

KVKK' DAN KİŞİSEL VERİLERİN YURT DIŞINA AKTARIMINDA ÖNEMLİ BİR ADIM: BAĞLAYICI ŞİRKET KURALLARI

Murat Volkan Dülger* / Cansu Ceren Kahraman*

Giriş

Bilindiği üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 7 Nisan 2016'da yürürlüğe girmesinden beri, kişisel verilerin yurt dışına aktarımı tam bir muammadan ibaret. Çünkü güvenli olmayan ülkelere veri aktarımı yapılabilmesi için Kurul'a kişisel verilerin korunduğuna ve korunacağına ilişkin bir taahhütname ile başvurarak izin alınması gerekmekte. Ancak (Kurul'a sayıları çok olmamakla birlikte bazı veri sorumluları tarafından izin başvurusunda bulunduğu biliniyor) Kurul'a bu zamana kadar yapılan başvurulardan herhangi bir sonuç elde edilemedi. Sonuç elde edilemediği gibi Kurul güvenli olan ülkelerin listesini de hala açıklamadı. Böyle bir durumda yurt dışına kişisel veri aktarımı yapmak isteyen veri sorumlularının elinde tek seçenek kaldı o da açık rıza. Ne yazık ki bu yol da teoride mümkün iken uygulamada (çalışanların açık rızalarının özgür iradeyle alınması sorunu, açık rızaların her zaman geri alınabilmesi gibi nedenlerle) imkansıza yakın.

Tabi ki bu cümlelerden Kurul'un kötü çalıştığı sonucu çıkarılmamalıdır. Kurul'un kişisel verilerin korunması mevzuatının Türkiye'de yerleşmesi için yoğun ve başarılı bir şekilde çalıştığı kabul edilmelidir. Ancak şu anda gerçekleştirilen yurt dışı aktarımların büyük çoğunluğunun hukuka aykırı bir şekilde gerçekleştirildiği de (Kanun'un dört yıl önce yürürlüğe girdiğini göz önüne aldığımızda) unutulmamalıdır. Kurul'un takdir edilmesi gereken noktaları olduğu gibi eleştirilmesi gereken noktaları da vardır. Açıkçası (kişisel verilerin korunması mevzuatına ve uygulamadaki sorunların çözümüne katkısı olduğunu düşündüğümüzden) bu tarz yapıcı eleştirilerin de gerekli olduğunu düşünüyoruz.

Güvenli olan ve olmayan ülkelerin açıklanmasının "karşılıklılık" ilkesinden dolayı zaman alması kabul edilebilir olsa da taahhütnamelere geri dönüşlerin olmaması ve veri sorumlularına hukuka uygun bir yurt dışı aktarımı için (açık rıza dışında) yol gösterilmemesi Kanun'un amacına ters düşmektedir.

* Doç. Dr., İstanbul Aydın Üniversitesi Hukuk Fakültesi Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku öğretim üyesi / Avukat, volkan.dulger@dulger.av.tr, ORCID: 0000-0003-4034-5436

* Stajyer Avukat, İstanbul Barosu, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Bölümü Yüksek Lisans Öğrencisi, cansuceren.kahraman@dulger.av.tr

Kurul'un son yaptığı duyuruda "Bağlayıcı Şirket Kuralları"nın benimsendiğini duyurması da tam olarak son eleştirimiz ile ilgilidir. Geç de olsa Kurul yurt dışı aktarım konusunda harekete geçerek veri sorumlularına alternatif bir yol göstermiş oldu. İşte bu çalışmamızın konusunu da AB kişisel verileri koruma mevzuatında uzun yıllardan beri mevcut olan "Bağlayıcı Şirket Kuralları"nın Türkiye'ye uyarlanmış hali oluşturmaktadır.

I. AB Hukukunda Bağlayıcı Şirket Kuralları

Türkiye'de bağlayıcı şirket kurallarından bahsetmeden önce mehzaz düzenlemesi olan AB, kişisel verileri koruma mevzuatında yer alan, bağlayıcı kurumsal kurallardan bahsedilmesi gerektiğini düşünüyoruz.

