NODE 01
NODE 04
NODE 05
NODE 02
NODE 06
NODE 03
BLOCK 01
BLOCK 01
NODE 01
NODE 02

GDPR ve KVKK Ekseninde *Bağlayıcı Şirket Kuralları*

Doç. Dr. Murat Volkan DÜLGER & Av. Cansu Ceren KAHRAMAN

95/46/EC sayılı Direktif'in kabul edildiği yılların öncesinde, Avrupa Birliği'nde ticari ilişkilerin gelişmesi ile birlikte sınır ötesi veri akışının olacağı tahmin ediliyordu. Bu nedenden dolayı kişisel verilerin korunması için düzenleme yapma ihtiyacı hissedilerek söz konusu Direktif kabul edildi.

İnternetin kamuya açılması ile oluşan büyük veri olgusu ve bunun olumlu ve olumsuz getirileri (big data) Avrupa Komisyonu'nun Direktif'i kabul ederek ne kadar da doğru bir tahmin yaptığını gösterdi. Gerçekten de dijital çağ ile birlikte, özellikle çok uluslu şirketlerin iş süreçleri kapsamında kişisel veri işleme ve akışında büyük bir artış yaşandı. Çok uluslu şirketler farklı ülkelerde yer alan grup şirketleri bünyesinde işçilerin maaş, kıdem vb. verilerini iş sözleşmesi ve kanunlardan kaynaklı yükümlülüklerin yerine getirilmesi amacıyla, müşterilerinin verisini de satış faaliyetlerinin kapsamında işlediler. Tüm işlemiş oldukları verileri tedarikçileri, iş ortakları ve diğer grup şirketleri ile uluslararası alanda paylaştılar.

Teknolojideki gelişmeler ile çok uluslu şirketler merkezi bir bilişim sisteminin yanında birden fazla yerde konumlanmış ve çok hızlı bir şekilde uluslararası veri paylaşımına izin veren bilişim sistemlerini kullanmaya başladılar. Bu gelişmelerin ardından dinamik yönlendirmenin ve bulut sisteminin de kullanılmaya başlanmasıyla birlikte internet ortamında paylaşılan

ve saklanan veriler neredeyse takip edilemez bir hal aldı. Bundan dolayı Direktif yetersiz kaldı ve Direktif'in üst versiyonu olarak nitelendirilebilecek GDPR kabul edildi.

Avrupa Birliği'nin veri korumasına ilişkin düzenlemesine göre, farklı ülkelerde yer alan grup şirketleri kendi aralarında veri paylaşımı yaparken aynı anda birden fazla ülkenin kişisel verilerin korunması mevzuatındaki yükümlülüklerin yerine getirilmesi gerekiyordu. Çok uluslu şirketler iş süreçleri içerisinde düzenli olarak veri paylaşımı yaptıklarından dolayı yükümlülükleri yerine getirmiş olmanın daha kolay yollarını aramaya başladılar. Buldukları çözüm ise veri paylaşımı yaptıkları tüm ülkelerdeki yükümlülükleri içerisine alacak neredeyse dünya çapında bir veri gizliliği politikası oluşturmaktı.

Politikalarını oluşturan şirketler için her şeyin istedikleri gibi gitmesine bir adım daha vardı ki o da Veri Koruma Otoriteleri'ne (DPO) hazırlamış oldukları politikaları kabul ettirmekti. Bunun için de veri koruma otoritelerine baskı yapmaya başladılar. Baskıların sonuç vermesi ile birlikte görünürde yeterli önlemleri içeren şirket gizlilik politikaları çerçevesinde (ama aslında yeterli önlemler alınmaksızın) kişisel veriler paylaşılmaya başlandı. Bu durumun önüne geçmek amacıyla da "Bağlayıcı Kurumsal Kurallar" (Binding Corporate Rules) oluşturuldu.

Günümüzde Avrupa Ekonomik Alanı'ndaki neredeyse her şirketin kişisel verilerin korunmasına ilişkin politikası olmasına rağmen birçok veri koruma otoritesi tarafından şirketlerin bilişim sistemlerinin tam bir koruma için yetersiz olduğu belirtilmektedir. Bu tespiti başka kelimelerle ifade etmemiz gerekirse şirketler kişisel verileri koruduklarını taahhüt etmelerine rağmen aslında kişisel verileri fiilen korumamakta ya da koruyamamaktadırlar. Böylece GDPR'ın hükümlerinin ihlali sonucunda şirketlere cirolarının belirli bir yüzdesi üzerinden (Türkiye'de kesilen idari para cezalarından çok daha fazla) ceza kesilmesinin yeterli olmadığını, veri koruma otoritelerin imkanlarının kişisel verilerin korunması mevzuatına uyum için şirketleri zorlamak bakımından tek başına yetersiz kaldığını söylememiz mümkündür.

Bu makalemizde öncelikle bağlayıcı kurumsal kuralların oluşturulma nedenlerinden, işlevlerinden, kuralların kabul edilmesi için onay başvurusunun nasıl yapılacağından bahsettikten sonra bu kuralların niteliklerine ilişkin diğer özelliklerine değinerek 6698 sayılı Kanun kapsamında yurtdışı veri paylaşım taahhütnameleri ile bu kuralların ilişkisini değerlendireceğiz.

BAĞLAYICI ŞİRKET KURALLARININ ORTAYA ÇIKIŞI

Kişisel verilerin sınır ötesi paylaşımı, küresel ticaretin ve sosyal ilişkilerin gelişimi için son derece önemli ve gereklidir. Ülkeler vatandaşlarının verilerine yabancı kişi ve kuruluşların kişilerin erişebileceği endişesi ile paylaşım konusunda kısıtlamaların olduğu düzenlemeler yapma yoluna gitmişlerdir. Bu nedenle günümüzde artık neredeyse her ülkenin kişisel verileri koruma mevzuatı bulunmaktadır.

Direktif'e göre çok uluslu şirketler, grup şirketlerine veri paylaşımı yaparken birden fazla ülkenin mevzuatından kaynaklanan yükümlülükleri aynı anda yerine getirmek zorundaydılar. Her ülkenin kendi veri koruma mevzuatına sahip olması (her ne kadar bu düzenlemeler yapılırken diğer ülkelerin veri koruma mevzuatları dikkate alınsa da) verilerin ülkeler arasında istenildiği kadar rahat paylaşılmasını engellemekteydi. Bu engeli aşmak için şirketler kendi gizlilik politikalarını oluşturarak bu politikaları Veri Koruma Otoritelerine kabul ettirmeye çalıştılar. Ama oluşturdukları bu politikalar ne yazık ki kişisel verileri görünüşte koruyan politikalardı.

Şirketlerin tam olarak korumadan kişisel verileri paylaşmalarının önüne geçmek amacıyla Avrupa Komisyonu Madde 29 Çalışma Grubu şirket gizlilik politikalarının karşılaması gereken bazı kriterler oluşturdu. Bu kriterlerden ilki şirket gizlilik politikalarının hem şirket içinde (şirket ve ona bağlı grup şirketlerinde) hem de şirket dışında, bireylerin çıkarları doğrultusunda şirketler için bağlayıcı olmasıydı. İşte bu bağlayıcılık özelliğini vurgulamak amacıyla da Madde 29 Çalışma Grubu bu politikaları "Bağlayıcı Kurumsal Kurallar" (Binding Corporate Rules) olarak adlandırdı.

Ancak bazı veri koruma otoriteleri Madde 29 Çalışma Grubu'nun görüşlerine rağmen bağlayıcı kurumsal kuralları kabul etmeyi reddederek veri paylaşımı için bazı ek şartların varlığını aradılar. Aynı durum GDRP'ın

yürürlükte olduğu günümüzde de geçerlidir. Bu bakımdan bağlayıcı kurumsal kuralların (veri paylaşımı konusunda ulusal düzenlemesi olan) AB dışındaki ülkeler tarafından da geçerli bir veri paylaşım aracı olarak kabul edilip edilmeyeceğine dair hala bir belirsizlik söz konusudur. Başka bir deyişle bağlayıcı kurumsal kuralların, küresel düzeyde -temelde tam anlamıyla- gerçekleştirilip gerçekleştirilemeyeceği ve gerçekleştirilebilecekse de ne zaman olacağı hala belirsizdir.

Önümüzdeki on yıl içerisinde küresel bir veri koruma düzenlemesi yapılabilecek gibi de gözükmemektedir. Küresel bir veri koruma düzenlemesi yapılana kadar ticareti ve sosyal gelişmeleri hızlandırmak ve yenilerinin de önünü açmak amacıyla bu kurallar çok önemli bir araçtır. Onlar sayesinde ülkeler arası veri paylaşımı daha kolay ve daha az maliyetle yapılabilmektedir.

GDPR'DA BAĞLAYICI KURUMSAL KURALLAR

95/46/EC sayılı Direktif zamanında Madde 29 Çalışma Grubu tarafından oluşturulan bağlayıcı kurumsal kurallar GDPR'da ayrıntılı olarak düzenlenmiştir. GDPR'ın 45. maddesine göre "Komisyonun bir üçüncü ülke veya söz konusu üçüncü ülke dahilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun yeterli düzeyde bir koruma sağladığına karar verdiği hallerde, bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleşebilir. Böylesi bir aktarım için spesifik bir onay gerekmez." Ancak "45(3) maddesi uyarınca alınan bir karar olmaması halinde, ancak bir veri sorumlusu veya işleyenin uygun güvenceler sağlamış olması halinde ve uygulanabilir veri sahibi hakları ve veri sahiplerine yönelik etkili kanun yollarının mevcut olması koşuluyla, söz konusu veri sorumlusu veya işleyen bir üçüncü ülke veya uluslararası bir kuruluşa kişisel veri aktarabilir."

