www.kvkk.gov.tr
Kişisel Verileri Koruma Dergisi
Cilt:4 Sayı:2
Geliş:01.11.2022
Kabul:30.11.2022

Birleşme Devralma Süreçlerinde Due Diligence Aşamasının Kişisel Verilerin Korunması Hukuku Paralelinde Değerlendirilmesi

Ozan, AKMAN
Leiden Üniversitesi, L.L.M, Amsterdam, Hollanda
ORCID ID: 0000-0003-3089-9371
Naz CALAY
Avukat, L.L.M, İstanbul, Türkiye
ORCID ID: 0000-0001-6348-5971

ÖZ
Şirket birleşme ve devralma süreçlerinin due diligence aşamaları hedef şirket ve alıcı arasında veri paylaşımının yoğun olduğu işlemlerdir. Süreç boyunca alıcı, birleşme devralma sürecine ilişkin isabetli bir ticari karar verebilmek adına hedef şirkete ilişkin mümkün olduğunca veri edinmek, edindiği veriler ışığında işlemin barındırdığı riski değerlendirmek ister. Bu amaç doğrultusunda due diligence çalışması kapsamında hedef şirketin finansal, hukuki, vergisel, çevresel, insan kaynakları gibi pek çok konudaki durumu analiz edilir ve kaçınılmaz olarak birçok farklı kategoriden, çok fazla miktarda kişisel veri işlenir. İşlemeye konu edilen veriler arasında özel nitelikli kişisel verilerin de bulunması muhtemeldir. Due diligence sürecinde gerçekleşen kişisel veri işleme faaliyetleri, kişisel verilerin korunması mevzuatı ve veri koruma hukuku ilkeleri paralelinde gerçekleştirilmelidir. Bu makale, due diligence süreçlerinde doğabilecek hukuka aykırı veri işleme hallerini ve kişisel verilerin mevzuata uygun olarak işlenmesindeki pratik zorlukları göz önünde bulundurarak, sürecin veri koruma hukukuna uygun gerçekleştirilmesi yönünde tespitler yaparak çözüm önerileri sunacaktır.
Anahtar Sözcükler: Birleşme Devralmalar, Kişisel Verilerin Korunması, Due Diligence, Veri Koruma Hukuku İlkeleri

Evaluation of Due Diligence Phase In Mergers and Acquisitions In Line With Data Protection Law

ABSTRACT
The due diligence stage of mergers and acquisitions is a process during which an intensive data sharing occurs between the target and buyer companies. During the process, the buyer aims to obtain as much data as possible about the target company in order to make an accurate commercial decision by evaluating the risk factors that the target company may have. In line with this purpose, the target company's situation is analyzed with regards to many areas such as financial, legal, human resources, tax, and environmental matters, whereby large amount of personal data of different categories is processed inevitably. It is highly likely that sensitive data will also be processed during these data processing activities. Data processing activities that have been made during the due diligence stage should be carried out in accordance with the principles of data protection legislation and data protection law. This article will consider the unlawful data processing situations that may arise in due diligence processes and the practical difficulties in the processing of personal data in accordance with the legislation, and will provide solutions to prevent such incompliance.
Keywords:Mergers and Acquisitions, Data Protection, Due Diligence, Data Protection Principles

Atıf Gösterme	Akman, O., Calay, N., (2022). Birleşme Devralma Süreçlerinde Due Diligence Aşamasının Kişisel Verilerin Korunması Hukuku Paralelinde Değerlendirilmesi, *Kişisel Verileri Koruma Dergisi. 4*(2), 19-33. DOI:

