme olmaksızın, aşamalı olarak da sağlanabilecektir (GDPR, m. 33/4).

Görüldüğü üzere, KVKK'nın aksine, GDPR'da veri ihlalinin olması durumunda veri ilgisine yapılacak bildirimde yer alacak asgari unsurlar sayılmış ve ihlal bildiriminin yapılmasının istisnaları düzenlenmiştir. GDPR m. 34'teki atfa göre, veri ihlalinin gerçekleşmesi durumunda veri ilgisine yapılacak bildirimde veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka

bir temas noktasının isim ve irtibat bilgileri iletilir; kişisel veri ihlalinin olası sonuçları; uygun olduğu hallerde, kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler de dahil olmak üzere kişisel veri ihlalinin ele alınması için veri sorumlusu tarafından alınan veya alınması önerilen tedbirler açık ve sade bir dille açıklanır.

Ancak kimi durumlarda veri sorumlusu tarafından ilgiliye konuya ilişkin bildirim yapılmayabilir. Bunun için veri sorumlusunun uygun teknik ve düzenlemeye ilişkin koruma tedbirleri uygulaması ve kişisel verileri bu verilere erişim yetkisi bulunmayan herkese okunamaz hale getiren şifreleme gibi tedbirler başta olmak üzere bu tedbirlerin kişisel veri ihlalden etkilenen kişisel verilere uygulanmış olması veya veri ilgisinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alması ya da bildirimin ölçsüz bir çaba gerektirecek nitelikte olması gereklidir. Henüz bildirimin veri sorumlusu tarafından gerçekleştirilmediği durumda dahi kurum tarafından bildirim yapılması şartı getirilebilir veya bildirim yapmanın istisnalarından birinin yerine getirilmesini isteyebilir.

III. Kurulun 18 Eylül 2019 Tarihli, 2019/271 Sayılı Kararı ve 24 Ocak 2019 Tarihli, 2019/10 Sayılı Kararı

KVKK'da veri ihlal bildiriminin ne şekilde olacağı, bu bildirimde hangi unsurlara yer verileceğinin düzenlenmemesi, uygulamada ihlal bildirimini gerçekleştirmek isteyen veri sorumlusunun kafasında soru işaretleri yaratmaktaydı. Aynı zamanda bu durum ihlalden etkilenen kişiler bakımından da sorun yaratmaktaydı. Çünkü veri ilgililerine bilgi verirken veri sorumluları çekimser bir tutum gösteriyorlardı. Ancak veri ilgilisi kişiler, kişisel verileri hukuka aykırı yollarla başkaları tarafından elde edilmesinde bu ihlalin yaratabileceği olumsuz sonuçların bir an önce önüne geçilmesi ve en aza indirilmesine imkân verecek önlemler alınmasını isteme hakkına sahip olmalıdır.

Kurulun söz konusu kararına göre, veri sorumlusu, veri ihlali gerçekleştiğinde bunu ihlalden etkilenen kişilere ve Kurula açık ve sade bir dille bildirirken aşağıdaki unsurlara değinmelidir:

- İhlalin ne zaman gerçekleştiği,
- Kişisel veri kategorileri bazında (Kişisel veri / Özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği,
- Kişisel veri ihlalinin olası sonuçları,
- Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler,

- İlgili kişilerin veri ihlali ile bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları,

unsurlarına yer verilmesi gerektiğine karar verilmiştir.

Kurulun 24.01.2019 tarih ve 2019/10 sayılı kararı uyarınca ise yukarıda sayılan unsurları taşıması gereken veri ihlali bildirimi; veri sorumlusunun ihlali öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesi, söz konusu ihlalden etkilenen kişilerin belirlenmesini müteakip ise ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliriyorsa doğrudan, ulaşamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılması gereklidir.

Veri ihlali bildirimlerinde, bu kararda yer verilen form kullanılmalı; veri sorumlusu tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınmalı ve Kurul'un incelemesine hazır halde bulundurulmalıdır. Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı; son olarak, yasa kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, veri sorumlusu kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu planın gözden geçirilmelidir.

4. Kararların Hukuki Değerlendirmesi

Yukarıda açıkladığım üzere, KVKK veri ilgisine yapılacak veri ihlali bildiriminin en kısa sürede gerçekleştirileceği düzenlenirken bildirimin içeriğine ve nasıl gerçekleştirileceğine yer verilmemiştir. Oldukça önemli olan ancak yasada düzenlenmeyen bu iki hususa ilişkin boşluklardan ilki 24.01.2019 tarih ve 2019/10 sayılı kararı ile doldurulmaya çalışılmıştır. *“Veri sorumlusunca söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliriyorsa doğrudan, ulaşamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına”* karar verilmiştir.

Ancak sadece bildirimin nasıl gerçekleştirileceğine ilişkin karar verilmesi KVKK'nın kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini koruma amacı için yeterli değildi. Ayrıca uygulamada sık sık bu sorular tarafıma yönlendirilmekte olup yasada yer alan bu boşluğu, GDPR hükümleri ışığında cevaplamaktaydım. Nitekim Kurul geç de olsa doğru bir şekilde GDPR ile paralellik arz eden bir karar vererek bu görüşümü destekler nitelikte bir karar vermiş, hem de olası görüş ayrılıklarını ortadan kaldırmıştır.

İlk kararda, bu bildirimde hangi unsurların yer alması gerektiği yani içeriğine ilişkin belirsizlik giderilememiştir. Yalnızca usule yer verilen ilk karar, içeriğin de doldurulduğu ikinci kararla birlikte tamamlanmıştır. Veri ihlali bildirimine ilişkin temel sorunlar, bu iki kararın birlikte okunmasıyla çözümlenmiş olmaktadır.

GDPR'dan tek fark olarak Kurul, ihlalin ne zaman gerçekleştiğinin de belirtilmesi gerektiğini ifade etmiştir. Bunun dışında, GDPR ile aynı çözüm benimsenmiştir. Bu yönde bir yaklaşımın sergilenmesi, esasen pek de şaşırtıcı olmayan ve beklenen bir durumdur. Ancak Kurulun yasadaki bu boşluğun farkında olması ve vermiş olduğu yeni kararlar ile bu boşluğu gidermeye çalışması, sevindiricidir. Artık atılacak adım, veri ihlali bildirimini yükümlülüğüne tıpkı GDPR'da olduğu gibi, ayrı ve müstakil bir düzenlemeyle yer verilmesi ve Kurulun bu içtihatlarının yasalaştırması olmalıdır.

Her geçen gün mehzaz 95/46/EC sayılı Direktif'ten GDPR'a doğru yakınlaşılması, kişisel verilerin korunması hukuku alanındaki geçiş sürecimizin hızlandığını ve kısa sürede bu konuda Avrupa ülkelerine yetişmeye çalışıldığını göstermektedir.