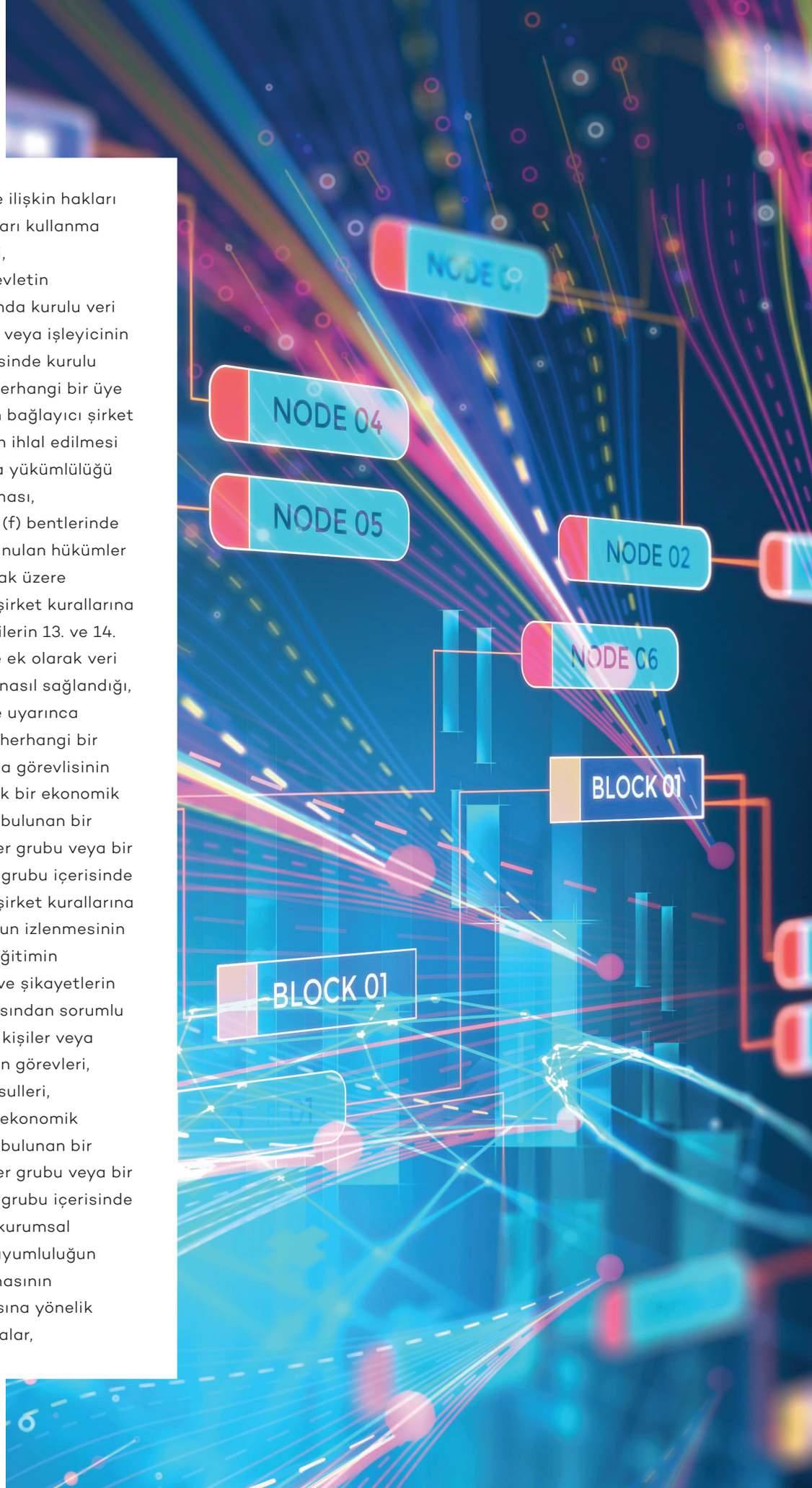
Uygun güvenceler, bir denetim makamından spesifik bir onay alınmasına gerek olmaksızın, 46. maddenin 2. fıkrasında sayılanlardan bir tanesi ile sağlanabilir. Bağlayıcı kurumsal kurallar da bunlardan bir tanesidir.

GDPR'ın 47. maddesinde bağlayıcı kurumsal kuralların taşıması gereken asgari unsurlar düzenlenmiştir. Bunlar:

- 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 bağlı 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 şikâyette 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 şirket kurallarının ihlal edilmesi hususunda yükümlülüğü üstüne alması,
- (d), (e) ve (f) bentlerinde atıfta bulunulan hükümler başta olmak üzere bağlayıcı şirket kurallarına 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 şirket kurallarına 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 mekanizmalardır.

BAĞLAYICI KURUMSAL KURALLAR KAVRAMI, KAPSAMI VE DAVRANIŞ KURALLARINDAN FARKI

Üçüncü bir ülkeye yapılan paylaşım, veriyi üçüncü bir ülkedeki başka bir veri sorumlusuna veya veri işleyene iletmekten oluşur; bunun hukuka uygunluğu ise (günümüzde) GDPR'ın belirlediği ilkelere ve somut olayın koşullarına göre değerlendirilmelidir. Bağlayıcı kurumsal kurallarda yer alan koruma ilkeleri büyük ölçüde GDPR'ın koruma ilkelerine uygun olmalıdır. Bu bakış açısıyla, genel bir ilke olarak, bağlayıcı kurumsal kuralların topluluk içinde uygulanması, kuralların ulusal veri koruma mevzuatına uygun olması koşuluyla herhangi bir sorun teşkil etmez. Bu koşullar yerine getirilirse, kurallar, şirket gruplarının gerçekten küresel bir gizlilik politikasına sahip olmalarını sağlar.

Aynı düşünce ve tanım gereği, bağlayıcı kurumsal kurallar küreseldir ve bu nedenle uygulanmalarında herhangi bir ayrım yapılmamalıdır. Kurallar, üyelerin kuruluş yeri veya veri ilgililerinin uyruğu vb. kriterler ya da değerlendirmelerden bağımsız olarak şirketler grubu boyunca uygulanmalıdır. Bununla birlikte, şirketler grubu kurallara uymaya çalışsa da AB kaynaklı veriler de denilen ve AB mevzuatına tabi olan ve daha sonra yurtdışına aktarılan kişisel veriler bakımından kuralların uygulanabilirliği zamanla farklılaşabilir.

Sonuç olarak, bu belgelerin amacı Direktifin 27. maddesinde öngörülen davranış kurallarından (code of conduct) farklı olduğu için, bunlara "davranış kuralları" olarak atıfta bulunmaktan ziyade, uygun bir terminoloji bulmak daha uygun görünmektedir. Çünkü bu belgelerin gerçek doğası, topluluk dışına aktarılan kişisel verilerin korunması için yeterli güvencenin sağlanmasıdır.

Davranış kuralları GDPR'ın 40. maddesinde -Direktif'e göre- daha ayrıntılı bir şekilde düzenlenmiştir. Davranış kuralları GDPR'da yer alan düzenlemelerin pratik yorumundan ibarettir. Veri sorumluları sektörlerine ilişkin, GDPR'ı yorumlayarak, kendi uyum kurallarını oluştururlar. Bu bakımdan GDPR'ın uygulanması sırasında karşılaşılabilecek sektörel ve teknolojik problemlere çözüm üretilmesi ve kişisel verilerin daha iyi korunmasını sağladığı için önemlidir. Sınırlı sayıda olmamakla birlikte GDPR'da hangi konuları içeren davranış kurallarının oluşturulabileceği sayılmıştır:

- Adil ve şeffaf veri işleme,
- Veri sorumluları tarafından özellikli bağlamlarda gözetilen meşru menfaatler,
- Kişisel verilerin toplanması,
- Kişisel verilerde takma ad kullanımı,
- Kamuoyuna ve veri ilgililerine sağlanan bilgiler,
- Veri ilgililerinin haklarının kullanımı,
- Çocuklara sağlanan bilgiler ve çocukların korunması ve çocuklar üzerinde velayet hakkına sahip olanların rızasının alınma şekli,
- GDPR'ın 24. ve 25. maddelerinde atıfta bulunulan tedbirler ve usuller ile 32. maddede atıfta bulunulduğu üzere işleme faaliyetinin güvenliğinin sağlanmasına yönelik tedbirler,
- Kişisel veri ihlallerinin denetim makamlarına bildirimi ve söz konusu kişisel veri ihlallerinin veri ilgililerine iletilmesi,
- Üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarılması,
- Veri ilgililerinin 77. ve 79. maddeler uyarınca haklarına halel gelmeksizin, veri sorumluları ve veri ilgilileri arasında ihtilafların çözümüyle ilgili mahkeme dışı işlemler ve diğer ihtilaf çözüm usulleri.