AB'de bağlayıcı şirket kuralları 95/46/EC sayılı Direktif'in yürürlükte olduğu dönemde oluşturuldu. Direktif'e göre çok uluslu şirketler, grup şirketlerine veri aktarımı yaparken birden fazla ülkenin mevzuatından kaynaklanan yükümlülükleri aynı anda yerine getirmek zorundaydılar. Bu durum da çok uluslu şirketlerin iş süreçlerini yavaşlatıyordu. Söz konusu engeli aşmak için çok uluslu şirketler kendi gizlilik politikalarını oluşturarak veri koruma otoritelerine kabul ettirmeye çalıştılar.

Kabul ettirilmeye çalışan politikalar da kişisel verilerin yurt dışına rahatça aktarılmasını sağlayan; ancak kişisel verileri de tam olarak korumayan politikalar. Bu durumun önüne geçmek için Avrupa Komisyonu Çalışma Grubu 29, bu gizlilik politikalarının taşınması gereken asgari şartları belirledi ve asgari şartlara sahip kuralları "Bağlayıcı Şirket Kuralları (Binding Corporate Rules)" olarak adlandırdı.

Çalışma Gurubu 29'un çalışmaları sonucu oluşturulan bu kurallara, sonrasında taşınması gereken asgari şartlarla birlikte GDPR'da yer verildi. GDPR'a göre de bağlayıcı şirket kuralları şu asgari şartları taşımalıdır:

- Ortak ekonomik faaliyette bulunan bir teşebbüsler grubunun veya bir işletmeler grubunun ve her üyesinin yapısı ve irtibat bilgileri,
- Kişisel veri kategorileri, işleme türü ve amaçları, etkilenen veri sahiplerinin türü ve söz konusu üçüncü ülke veya ülkelere ilişkin açıklama da dahil olmak üzere veri aktarımları veya aktarım dizisi,
- Bunların hem içsel hem de dışsal olarak hukuki bağlayıcılık yapısı,
- Amaç sınırlaması, verilerin en alt düzeye indirilmesi, sınırlı saklama süreleri, veri kalitesi, özel ve olağan veri koruması, işleme faaliyetine yönelik yasal dayanak, özel kategorilerdeki kişisel verilerin işlenmesi başta olmak üzere genel veri koruma ilkeleri, veri güvenliğinin sağlanmasına ilişkin tedbirler ve bağlayıcı kurumsal

kurallara bağı bulunmayan organlara transit aktarımlara ilişkin gerekliliklerin uygulanması,

- 22. madde uyarınca profil çıkarma da dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı kararlara tabi olmama hakkı,
- 79. madde uyarınca üye devletlerin yetkili denetim makamına ve yetkili mahkemelerine şikâyetle bulunma ve tazminat alma hakkı ve uygun olduğu hallerde, bağlayıcı kurumsal kurallara ilişkin bir ihlalden dolayı tazminat hakkı da dahil olmak üzere veri ilgililerinin işleme faaliyetine ilişkin hakları ve bu hakları kullanma yöntemleri,
- Bir üye devletin topraklarında kurulu veri sorumlusu veya işleyicinin Birlik içerisinde kurulu olmayan herhangi bir üye tarafından bağlayıcı kurumsal kuralların ihlal edilmesi hususunda yükümlülüğü üstüne alması,
- (d), (e) ve (f) bentlerinde atıfta bulunulan hükümler başta olmak üzere bağlayıcı kurumsal kurallara ilişkin bilgilerin 13. ve 14. maddelere ek olarak veri ilgililerine nasıl sağlandığı,
- 37. madde uyarınca belirlenen herhangi bir veri koruma görevlisinin ya da ortak bir ekonomik faaliyette bulunan bir teşebbüsler grubu veya bir işletmeler grubu içerisinde bağlayıcı kurumsal kurallara uyumluluğun izlenmesinin yanı sıra eğitimin izlenmesi ve şikayetlerin ele alınmasından sorumlu olan diğer kişiler veya kuruluşların görevleri,
- Şikâyet usulleri,
- Ortak bir ekonomik faaliyette bulunan bir teşebbüsler grubu veya bir işletmeler grubu içerisinde bağlayıcı kurumsal kurallara uyumluluğun doğrulanmasının sağlanmasına yönelik mekanizmalar,
- Kurallara ilişkin değişikliklerin raporlanması ve kaydedilmesi ile bu değişikliklerin denetim makamına raporlanmasına ilişkin mekanizmalar.