Davranış kuralları hazırlamayı veya mevcut kuralları değiştirmeyi veya mevcut kuralların kapsamını genişletmeyi amaçlayan birlikler ve diğer organlar; kurallar, değişiklik veya kapsam genişletmeye ilişkin taslağını GDPR'ın 55. maddesi7 uyarınca yetkin denetim makamına ibraz eder. Denetim makamı kurallar, değişiklik veya kapsam genişletmeye ilişkin taslağın GDPR ile uyumlu olup olmadığı konusunda bir görüş sunar ve kuralların yeteri kadar uygun güvenceleri sağladığını belirlemesi durumunda, kuralları veya taslağı onaylar. Kurallar veya değişiklik ya da kapsam genişletmeye ilişkin, taslağın onaylandığı hallerde ve ilgili davranış kurallarının çeşitli üye devletlerdeki işleme faaliyetleri ile ilgili olmadığı hallerde, denetim makamı kuralları tescil eder ve ayrıca yayımlar.

Davranış kuralları onaylandıktan sonra şirketler, davranış kurallarının gerekliliklerine uygunluğunu sürekli olarak kendi kendine izlemek zorundadır. Bu bağlamda denetim otoriteleri, işletmenin faaliyetlerinin davranış kurallarına sürekli olarak uygunluğunu belirlemek için az çok rutin olmayan kontroller gerçekleştirecektir.

Açıkça görülüyor ki bağlayıcı şirket kuralları ile davranış kurallarının birbirine benzer yönleri bulunmakla birlikte temelde farklı iki kurumdur. Davranış kuralları, veri işleme kapsamında şirketin idari ve teknik gereksinimlerini belirtir. Böylece şirketlerin faaliyetlerinin GDPR'a uygun olup olmadıklarını ve nasıl denetleneceklerini belirlemelerine izin verilmiş olur. Ancak uyuma ilişkin kendi denetimleri, veri denetim otoriteleri nezdinde uyumluluğun kanıtı olarak kullanılamaz.

Aslında davranış kuralları, GDPR'ın soyut hükümlerinin pratik bir yorumudur. Bağlayıcı kurumsal kurallar ise veri sorumlularının üçüncü ülkelere veri paylaşımı yapılmasını ve paylaşım sırasında verilerin güvenliğini sağlayan kurallardır.

Bağlayıcı şirket kuralları (terminolojik olarak) "uluslararası veri paylaşımları için bağlayıcı şirket kuralları" veya "uluslararası veri paylaşımları için yasal olarak uygulanabilir kurumsal kurallar" olarak ifade edilebilir. Burada "bağlayıcı veya yasal olarak uygulanabilir" ifadesinin tercih edilmesinin nedeni, Direktif'in 26. maddesinin 2. fıkrası kapsamında "yeterli güvence" olarak kabul edilebileceğinden, şirket ifadesi ise bunların genellikle merkezin sorumluluğu altında kurulan çok uluslu şirketlerde uygulanan kurallardan oluşmasından, uluslararası veri paylaşımı da varlığının temel nedeni olmasından dolayı tercih edilmiştir. Nitekim bu şekilde bir terminolojinin kullanılması bağlayıcı kurumsal kuralların niteliğini daha doğru bir şekilde ortaya koymaktadır.

Şirketler grubu kavramı kimi zaman hiyerarşik olarak yapılandırılmış çok uluslu şirketleri ifade edebileceği gibi kimi zaman farklı ekonomik faaliyetlerde bulunan bir şirketler grubunu da ifade edebilir. Bu nedenle bağlayıcı kurumsal kurallar için başvuru yapılırken şirketlerin yapı ve faaliyetlerindeki farklılıklar göz önünde bulundurulmalıdır.

Holdingler için (loose conglomerates) bağlayıcı kurumsal kuralların uygun bir araç olması pek olası değildir. Çünkü bünyesindeki birbirinden farklı alanlarda faaliyet gösteren şirketlerin tamamının ihtiyaçlarının tek bir metin ile karşılanması çok zordur. Bu holdingler için aynı kurumsal grup içindeki alt grupları birbirinden ayırmak, veri alışverişi için ciddi sınırlamalar ve koşullar belirlemek gereklidir.

Uygulamada, (dünya çapındaki grup içi aktarımları bu şekilde düzenlemek istedikleri için) çok uluslu şirketlerin bu mekanizmaların en sık kullanıcıları olması beklenmektedir. Madde 29 Çalışma Grubu, bu belgeye dayanarak verilen herhangi bir yetkilendirmenin kapsamının yalnızca şirketler grubu içindeki paylaşımları veya paylaşım kategorilerini diğer bir deyişle, bu kurumsal kurallara bağlı şirketler arasındaki kişisel veri alışverişini etkileyeceğini vurgulamaktadır.

BAĞLAYICI ŞİRKET KURALLARININ İŞLEVİ

Bağlayıcı şirket kuralları 95/46/EC sayılı Direktif'in 25. maddesi ile veri koruma ilkesine uyum kapsamında çok uluslu şirketlere Avrupa Ekonomik Alanı dışındaki iştiraklerine veri paylaşımı yapmalarını sağlamak amacıyla oluşturulmuştur. Bu nedenle bağlayıcı kurumsal kuralların ilk ve öne çıkan işlevi veri paylaşımını sağlamasıdır. AB'nin kişisel veri mevzuatı kişisel verilerin paylaşılması için veri paylaşılan ülkede de korumanın olması ve o ülkenin de yükümlülüklerini yerine getirmesini aramaktadır. Özellikle çok uluslu şirketler için ülkelere göre başka prosedür ve politika uygulamak iş süreçlerinin aksamasına neden olan bir durumdur. Nitekim bağlayıcı şirket kurallarının ortaya çıkış amacı da yaşanan ve yaşanabilecek aksaklıkların önüne geçmektir.

Bağlayıcı şirket kurallarının diğer bir işlevi ise hesap verilebilirliktir. Başka bir deyişle AEA kapsamındaki tüm otoriteler tarafından kabul görmesi ve denetlenebilmesi nedeniyle şirketler, kurallara uygun işleme yapmak ve yapmış olduğu işleme faaliyeti hakkında da gerektiğinde açıklama yapma yükümlülüğüne sahiptir. Kuralların başka bir işlevi ise veri gizliliğinin yönetimini sağlamasıdır. Bunu da her otorite tarafından şirketlerin denetime tabi tutulabiliyor olması ile gerçekleştirir. Her otorite tarafından denetlendiğinden şirketin veri gizliliği kontrol altında tutulabilir. Kuralların son işlevi ise kişisel verilerin korunması konusunda farkındalık yaratması ve veri koruması sağlamasıdır. Kurallar ile veri sorumlusu şirketler kişisel verileri tam olarak korumak zorundadırlar. Yine bu durum da denetim ve hesap verilebilirlik ile doğrudan ilişkilidir.

Tüm bunların yanında bağlayıcı kurumsal kurallar şirketin kişisel verileri koruduğunu ifade etmesi nedeniyle müşterilerde

güven yaratarak ticari itibarı dolayısıyla da ticari gelirleri arttırıcı etkiye de sahiptir.

KİŞİSEL VERİLERİN PAYLAŞILMASINA İLİŞKİN YAKLAŞIMLAR BAKIMINDAN BAĞLAYICI KURUMSAL KURALLARIN ROLÜ

Kişisel verileri koruma ile ilgili yasal düzenlemeler yaparken her ülkenin farklı bir bakış açısıyla hareket ettiği görülmektedir. Örneğin Avrupa Birliği kişisel verileri korumayı, temel hak ve özgürlükleri koruma kapsamında değerlendirerek yasal düzenlemelerini bu bakış açısıyla gerçekleştirmektedir. Oysa Asya Pasifik Ekonomik İşbirliği ve Amerika Birleşik Devletleri konuya ekonomik çıkarları korumak adına bir mülkiyet hakkı olarak ele almaktadır. Aslında bu farklılıklar veri koruma düzenlemelerinin ülkeden ülkeye ne kadar değiştiğini gözler önüne sermektedir.

Kişisel verileri paylaşma noktasında temelde iki yaklaşım şekli mevcuttur. Bunlardan ilki bölgesel temelli kurallar, ikincisi ise organizasyon temelli kurallar yaklaşımıdır. Avrupa Birliği'nin yaklaşımı, bölgesi içerisinde kişisel verileri koruması nedeniyle birinci yönteme örnektir. Asya Pasifik Ekonomik İşbirliği'nin (APEC) hazırlamış olduğu Gizlilik Çerçevesi ise, nerede konumlandığına bakmaksızın (bir başka organizasyona yapılan veri paylaşımlarından sonra da) organizasyonun kendi bünyesindeki faaliyetler bakımından kişisel verileri koruması itibariyle de ikinci yaklaşıma örnektir. Bu iki yaklaşımın başlangıç noktaları çok farklı görünse de iki sistem büyük ölçüde uygulamalarında birleşmektedir.

APEC, Gizlilik Çerçevesi aracılığıyla da üye ülke kuruluşlarının yurtdışına veri paylaşımını kolaylaştıracak şekilde "Sınır Ötesi Gizlilik Kuralları" (CBPR) benimsemelerini sağlamaya çalışmasıyla benzer bir organizasyonel amacı hedeflemektedir. APEC Gizlilik Çerçevesi, aynı zamanda, üye ülkeleri, katılımcı ülkelerin veri koruma ihlallerinin soruşturulmasında iş birliği yapmaları için ikili veya çok uluslu düzenlemeler geliştirmeye teşvik ettiği için bölgesel yaklaşımın unsurlarını da içermektedir. Ayrıca APEC Gizlilik Çerçevesi, ikili veya çok uluslu iş birliğinin ulusal yasalar veya politikaların ihlaline yol açması durumunda sınırlandırılabileceğini hatta reddedilebileceğini belirtmektedir. Dolayısıyla, karşı tarafın yasaları bir ülkenin ulusal yasalarına

"eşdeğer" olarak kabul edilmezse, iş birliği reddedilebilir. Bu durum da AB'nin yeterlilik kurallarına çok benzer bir sonucu ortaya çıkarır. Bağlayıcı kurumsal kuralların böyle bir durumda rolü, AB ve APEC üye ülkelerinin uygun evrensel veri koruma seviyesinin ne olması gerektiği konusunda anlaşamadığı durumlarda, uluslararası veri paylaşımını kolaylaştırarak iki sistem arasında köprü görevi görmesidir.