II. Türk Hukukunda Bağlayıcı Şirket Kuralları

Kurul duyurusunda mevcut yurt dışına veri aktarım yollarının çok uluslu şirket toplulukları arasında yapılacak veri aktarımları bakımından uygulama pratiğini sağlamakta yetersiz kalabildiğini; bu nedenle de bağlayıcı şirket kurallarının benimsendiğini belirtmiştir. Ayrıca “Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu” ve “Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman” da yayınlamıştır.

Başvurunun ayrıntılarına geçmeden önce başvurunun kim veya kimler tarafından yapılacağı sorusunun cevaplanması gereklidir.

Grubun¹ Türkiye’de yerleşik merkezi var ise burası, grubun Türkiye’de yerleşik merkezi yok ise Türkiye’de yerleşik bir grup üyesi² kişisel verilerin korunması konusunda yetkilendirilerek “Yetkili Grup Üyesi” tarafından başvuru yapılmalıdır. Başvuru yapmaya yetkili kişi başvuru formu ile birlikte Kurul’a bağlayıcı şirket kurallarını ve başvuru ile ilgili görülen diğer tüm bilgi ve belgeleri de elden veya posta yoluyla sunmalıdır. Yapılan başvurular, Kurum tarafından, resmi başvuru tarihinden itibaren bir yıl içerisinde değerlendirilerek sonuca bağlanır. Gerekmesi halinde bu sürenin, altı aylık sürelerle uzatılması da mümkündür. Başvurunun Kurulca onaylanması durumunda ise, bu durum Kurum tarafından ilgisine bildirilir, gerekmesi halinde de ilan edilir.

Başvuru formunda başvurucudan aşağıdaki konulara ilişkin olarak bilgi vermesi istenmektedir:

- Başvurucunun bilgileri,
- Bağlayıcı şirket kurallarına ilişkin bilgiler (bağlayıcılık unsuru, etkili uygulama, kurum ile koordinasyon, kişisel verilerin işlenmesi ve aktarımı, raporlama ve kayıt değişikliği mekanizmaları, veri güvenliği, hesap verilebilirlik ve diğer esaslar/araçlar, yardımcı bilgi ve belgeler).

Başvuru formunda ayrıca bağlayıcı şirket kurallarına ilişkin genel hükümlere de yer verilmiştir. Burada bağlayıcı şirket kurallarında açık ve anlaşılır bir dil kullanılması gerektiği, grup ve grup üyelerinden her biri bağlayıcı şirket kurallarının yorumlanması ve uygulanmasıyla ilgili Kurum’un talimatlarına uygun hareket etmeyi kabul ettiği, kuralların uygulanması bakımından, başvuru yapmaya yetkili kişinin muhatap olduğu, grubun kurallar kapsamında aktarılan kişisel verileri 6698 sayılı Kanuna ve kurallara uygun olarak işleyeceği, herhangi bir nedenle Kanuna ve Taahhüde uygunluk sağlanamazsa Kurum’un konu ile ilgili derhal bilgilendirileceği, bu durumda Kurum’un, veri aktarımını askıya alma ve Kuralları feshetme hakkına sahip olacağı, kurallar kapsamında işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durum en kısa sürede başvuru yapmaya yetkili kişiye bildirileceği, bu kişilerin ise durumu en kısa sürede ilgisine ve Kurula bildireceği Kurul’un, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da

¹ “Bir şirketler topluluğuna bağlı olarak faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularının tümünü ifade eder.”