ÜLKELERİN YASAMA VE YÜRÜTME YETKİLERİNİN KAPSAMI BAKIMINDAN BCR'LARIN ROLÜ

Kural olarak her yasa, yürürlüğe konulduğu ülkenin kendi siyasi sınırları içerisinde geçerlidir. Bu kural egemenlik yetkisinin doğal bir sonucu olup ülkesellik ilkesi olarak adlandırılır. Bazen ülkeler yasama, yürütüme veya yargı yetkilerinden (egemenliklerinden) bir kısmını devrederek uluslararası alanda bir üst organizasyonun yetkisini kabul etmektedirler. Avrupa Birliği de bunun en önemli ve tipik örneğidir.

Teknolojinin gelişmesi, saniyeler içerisinde kişisel verilerin dünyanın diğer bir ucuyla paylaşılmasını sağlamıştır. Özellikle çok uluslu şirketlerin ticari faaliyetleri ile aynı anda çok sayıda ülkenin vatandaşının verileri paylaşılır hale gelmiştir. Bu nedenle kişisel veriler hakkında ülkelerin sadece kendi siyasi sınırları içerisinde uygulanan ve koruma sağlayan düzenlemeler yetersiz kalmıştır. Birçok ülke de kişisel verileri koruma yasalarının uygulama kapsamını geniş tutarak yurtdışı ile paylaşılan verilerini korumaya çalışmaktadır.

Ancak ülkelerin yurtdışına aktarılan verilerini korumaya çalışmaları, beraberinde uluslararası hukuk bakımından birçok soruyu ve sorunu ortaya çıkarmıştır. Çünkü bir anlaşma ve yetki söz konusu olmadıkça bir ülkenin yasasının bir başka ülkede uygulanması ulusal hukuk düzenlemelerine göre mümkün değildir. Bu yüzden kişisel verilerin korunması konusunda, özellikle kişisel veri ihlalinin olduğu durumlarda, yapılması gereken diğer Veri Koruma Otoriteleri ile iş birliği yapmaktır. Böylece her ülkenin yasama, yürütme ve yargı yetkileri ihlal edilmeden kişisel verilerin korunması sağlanacaktır. Ancak tam bir iş birliğinin dahi kişisel verilerin korunması konusunda (ülkelerin mevzuatlarının farklılığı nedeniyle oluşabilecek yasal boşluklar nedeniyle) ihlallerin önüne, tamamen geçebileceğini düşünmüyoruz.

Küresel çapta uygulanabilir bir düzenlemenin yapılmasının önemi tam da bu noktada kendini gösterir. Saniyeler hatta saliseler içerisinde çok büyük miktarda kişisel veri ülkeler arasında paylaşılabildiği, bu verilerin de kendi ticari pazarını oluşturduğu günümüzde kişisel verilerin korunması gerekliliği kaçınılmazdır. Avrupa Birliği'nde yaşayan bir kişinin kişisel verisinin AEA dışında işlenmesi durumunda veriyi işleyen ülkede de GDPR'ın uygulanabileceğinin düzenlenmesi bu nedenledir.

Ancak GDPR'in tüm Avrupa Birliği ülkeleri bakımından tek bir düzenleme olması nedeniyle önemli bir adım olduğu göz ardı edilmemekle birlikte kapsamı ülkelerin egemenlik yetkisi bakımından (AB üyesi olmayan ülkeler için) sorun oluşturabilir. AB üyesi olurken ülkeler egemenlik yetkilerinden bir kısmını üyeliğin kendilerine sağlayacağı avantajlardan dolayı Birliğe devretmektedirler. Ancak Birliğe üye olmayan ülkeler bakımından böyle bir durum söz konusu değildir. Bu, uluslararası taraf olunmayan bir organizasyonun düzenlemesinin Türkiye'de uygulanmaya çalışılması anlamına gelir. Bir örnekle açıklamak gerekirse Türkiye merkezli bir otele kalmaya gelen aslında Özbekistan vatandaşı olan ama Almanya'da yaşayan bir kişinin kişisel verileri GDPR'a aykırı olarak paylaşıldığında Alman Veri Koruma Otoritesi, Türkiye'deki 6698 sayılı Kanun'a tabi olan otele nasıl yaptırım uygulayacaktır? Bu sorunu çözmek için en iyi çözüm Türk veri koruma otoritesi olan Kişisel Verilerin Korunması Kurumu ile Alman Veri Koruma Otoritesi'nin iş birliği yapmasıdır. Yani Alman Veri Koruma Otoritesi bir ihlal gerçekleştiği konusunda Kişisel Verilerin Korunması Kurumu'nu uyaracak ve bunun üzerine de KVKK denetimlerini yaparak 6698 sayılı Kanun'a göre idari para cezası uygulayacaktır. Bu çözüm yaptırımın nasıl uygulanacağı gibi problemleri çözmekte yardımcı olsa da mevzuatlar arası farklılıktan kaynaklanan sorunların ve ihlal durumlarının önüne geçememektedir.

İşbirliğinin de dolduramadığı bu boşluklarda bağlayıcı kurumsal kurallar devreye girmekte ve özellikle çok uluslu şirketler tarafından veri korumasının olmadığı veya daha az olduğu ülkelerdeki grup şirketlerine uygulanması nedeniyle (ülkenin vatandaşları da

bu korumadan yararlandığı için) önemli bir işleve sahip olmaktadır.

BAĞLAYICI ŞİRKET KURALLARI VE ABD - AB VERİ PAYLAŞIMI

GDPR'da üçüncü ülkelere veri paylaşımı sıkı koşullara sahiptir. Ancak verinin paylaşılacağı üçüncü ülkede de yeterli veri korumasının sağlanması durumunda veriler paylaşılabilir. Yeterli korumanın sağlandığı Avrupa Komisyonu kararı veya sözleşmelerde yer alan model şartlar ya da bağlayıcı kurumsal kuralların var olması durumunda kabul edilmektedir. İlkinden başlamak gerekirse Avrupa Komisyonu kişisel verileri (paylaşım yapılacak üçüncü ülkenin yasalarının) yeterli bir şekilde koruduğuna ve dolayısıyla paylaşım yapılabilecek üçüncü ülkeleri açıklamaktadır. Ancak bu şekilde hakkında karar verilen ülke sayısı çok azdır. Karar verilen ülkelere örnek olarak İsviçre ve İsrail (ABD bu ülkelerden biri değildir) gösterilebilir.

Bağlayıcı kurumsal kuralların temel avantajı, geliştirildikten ve işletildikten sonra, (şirketin gereksinimlerini karşılamak için) çeşitli grup içi paylaşımlar bakımından, bir çerçeve sağlayabilmesidir. Ama diğer taraftan bu kuralları benimseyen şirketlerin uyumu düzenli olarak izleyerek sürdürmesi gerekir. Bu kapsamda şirketlerin gerek belirli periyotlarda gerek de ansızın denetimler gerçekleştirmeleri ve personellerine eğitim vermeleri önemlidir.

Bağlayıcı kurumsal kurallar dışında veri paylaşımına izin verilen diğer bir yol, (şirketlerin tüm veri koruma otoriteleri ile çok sayıda anlaşma yapma zahmetinden kurtaran) sözleşmelerde yer alan "model hükümlerin" (model clause) kullanımıdır. Bu şartların kullanımına izin verilse de uygulamada Avrupa Komisyonu tarafından onaylanmış olmasına rağmen bazı veri koruma otoriteleri tarafından, zaman alan, ayrıca bir süreç işletilmektedir. Bu da şartların kullanım oranını azaltmaktadır. Buna rağmen geleneksel olarak, veri paylaşımlarını meşrulaştırmak için yeterli düzeyde koruma sağlamayan ülkeler için en sık kullanılan, "standart sözleşme maddeleri" veya "model hükümler" olarak adlandırılan bu mekanizmadır. Bu kurallaru, 95/46/EC Veri Koruma Direktifi kapsamında Avrupa Komisyonu tarafından önceden onaylanmış bir sözleşme hükümleeri olup, kişisel verilerin AB standartlarına uygun olarak korunması amacıyla hem ihracatçılara hem de ithalatçılara uygulanacak belirli yükümlülükler tesis etmiştir. GDPR kapsamında hukuki anlamda daha kapsayıcı olan hükümlerle değiştirilinceye veya yerine yenisini getirilinceye kadar Direktif zamanında oluşturulan bu model hükümler geçerliliğini korumaktadır.

Avrupa Komisyonu tarafından onaylanan model hükümler (veri koruma yetkilileri tarafından bu kapsamdaki yeni sözleşmelerin değerlendirilmesi nedeniyle) veri paylaşımında sözleşmesel yolların gelişimi bakımından önemli bir rol oynamaktadır. Microsoft, Amazon Web Services ve Google gibi bazı teknoloji şirketleri, üçüncü ülkelere veri paylaşımı konusunda kendi sözleşmelerini hazırlayarak veri koruma otoritelerine onaya sunulmasına öncülük etmektedirler. Model hükümlerin en büyük avantajı şirketler kendi yapı, faaliyet ve imkanlarına göre sözleşmeleri hazırladıklarından dolayı daha gerçekçi bir veri koruması taahhüt ederek, olası sözleşmesel yükümlülüklerinin ihlalinin önüne geçilmiş olmaktadır. Model hükümlerin temel avantajları şunlardır:

- Sözleşme, Avrupa Komisyonu veya Avrupa veri koruma yetkilileri tarafından kabul edilen standart sözleşme hükümlerine dayandığı ölçüde, prensip olarak, veri paylaşımlarını meşrulaştırmak için geçerli bir mekanizma olarak kabul edilmektedir.
- Taslak hale getirmek ve sözleşmeyi akdetmek çok zaman alıcı olmamaktadır.

Ancak, bazı temel dezavantajları da vardır:

- Sözleşme metinlerinin devinim halinde olmayan yapısı göz önüne alındığında çoklu ve değişen paylaşımlar için yeterli olmama ihtimali vardır.
- Avrupa Komisyonu veya veri koruma yetkilileri tarafından aranan standartları karşılayabilmek için, sözleşmenin taraflarca kişisel verilerin kullanımını etkileyen çok sıkı şartlar içermesi gereklidir.

2016 yılına kadar model hükümlerden başka veri sorumluları için yurtdışına veri paylaşımını kolaylaştırıcı diğer bir yol ise Güvenli Liman (Safe Harbor) ilkeleriydi. Güvenli Liman başka bir deyişle Uluslararası Güvenli Liman Gizlilik İlkeleri, ABD ve AB bünyesindeki özel kuruluşların kişisel

verileri ifşa etmelerinin ve kaybetmelerinin önüne geçmek amacıyla (veri paylaşımını kolaylaştırıcı nitelikte) 1998 ve 2000 yılları arasında geliştirilen ilkelerdi. Bunlar, bildirim, seçim, ileriye aktarım, erişim, güvenlik, veri bütünlüğü ve uygulamadır. Şirketler Güvenli Liman ile veri koruma önlemlerini aldıklarını ve yedi temel ilkeye uyduklarını onayladılar.Ancak Güvenli Liman İlkeleri'nin Avrupa Adalet Divanı tarafından 2016 yılında artık geçerli olmadığına karar verildi. Güvenli Liman İlkelerinin geçersiz kabul edilmesi bağlayıcı kurumsal kurallar gibi veri paylaşımını meşrulaştıran yöntemlerin geçerliliğine şüphe ile yaklaşılmasına neden oldu.

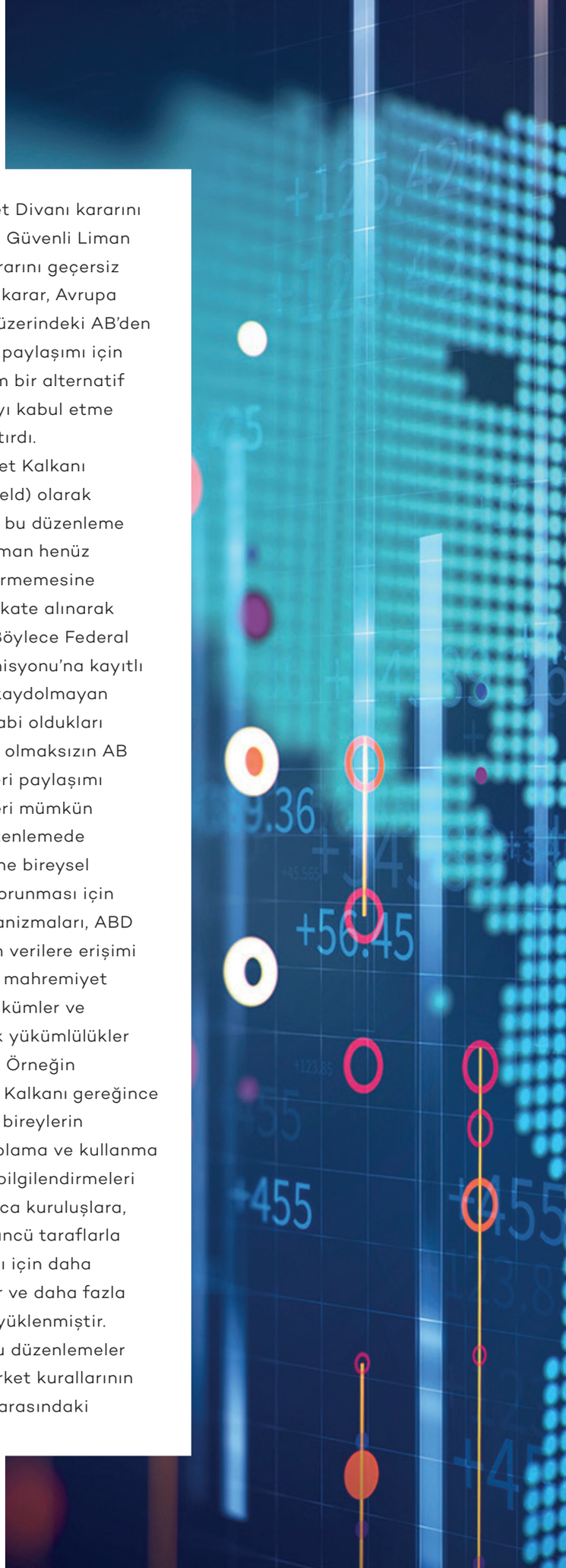
Şirketlerin veri paylaşımı için yeniden model hükümleri kullanmaları ve büyük bir evrak işi ile uğraşmaları anlamına geleceğinden Güvenli Liman İlkelerinin yerini alacak düzenleme Avrupa Komisyonu ve ABD müzakereleri sonucu oluşturuldu. Öncelikle Avrupa komisyonu Güvenli Liman'ın zayıf yönlerini ele alan ve geçerli bir mekanizma olarak kalmasını sağlamayı amaçlayan on üç öneride bulundu. Bu öneriler, ABD yetkilileri tarafından şeffaflık, tazmin, icra ve verilere erişim olmak üzere dört geniş öncelik üzerine odaklanarak incelendi. Haziran 2014'te, daha sonra Adalet Komiseri Viviane Reding, ABD Ticaret Bakanlığı'nın Komisyon'un on üç tavsiyesinin on ikisini kabul ettiğini bildirdi. Ancak, çekişmeli konu, ulusal güvenlik istisnasının sadece gerekli ve orantılı olduğu zaman uygulanması gerektiği yönündeki son tavsiyeydi.

Güvenli Liman'ı geçersiz kabul edilmesinde asıl etkili olay ise İrlanda Veri Koruma Kurumu'na, Facebook İrlanda ile kişisel verilerin Amerika Birleşik Devletleri'ne paylaşılmasının sona erdirilmesini talep eden Avusturyalı hukuk öğrencisi Maximilian Schrems tarafından yapılan şikayettir. Schrems, Facebook İrlanda'nın – Facebook'un Avrupalı kullanıcılar bakımından veri sorumlusu olduğunu ve artık (ABD istihbarat ajanslarının olduğu gibi) bu verilere sahip olduğu geniş erişim nedeniyle ABD'ye yapılan paylaşımları meşrulaştırmak için Güvenli Limanın hukuki çerçevesine güvenilemeyeceğini iddia etti.

Şikâyet daha sonra İrlanda Yüksek Mahkemesine oradan da AB hukukunun yorumlanmasına ilişkin en yüksek yargı makamı olan Avrupa Birliği Adalet Divanı'na (ABAD) iletildi. 6 Ekim 2015 tarihinde, Avrupa Birliği Adalet Divanı kararını yayınladı ve Güvenli Liman yeterlilik kararını geçersiz ilan etti. Bu karar, Avrupa Komisyonu üzerindeki AB'den ABD'ye veri paylaşımı için daha sağlam bir alternatif mekanizmayı kabul etme baskısını artırdı.

Mahremiyet Kalkanı (Privacy Shield) olarak adlandırılan bu düzenleme GDPR (o zaman henüz yürürlüğe girmemesine rağmen) dikkate alınarak hazırlandı. Böylece Federal Ticaret Komisyonu'na kayıtlı şirketlerin, kaydolmayan şirketlerin tabi oldukları kısıtlamalar olmaksızın AB ile kişisel veri paylaşımı yapabilmeleri mümkün oldu. Bu düzenlemede veri ilgililerine bireysel haklarının korunması için çözüm mekanizmaları, ABD hükümetinin verilere erişimi bakımından mahremiyet sağlayıcı hükümler ve şirketlere ek yükümlülükler getirilmiştir. Örneğin Mahremiyet Kalkanı gereğince kuruluşların bireylerin verilerini toplama ve kullanma konusunda bilgilendirmeleri gerekir. Ayrıca kuruluşlara, verilerin üçüncü taraflarla paylaşılması için daha katı koşullar ve daha fazla sorumluluk yüklenmiştir.