² “Şirketler topluluğuna bağlı bir şirket ya da teşebbüs ile ortak bir ekonomik faaliyette bulunan ya da veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan bir gruptaki veri sorumlularını ifade eder.”

uygun göreceği başka bir yöntemle ilan edebileceği, kurallar kapsamında kişisel verilerin grup üyeleri dışındaki kişilere aktarılamayacağı, grup üyeleri dışındaki kişilere aktarım yapılmak istendiğinde taahhütname yolunun kullanılması gerektiği, grup üyelerinden herhangi birinin grupla bağının kesilmesi, kuralların herhangi bir nedenle sona ermesi gibi durumlarda, aktarıma konu kişisel veriler yedekleri ile grubun Türkiye’de yerleşik merkezine veya grubun merkezi Türkiye’de değil ise kişisel verilerin korunması konusunda yetkilendirilmiş Türkiye’de yerleşik bir Grup üyesine gönderileceği veya yedekleri ile birlikte tamamen yok edileceği, kurallarda ulusal mevzuatta bu yükümlülüğün yerine getirilmesini engelleyen hükümler varsa, aktarıma konu kişisel verilerin gizliliğini güvence altına almak için gerekli idari ve teknik tedbirler alınarak veri işleme faaliyetinin sınırlandırılacağı, grup ve grup üyeleri, işledikleri kişisel verileri, 6698 sayılı Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacı dışında kullanamayacağı ve de bu yükümlülüğün herhangi bir süre ile sınırlı olmadığı belirtilmiştir.

Yayınlanan diğer bir doküman ise “Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman”dır. Bu dokümanda bağlayıcı şirket kuralları ile başvuru formu arasındaki farklar ve benzerlikler ile bağlayıcı şirket kurallarına ilişkin açıklamalar bir tablo halinde ifade edilmiştir.

Tabloda bağlayıcı şirket kurallarına uyma yükümlülüğü, ilgili kişinin hakları ve yasal iddiaları, grubun Türkiye’de yerleşik merkezi, kişisel verilerin korunması konusunda yetkilendirilmiş Türkiye’de yerleşik bir grup üyesi veya veri aktaran veri sorumlusunun kurallardan kaynaklanan tazminatın ödenmesi ve ihlallerin giderilmesi konusundaki yükümlülüğünü kabul etmesi, ispat yükünün şirket üzerinde olması, uygun farkındalık, eğitim ile şikayet mekanizmasının ve uygunluk denetiminin bulunması, Kurum ile koordineli çalışma görevinin, kuralların içeriğinin açıklanması gerekliliği, kuralların yer bakımından kapsamı hakkında açıklama, kurallara ilişkin değişikliklerin raporlanması, kaydedilmesi ve bunların Kurum’a bildirilmesi, Türkiye’den aktarım ya da sonraki aktarımları kapsar şekilde veri koruma ilkelerine ilişkin bir açıklama, hesap verebilirlik ve diğer araçlar hususlarının hem bağlayıcı şirket kurallarında hem de başvuru formunda yer alması gerektiği anlaşılmaktadır.

İlgili kişilerin kurallara kolay erişimi ve şeffaflığın sağlanması, kuralların uygulanması konusunda görevli personel yapılanmasının bulunması, ulusal mevzuatın grubun kurallara uymasını engellediği durumlarda şeffaflık hususlarının ise kurallarda yere alıp başvuru formunda yer almadığı görülmektedir.

III. Baęlayıcı řirket Kurallarının Deęerlendirilmesi

Baęlayıcı řirket kurallarına iliřkin olarak yayınlanan dokümanların alıřma Grubu 29'un daha öncesinde yayınlamıř olduęu dokümanların biraz deęiřtirilmiř ve eklemeler yapılmıř çevirisinden ibaret olduęu görölmektedir. Özellikle yayınlanan tablo, alıřma Grubu 29'un 24 Haziran 2008 tarihinde kabul edilen alıřma belgesinin³ birkaç küçük husus dıřındaki çevirisidir. Ne yazık ki dięer düzenlemelerimizde olduęu gibi burada da özgünlük problemi ile karřı karřıyayız. Özgün olmayan düzenlemeler ilk bařta bazı sorunları özmede yeterli gibi gözükse de sonrasında daha bařka problemler ıkarmaya bařlamaktadır. Bu konuya iliřkin birok örneđek vermek mümkündür.