Aslında bu düzenlemeler bağlayıcı şirket kurallarının ABD ile AB arasındaki



veri paylaşımı konusunda tercih edilen bir yöntem olmadığını göstermektedir. Böyle bir yaklaşımın nedeninin ulusal veri koruma mevzuatı olmayan ülkeler bakımından bağlayıcı kurumsal kuralların istenilen sonucu sağlayacak olmaması olduğunu düşünüyoruz. Çünkü son yıllarda yapılan ve özellikle Kaliforniya Eyaleti'ni kapsayan veri koruma düzenlemelerini göz ardı edersek şirketlerin yükümlülüklerini yerine getirecekleri ve bağlayıcı kurumsal kuralları da ona göre düzenleyecekleri bir kişisel veri mevzuatı ABD'de bukunmamaktadır.

ABD'de eyaletler temelinde kişisel veriler düzenlenmektedir. Bu da şirketlerin iş ilişkisi içine girdikleri her eyalet için farklı yükümlülükleri yerine getirmeleri anlamına gelmekte, bu da şirketler için hem maliyetin artmasına hem de zaman kaybına neden olmaktadır. Bu durumun önüne geçmek için son zamanlarda özellikle Kaliforniya eyaletindeki düzenlemelere benzer tüm ABD'de genelinde geçerli olacak bir veri koruma yasasının önümüzdeki yıllarda düzenleneceğinin en büyük göstergesi olmaktadır.

1998 TARİHLİ BÜYÜK BRİTANYA VERİ KORUMA KANUNU'NUN İLKELERİ BAKIMINDAN BAĞLAYICI ŞİRKET KURALLARI

Bağlayıcı kurumsal kurallar 95/46/EC sayılı Direktif'in yürürlükte olduğu dönemde oluşturulmuştur. Ama kurallar oluşturulurken tek etkilenen düzenleme Direktif değildir.

Büyük Britanya Krallığı (günlük kullanımda İngiltere olarak bilinen ülke) tarafından 1998 yılında Veri Koruma Kanunu (Data Protection Act 1998) kabul edilmiştir. Kanun 95/46/EC sayılı Direktif'in yükümlülüklerini yerine getirmek amacıyla oluşturulmuş olup (1981 tarihli Avrupa Konseyi Veri Koruma Sözleşmesi'nin gerekliliklerini de karşılamaktadır) 1984 tarihli Veri Koruma Kanunu'nu ilga etmiştir.

1998 tarihli Veri Koruma Kanunu kendisini bireylerle ilgili bilgilerin işlenmesine dair hükümler olarak tanımlamaktadır. Aslında sonuçları itibariyle bu cümle düşünülmeye değer bir cümledir. Çünkü her kamu kurumu, her şirket, hatta bilgisayarı olan her kişi de işleme yapmaktadır. Buradan da herkese yükümlülük yüklediği şeklinde bir sonuç çıkarılmaktadır.

Bu yasa ile belirlenebilir gerçek kişilerin verilerinin işlenmesi düzenlenmiştir. Bu yasanın oluşturulmasının altında iki düşünce yatmaktadır. İlki kişisel verilerin işlenirken gizliliğini sağlamak, ikincisi ise ülkeler arasındaki veri akışının devamını sağlamaktır. Aslında açıkça görülüyor ki GDPR da dahil olmak üzere kişisel verilere ilişkin yapılan tüm düzenlemelerin temelinde aynı düşünceler yatmaktadır. Teknolojinin gelişmesiyle yalnızca kişisel verileri koruma düzenlemeleri değişmiş ve gelişmiştir.

Bağlayıcı kurumsal kurallar üzerindeki etkisinden dolayı 1998 tarihli Veri Koruma Kanunu çok önemlidir. 1998 tarihli Veri Koruma Kanunu'nda toplamda sekiz tane ilke düzenlenmişti. Bunlar; adil olma ve hukuka uygunluk ilkesi, amaç ilkesi, yeterlilik ilkesi, doğruluk ilkesi, saklama ilkesi, haklar ilkesi, güvenlik ilkesi ve uluslararası paylaşım ilkesidir. GDPR'da da bu ilkelere benzer ilkeler düzenlenmiştir. Farklı olarak GDPR'da hesap verilebilirlik ilkesi düzenlenirken haklar ve uluslararası paylaşım ile ilgili ilkeler düzenlenmemiş olup bu konular bölüm üçte ve bölüm beşte ayrıntılı olarak ele alınmıştır.

Bağlayıcı kurumsal kurallar bakımından önemli olan ise sekizinci ilkedir. Sekizinci ilkeye göre, "Kişisel verilerin işlenmesi kapsamında veri ilgilisinin hak ve özgürlükleri için yeterli koruma

sağlanmadığı takdirde Avrupa Ekonomik Alanı dışındaki bir ülkeye veya bölgeye veri paylaşımı yapılamaz.".

İlke, veri paylaşımı bakımından şirketlere kendi denetimlerini gerçekleştirme imkânı da verir. Ancak AEA dışındaki bir ülkeye paylaşımı yapılması durumunda denetimin sınırlı olacağı açıktır. GDPR kişisel verilerin korunmasında ana düzenleme olmasına rağmen GDPR'ı etkilediği ve GDPR'ın mantığına da uymasından dolayı sekizinci ilke bağlayıcı şirket kurallarından bahsedilirken değinilmesi gereken bir ilkedir.

Büyük Britanya Krallığı GDPR'ın kabul edilmesinin ardından GDPR'a uyumu sağlamak için 2018 yılında Veri Koruma Kanunu'nu (Data Protection Act) yürürlüğe koymuştur. GDPR, AB üyesi her ülke için geçerli olmakla birlikte GDPR ülkelere kendi "kişisel verilerin korunması mevzuatını" yapma yetkisi de tanımaktadır. 2018 yılında kabul edilen yasa da GDPR'ın bir nevi açıklaması niteliğindedir. Bu nedenle de GDPR ile 2018 yılında kabul edilen Veri Koruma Kanunu'nun birlikte okunması gereklidir. Kanun da GDPR standartlarını uygulamaktadır. Ancak GDPR düzenlemelerini ulusal düzeyde uygulanacak şekilde yasalaştırmıştır. Örneğin, Veri Koruma Kanunu'nda (2018) GDPR'da yer almayan göç ile ilgili özel veri işleme düzenlemesi yapılmıştır.

BAĞLAYICI ŞİRKET KURALLARININ TAŞIMASI GEREKEN KRİTERLER

Bağlayıcı şirket kuralları kapsamında veri ilgilileri, tek taraflı teşebbüslerin (mümkünse ulusal yasalar uyarınca) hukuki etkileri ya da (bunu mümkün kılan şirketler grubunun üyeleri arasındaki) sözleşme düzenlemeleri bakımından üçüncü taraf lehtarlar olmalıdır. Başka bir deyişle bağlayıcı şirket kuralları veri ilgililerine kişisel verileri konusunda haklar tanımalıdır.

Kurallarda tüm şirketler grubuna uygulanan zorunlu yasal yükümlülüklerin bu kuralların uygulanmasını engelleyebileceğine ilişkin açık bir hüküm de yer almalıdır. Hüküm doğası gereği kişisel verileri koruma taahhütlerini yerine getirme konusunda olumsuz bir etkiye sahiptir. Ancak mevzuata uyum öncelik olduğundan böyle bir hükmün yer alması gereklidir. Böyle bir durum ile karşılaşıldığında (soruşturmanın gizliliği vb. bir durum yok ise) Avrupa Birliği'ne bilgi verilmelidir. Avrupa Birliği yetkili veri koruma otoritesine danışarak ne yapılması gerektiğine ilişkin karar alır ve kararı uygulaması amacıyla şirkete kararı bildirir.

Belirtmek gerekir ki tüm grup şirketine uygulanan ve demokratik toplum gerekliliklerinin ötesine geçmeyen zorunlu yasal gereklilikler bağlayıcı şirket kurallarıyla çelişmemektedir. Çelişmeyen bu yükümlülüklere suç gelirlerinin aklanmasına karşı raporlama veya vergi raporlaması yükümlülükleri örnek gösterilebilir. Bu yükümlülükler konusunda da şüpheye düşülmesi durumunda şirket grupları de yetkili Veri Koruma Otoritesine danışmalıdır.

BAĞLAYICI ŞİRKET KURALLARININ BAĞLAYICI NİTELİĞİ

Şirketler, veri işleme ihtiyaçlarına farklı yasal ve kültürel arka planlar ile farklı iş felsefeleri ve uygulamaları temelinde yanıt verir. Bu unsurlarla ilgili olarak neredeyse her çok uluslu şirketin bu konuya farklı bir şekilde yaklaştığını söylemek mümkündür. Bu farklılıklara rağmen (yurtdışına veri paylaşımı yapılırken kişisel verileri korumak amacıyla kullanılacak) bağlayıcı şirket kurallarının en önemli özelliği kurallarının hem içeride hem de dışarıda bağlayıcılığıdır.

Bağlayıcılık niteliğinin daha iyi anlaşılması ve olası karışıklıkların önüne geçilebilmesi amacıyla kurallara uygunluk ve yasal olarak uygulanabilirlik kavramlarının bu kurallarla olan ilişkisinden bahsedilmesi gereklidir. Bağlayıcı şirket kurallarının bağlayıcılığı bu iki hususun ortak değerlendirmesini ifade eder. Başka bir deyişle yapılan tek taraflı taahhütlerin veya aynı etkiyi yaratan sözleşmelerin sadece yasal olarak uygulanabilirliğinin değerlendirilmesi, özellikle veri ilgililerinin hakları bakımından, orantısız bir çaba gerektirebileceğinden uygulanabilirliğin de değerlendirilmesi gereklidir yani uygulamada da bağlayıcı olması sağlanmalıdır. Uygulamada kuralların bağlayıcı niteliği, ancak çalışanlara eğitim verilmesi ve aykırı davranılması durumunda disiplin prosedürlerinin işletilmesi ile sağlanabilir. Özellikle disiplin prosedürlerinin varlığı ile çalışanlar kuralları uygulama zorunluluğunu hissedecektir. Aksi bir durum veri ilgililerine kâğıt üzerinde haklar tanırken haklarını fiilen kullanamamalarına neden olacaktır. Aslında bağlayıcılık niteliği de tüm bunları ifade etmektedir. Özetle bağlayıcı şirket kuralları hem yasal mevzuata uygun olmalı hem de uygulayıcı süjeler için geçerli olmalıdır.

BAĞLAYICI ŞİRKET KURALLARININ BAŞVURUSU

Şirketler bağlayıcı şirket kurallarını uygulayabilmek için veri koruma otoritelerine onay için başvurmalıdırlar. GDPR'ın 63. maddesindeki "Bu Tüzük'ün Birlik içerisinde tutarlı bir şekilde uygulanmasına katkıda bulunulması amacıyla, denetim makamları, bu kesimde belirtilen tutarlılık mekanizması vasıtasıyla, birbirleriyle ve uygun olduğu hallerde, Komisyon ile işbirliği yapar." düzenlemesine göre tutarlılık mekanizmasına uygun bir şekilde ilgili otorite tarafından onaylanacaktır.

Bağlayıcı şirket kurallarının onaylanması için başvuran veri sorumlusunun birden fazla ülkede tüzel kişiliği olması durumunda tüzel kişiliklerin olduğu tüm ülkelerdeki veri koruma otoritelerine bu başvuru yapılmalıdır. Veri Koruma Otoritesi taslak kararını, bağlayıcı şirket kuralları hakkında görüş bildirecek olan Avrupa Veri Koruma Kuruluna (EDPB) bildirir. Bağlayıcı kurumsal kurallar EDPB görüşüne uygun olarak tamamlandığında, yetkili makam olan Veri Koruma Otoritesi kuralları onaylar.

Onay vermek için yapılan değerlendirme kişisel verilerin yurtdışına aktarılması sırasında verileri korumak için veri sorumlusu tarafından taahhüt edilen güvencelerden oluşur. Bu nedenle, bu uygulama Direktifin 27. maddesinde belirtilen davranış kurallarının onaylanmasından, yani belirli bir sektördeki ulusal veri koruma mevzuatının pratikte uygulanmasına yönelik mesleki kurallardan farklıdır. Bir şirket grubunun iç kuralları, veri koruma yükümlülüklerinin yerine geçemez. Ulusal yasalara uyum elbette herhangi bir yetki verilmesi için olmazsa olmaz koşuldur. Bağlayıcı kurumsal kuralların onayı için aşağıdaki prosedürün izlenmesi gereklidir:

Öncelikle (tüm AEA üye devletleri tarafından kullanılabilen) formun baş yetkili olduğu düşünülen Veri Koruma Otoritesi'ne sunulması gereklidir. Baş yetkili Veri Koruma Otoritesi tüm otoritelerle koordinasyonu sağlayarak AEA bünyesinde bağlayıcı kurumsal kuralların onay prosedürünü işleten otoritedir. Başvuran bir şirket grubu, aşağıdaki kriterler kapsamında baş yetkili veri otoritesi seçimini temellendirmelidir:

a. Grubun Avrupa genel merkezinin bulunduğu yer;
b. Veri koruma sorumlulukları olan şirketin, grup içindeki yeri;
c. Grupta bağlayıcı kurumsal kuralları uygulamak için en iyi olan şirketin (yönetim fonksiyonu, idari yük vb. açısından) yeri;
d. İşlemenin amaçları ve araçları açısından çoğu kararın alındığı yer;
e. AB içinde olup da AEA dışında en fazla paylaşım gerçekleşecek üye ülkeler.

Veri koruma otoritelerinden bir tanesi bağlayıcı şirket kurallarının onayı bakımından baş yetkili konumundadır. Baş yetkili olan otoritenin belirlenebilmesi amacıyla form, Veri Koruma Otoritesi tarafından şirketin onay almak istediği tüm otoritelere gönderilir. Baş yetkili otoritenin belirlenmesinin ardından yetkili otorite onay başvurusu yapan şirkete bildirilir. Ardından baş yetkili otorite, bağlayıcı kurumsal kurallar dahil olmak üzere formun tamamını göndererek (karar vermek için) ilgili tüm otoritelerle iş birliğini sağlar. Sonrasında ise baş yetkili otorite taslak kararını Avrupa Veri Koruma Kurulu'na bildirir. Avrupa Veri Koruma Kurulu'nun görüşüne uygun olarak bağlayıcı kurumsal kararlar tamamlandıktan sonra otorite tarafından onaylanır. Onaylanan kuralların birer örneği bu sefer AEA içindeki tüm veri koruma otoritelerine gönderilir.

Onaylanma süreci yaklaşık 16 - 17 ayı bulmaktadır. 5 ay baş yetkili otorite tarafından başvurunun değerlendirilmesi, 3- 4 ay diğer otoritelerle karşılıklı tanıma ve iş birliği prosedürün işletilmesi ve 8 ay da başvurana cevap verilmesi sürmektedir.

Söz konusu başvuru formu temelde üç bölümden oluşmaktadır. Birinci bölümde başvurucunun ve grup şirketinin yapısına ilişkin bilgiler yer alır. İkinci bölümde veri akışına ilişkin kısa bir bilgi verilir.

Söz konusu başvuru formu temelde başvuran bilgisi ve arka plan belgesi olmak üzere iki bölümden oluşur. Birinci bölümde, başvuran ve grup şirketinin yapısına, veri akışına ve baş yetkili Veri Koruma Otoritesi'nin belirlenmesine ilişkin bilgiler yer alır. Veri akışı ile ilgili bilgi verilirken veri paylaşımının doğasından, amacından ve paylaşım yapılan kişilerden bahsedilir. Veri Koruma Otoriteleri başvuranın belirlemesi ile bağlı olmayıp, yukarıda da belirttiğimiz üzere başka bir otoriteyi baş yetkili seçebilirler.

Formda kuralların ihlal edildiği iddiasıyla ilgili olarak ispat yükünün, paylaşımın merkezinde veya Avrupa Birliği'nin merkezinde ya da talebin nereden kaynaklandığına bakılmaksızın yetki verilmiş veri koruma sorumlulukları olan kuruluşun bir bölümüne

ait olduğu açıkça ifade edilmelidir. Formun devamında uygunluğu denetleyecek mekanizmalar öngörülmeli ve ülkenin iç hukukunun her otoritenin denetimine izin vermemesi ihtimaline binaen tüm otoritelerin denetleme yapabileceğine ilişkin izin verilmelidir. İkinci bölümün sonraki kısmında bağlayıcı şirket kuralları ile tüm otoriteler arasındaki koordinasyonun nasıl sağlanacağı belirtilmelidir. Ardından veri akışı ve veri işleme tanımlanarak kurallardaki değişikliklerin veri koruma otoritelerine bildirilmesi mekanizması ile verilerin korunması için taahhüt edilen güvenlik önlemleri açıklanmalıdır.

Formdaki alanların yetersiz kalması durumunda forma ek sayfa eklenmesi mümkündür. Forma eklenen bilgilerden bazılarının gizli tutulması gerektiği, ticari sır vb. olduğu belirtilebilir. Üçüncü bir tarafın bu bilgilerin açıklanmasına yönelik talebinin olması durumunda ulusal mevzuata uygun olarak Veri Koruma Otoritesi tarafından söz konusu bu talep değerlendirilir.

Belirtmek gerekir ki 2015 yılı itibariyle toplamda İngiltere (17), Hollanda (12), Almanya (7), Fransa (24), Belçika (1), İrlanda (1),

Malta (1), Lüksemburg (2) ve Danimarka (1) olmak üzere toplamda 66 tane BCR onaylanmıştır. 25 Mayıs 2018 itibariyle ise bu sayı 135'e çıkmıştır.

BAĞLAYICI ŞİRKET KURALLARINDA DEĞİŞİKLİK YAPILMASI

Zamanla oluşan iş faaliyetleri ile süreçlerindeki değişikliklere ve teknolojide gerçekleşen gelişmelere bağlı olarak kişisel verilerin paylaşımının da değişebileceğinden Madde 29 Çalışma Grubu tarafından şirketlerin bağlayıcı kurumsal kurallarda değişiklik yapabilecekleri öngörülmüştür.

Gerekli şartların yerine getirildiği takdirde onay için tekrardan başvurmak zorunda kalmaksızın bağlayıcı kurumsal kuralların güncellenmesi mümkündür. Böylece şirketlerin değişikliklere kolayca adapte olmalarına imkân verilmiştir. İlgili şartlar şu şekildedir:

- Verinin paylaşıldığı veri sorumlusu veya veri işleyenin kurallara etkili bir şekilde uyacağından emin olmadan kişisel veriler paylaşılmamalıdır.
- Şirket grubunun bir bölümü veya görevlendirilmiş bir kişi tarafından kurallardaki güncellemeler takip edilmeli, talep üzerine veri ilgililerine ve veri koruma otoritelerine gerekli bilgi sağlanmalıdır.
- Kurallarda yapılacak herhangi bir değişiklik, değişikliği haklı kılacak nedenler ve açıklamalarıyla birlikte ilgili Veri Koruma Otoritesi'ne yılda bir kez rapor edilmelidir.