Gerek AB ile ticari iliřkilerimizin yoğunlukta olması gerekse de Kanun'un mehz düzenlemesinin 94/46/EC sayılı Direktif olmasından dolayı, baęlayıcı řirket kurallarına iliřkin, düzenlemenin benzer olmasının AB ile uyumun saęlanabilmesi için iřlevsel olduęu kabul edilebilirse de benzerlięin ok fazla olması durumunda (neredeyse birebir çeviri) Kurul'un itibarının zedeleyebileceęini düşünüyöruz. Hem ierik hem de řekilsel aıdan özgünlüęe biraz daha fazla odaklanılması gereklidir. En azından özgün ieriklerle bilgilendirmeler yapılmalıdır.

Özgünlük dıřında deęerlendirme yapmak gerekirse bařvuru formu baęlayıcı řirket kurallarının bir özeti ve/veya kiřisel verilerin güvenlięinin nasıl saęlandıęına iliřkin bir belge olarak kabul edilebilir. Tablonun, ierik olarak ok fazla bilgi isteyen, bařvuru formu ile baęlayıcı řirket kurallarının (ilk bařta aynı dokümanmıř izlenimi yaratması nedeniyle) farklılıklarını ve benzerliklerini ortaya koyması bakımından iřlevsel olduęu söylenebilir. Ayrıca GDPR'da düzenlenen baęlayıcı řirket kurallarında olduęu gibi Kurul'un benimsedięi baęlayıcı řirket kurallarının da veri aktarımını saęlaması ve hesap verilebilirlik iřlevlerini saęladıęı belirtilmelidir.

Sonuç

Baęlayıcı řirket kuralları, özellikle ok uluslu řirketlerin yurt dıřına kiřisel veri aktarırken büyük kolaylık saęlayan düzenlemelerdir. Kurul'un da böyle bir düzenlemeyi Türk kiřisel verilerin korunması mevzuatı için benimsemesi ok önemli bir adımdır. Bu adımın önemini koruması için (yurt dıřı aktarım için yapılan taahhütnamelerin aksine) yapılan bařvuruların sonuçlarının açıklanması ve kamuoyu ile baęlayıcı řirket kurallarındaki eksikliklerin neler olduęunun paylařılması gereklidir. Aksi durumda yurt dıřı aktarım taahhütnamelerinden farklı olmayacaktır. Uygulamada hukuka aykırı veri aktarımına devam edilecektir ve asla tam bir uyum saęlanamayacaktır. Belirtmemiz gerekir ki bařvurulara dönüř sürelerinin de uzun

³ alıřma Grubu 29, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, 24 Haziran 2008.

olması nedeniyle de dönüş yapılana kadar yurt dışı aktarımlar hukuka aykırı olmaya devam edecektir. Bu noktada mümkün olduğunca hızlı dönüşler yapılmalıdır.

Ayrıca gerek içerik gerekse de şekil açısından da düzenlemelerin daha özgün yapılmasına dikkat edilmelidir. Bu hususa dikkat edildiğinde kişisel verilerin korunmasında başarılı çalışmalar gerçekleştiren Kurul'un itibarının zedelenebilmesinin önüne geçilmiş olacaktır. Özellikle bizler (kişisel verilerin korunması mevzuatı konusunda çalışan hukukçular) tarafından benzerlikler kolayca fark edilebilmektedir.

Son olarak belirtmek gerekir ki Kurul'un üzerine düşen görevler olduğu gibi veri sorumlularının da üzerine düşen görevler vardır. Atılan bu önemli adımın yerini bulması amacıyla çok uluslu veri sorumlularının bir an önce bağlayıcı şirket kurallarını oluşturmaları ve Kurul'a başvurmaları gerektiğini, (ne yazık ki mevcut durumun neredeyse zorunlu kıldığı) hukuka aykırı veri paylaşımına bir an önce son vermeleri gerektiğini düşünüyoruz.