TÜRK HUKUKU'NDAKİ YURTDIŞI VERİ PAYLAŞIM TAAHHÜTNAMELERİ İLE BAĞLAYICI ŞİRKET KURALLARININ İLİŞKİSİ

6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre, kişisel verilerin yurtdışına paylaşılmasında ana kural veri ilgilisinden açık rızasının alınmasıdır. Ancak yasa bazı şartların sağlanması durumunda yurtdışına paylaşım yapılırken açık rızanın alınmasının zorunlu olmadığını düzenlemektedir.

Açık rıza, yasanın 3. maddesine göre, "Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı" ifade eder. Bu rızanın konuya özel olması ve rıza alınmadan önce de konuya ilişkin olarak veri ilgilisinin aydınlatılması gereklidir. Ayrıca rıza bir hizmetin sunulmasının ön şartı olmamalıdır. Açık rıza veri ilgilisi tarafından istenilen zamanda geriye alınabileceğinden ticari hayatın sürdürülebilmesi için mümkün olduğunca açık rızayla kişisel veriler işlenmemeli, açık rıza olmaksızın veri işlemeye imkan veren istisnalar kapsamında faaliyetler sürdürülmelidir. Saniyeler içerisinde yurtdışıyla veri paylaşımının yapılabildiği günümüzde, ticaret gerçekleştirilirken bir veri ilgilisinin rızasını geri alması bile iş işleyişini büyük ölçüde etkileyecektir. Bu gibi durumların önüne geçmek için Kişisel Verilerin Korunması Hukuku, ticari faaliyetleri zorlaştırıcı bir etken olarak değil de ticari faaliyetler devam ederken kişisel verileri de koruyan bir hukuk olarak yorumlanmalıdır.

Türk Hukukunda yurtdışına veri paylaşımının istisnaları 6698 sayılı Kanun'un 9. maddesinde şu şekilde düzenlenmiştir:

"Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;
a) Yeterli korumanın bulunması,
b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir."

Hükme göre, kişisel veriler yurtdışı ile paylaşılırken paylaşılan ülkede ya yeterli koruma bulunmalı ya da veri sorumlusu tarafından kişisel verilerin korunacağına ilişkin bir taahhütname hazırlanarak Kurul'a onaylatılmalıdır. Aslında her iki şartın da gerçekleşebilmesi için Kurul tarafından güvenli olan ve olmayan ülkelerin açıklanması gereklidir. Ülkeler açıklandığında güvenli olan ülkelerde yeterli koruma olduğu kabul edildiğinden açık rıza almaksızın kişisel veriler aktarılabilir. Ancak bir ülkenin güvenli ülke olarak kabul edilebilmesi için o ülkenin de Türkiye'yi güvenli olarak kabul etmesi gereklidir. Şu an diplomatik nedenlerden dolayı hangi ülkelerin güvenli hangilerinin de güvenli olmadığı açıklanamamaktadır. Bu nedenle de şirketlerin şu an yurtdışı paylaşımı yaparken açık rıza almamalarından dolayı yapılan tüm paylaşımlar hukuka aykırılık oluşturmaktadır. Ancak son günlerde Cumhurbaşkanlığı tarafından yapılan basın açıklamalarında yurt dışına veri aktarımı konusunda mevzuat değişikliğine gidileceği ve bu sorunun bir çözüme kavuşturulmak istendiği ifade edilmektedir.

Çalışmamızın konusu bakımından asıl önemli olan ise taahhütname hazırlanması ve bunun Kurul tarafından onaylanmasının şartlarıdır. Özellikle Amazon Türkiye şirketlerinin yapmış olduğu taahhütname başvurularının kabul edilmesi nedeniyle bu yöntem daha da önem kazanmıştır. Taahhütnamelerin taşıması gereken asgari unsurlar yasanın yine aynı maddesinin devam eden fıkrasında düzenlenmiştir. Fıkraya göre taahhütname,

"a) Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,
ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri,"

içermelidir.

Bağlayıcı şirket kurallarının taşıması gereken unsurlar ile taahhütnamenin unsurları (ya da sağlaması gereken şartlar) karşılaştırıldığında bağlayıcı kurumsal kuralların unsurlarının daha fazla olduğu ve daha ayrıntılı bilgi istediği görülmektedir. Bağlayıcı şirket kuralları KVKK'nın yurt dışına veri aktarımına ilişkin şartlarından farklı olarak şirketin yapısına, baş yetkili Veri Koruma Otoritesine ve otoritelerin denetleme yetkisine ilişkin unsurlar barındırır. Bu farklılıkların nedeni AB'de geçerli olan GDPR'ın (öncesinde Direktif'in) tüm AB ülkelerinde geçerli tek bir düzenleme olmasından ama AEA'de çok sayıda Veri Koruma Otoritesi olmasından dolayıdır. Türkiye'de ise kişisel verilerin korunması konusunda tek yetkili otorite Kişisel Verilerin Korunması Kurumu'dur. Bu nedenle şirketleri tek denetleme yetkisine sahip olan kurumdur. Şirketlerin de baş yetkili bir otorite veya diğer kurumların denetleyebileceğini kabul etmesi gibi bir durum söz konusu değildir. Diğer unsurlar bakımından ise taahhütname ile kuralların unsurları benzerlik göstermektedir.

SONUÇ

Yukarıdaki hususlarla birlikte değerlendirdiğimizde taahhütnameleri benzerliklerine rağmen bağlayıcı şirket kuralları olarak değerlendirmek mümkün değildir. Ancak, 2019-2023 11. Kalkınma Planı'nda da kişisel verilerin

korunması mevzuatının GDPR'a benzetileceğinin ve değişikliklerin de bu kapsamda yapılacağının belirtilmesinden dolayı ülke bazında hazırlanan taahhütnamelerin sonrasında şirket bünyesinde yurtdışına yapılan tüm veri paylaşımlarını kapsayıcı nitelik alacağını, bağlayıcı şirket kuralları halini alacağını ve taahhütnamelere de bu bakış açısıyla bakılması gerektiğini düşünüyoruz.

Türkiye açısından Bağlayıcı Şirket Kurallarının nasıl uygulanacağı ise hala belirsizliğini korumaktadır. Bu konuda Kurul tarafından 10 Nisan 2020 tarihinde bir ilan yapılmış, ilan ekinde başvuru formu ve temel huşulara ilişkin yardımcı doküman yayınlanmıştır. Ancak bildiğimiz kadarıyla henüz sonuçlanmış bir başvuru bulunmamaktadır. Öte yandan yakın gelecekteki beklenti, özellikle yurt dışına veri aktarımını kolaylaştırmak ve bu konudaki tıkanıklığın önünü açmak için KVKK mevzuatında önemli değişikliklerin yapılması, mevcut mevzuatın daha fazla GDPR'a yaklaştırılmasıdır. ■

KAYNAKÇA

Avrupa Parlamentosu Araştırma Servisi, From Safe Harbour to Privacy Shield, Temmuz 2017.

Jan Dhont, Binding Corporate Rules: Building A Future- Proof Privacy Cmpliance Solution, 2015,https://www.slideshare.net/JanDhont1/20150318-gac-presentation-bcr-05052015-48184562,Erişim Tarihi: 23.01.2020.

Madde 29 Çalışma Grubu, Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, 10 Temmuz 2007.

Madde 29 Çalışma Grubu, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers 3 Haziran 2003.

Madde 29. Çalışma Grubu, Working Document Setting up a Framework For The Structure of Binding Corporate Rules, 24 Haziran 2008.

Madde 29. Çalışma Grubu, Working Document Setting Forth a Co- Operation Procedure For Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", 14 Nisan 2005.

Lokke Moerel, Binding Corporate Rules, 1. Baskı, Oxford Yayınları, İngiltere, 2012.

Türkiye Cumhuriyeti Cumhurbaşkanlığı, Strateji ve Bütçe Başkanlığı, 2019-2023 11.Kalkınma Planı, Temmuz 2019

Samantha Cutler, The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information, Boston College Law Review, Cilt 59, Sayı 4.

Paul Lambert, Understanding The New European Data Protection Rules, Boca Raton, CRC Press, 2017.

Peter Carey, Data Protection, Oxford, 5.Baskı, Oxford University Express, 2018.

Paul Voigt/ Axel von dem Bussche, The EU General Data Protection Regulation, Cham, Springer Iternational Publishing, 2017.

Rolf H. Weber/ Dominic Staiger, Transatlantic Data Protection in Practice, Berlin, Springer-Verlag GmbH, 2017

Stewart Room, Data Protection& Compliance in Context, Swindon, BCS, 2007, s.1-3.

İNTERNET SİTELERİ

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#approval-of-binding-corporate-rules,Erişim Tarihi: 19.01.2020.

https://ico.org.uk/for-organisations/binding-corporate-rules, Erişim Tarihi: 24.01.2020.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/, Erişim Tarihi: 24.01.2020.

https://en.wikipedia.org/wiki/Data_Protection_Act_1998, Erişim Tarihi: 25.02.2020.

https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles, Erişim Tarihi: 25.01.2020.

https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, Erişim Tarihi: 25.01.2020.

https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-