GİRİŞ

Günümüz teknolojisinin sunduğu imkanlar, gözetim ve bilişim teknolojilerindeki esaslı gelişmeler kişisel verilerin işlenmesini kolaylaştırmış olup kişisel verilerin korunmasına yönelik ihtiyacı gündeme getirmiştir. Özellikle 2000'li yıllardan itibaren internetin birey yaşantasında edindiği hayati konum, dijitalleşme ve kişisel veri toplama imkanları doğrultusunda ticaret şirketlerinin edinebileceği sınırsız avantajlar, toplumların kişisel verilerin korunmasına yönelik ihtiyacın bilincine varmasını sağlamıştır. Ancak kişisel verilerin korunmasına yönelik çalışmaların bu tarihten çok daha öncesine dayandığı görülmektedir. Nitekim bu doğrultudaki ilk çalışmaların 1960 yıllarında Amerika Birleşik Devletlerinde yapıldığı, 1970 senesinde ise Almanya'nın Hessen Eyaletinde ilk kez bir ulusal veri koruma kanunun yayımlandığı görülmektedir (Turan, 2017 sf.55-56). Öte yandan, kişisel verilerin korunmasına yönelik ilk uluslararası antlaşma olan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, Avrupa Konseyi tarafından 1981 senesinde imzaya açılmış ve Türkiye tarafından 1985 yılında imzalanmıştır. Ulusal düzeyde bakıldığında, kişisel verilerin korunması, Avrupa Birliği ("AB") uyum süreci kapsamında 7 Mayıs 2010 tarihinde T.C. Anayasası'nın ("Anayasa") 20. Maddesine eklenerek anayasal hak statüsünü elde etmiş, ve 7 Nisan 2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ile kişisel verilerin korunması, kanuni dayanağa bağlanmıştır. Kanun'un, büyük ölçüde Avrupa Birliği'nde halihazırda uygulamada olan 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğünden ("GDPR") önce yürürlükte bulunan 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifinden ("Direktif") esinlendiği görülmektedir.

Ticaret şirketleri, ticari faaliyetleri kapsamında gerçekleştirdikleri tüm işlem ve eylemlerde, kaçınılmaz olarak ciddi miktarda kişisel veri işlemektedir. Bu bağlamda, kişisel verilerin korunmasına uyum, ticaret şirketlerinin hem üçüncü kişilerle meydana getirdikleri tüm işlemlerde hem de kendi iç süreçlerinde, kapsamlı bir sorumluluğunu gündeme getirmektedir. Ticari hayatın şirketler için vazgeçilmez işlemlerinden olan, çoğunlukla ekonomik anlamda yüksek hacimli işlemler olarak karşımıza çıkan birleşme devralma işlemlerinde, taraflar arasında çok fazla kişisel verinin aktarıldığı, işlendiği, ve süreç boyunca muhafaza edildiği görülmektedir. Bu durum ise tarafların birleşme devralma süreçlerindeki işlemlerini, kişisel verilerin korunması mevzuatına uyumlu bir biçimde gerçekleştirmesinin önemini yadsınamaz kılmaktadır. Şüphesizdir ki, ticari hayatın akışı içerisinde, birleşme devralma işlemi taraflar açısından karar vermesi son derece güç bir işlem olabilir. Nitekim bir şirketin paylarının alınması, bir ticari işletmenin satın alınması ya da şirketlerin aynı çatı altında bir araya gelmesi kendi içerisinde pek çok risk barındırır. Bu sebeple de hedef şirket ile gerçekleştirilecek bir birleşme devralma işleminde, due diligence yapılarak risklerin öngörülmesi ve hesaplanması sürecin en önemli etaplarından birini ifade eder. Zira, belirlenen riskler doğrultusunda birleşme devralma işleminin bedeli de değişecektir (Esin, 2021, sf.116-131). Bu sebeple, alıcının ticari ve stratejik bir planlamayı doğru biçimde yapabilmesi için, hedef şirkete ilişkin gerekli, yeterli ve doğru bilgilere ulaşması gerekmektedir. Due diligence sürecinin temel amaçları doğrultusunda, bu süreç kısaca; hem satın alma hem birleşme işlemlerinde hedef şirketin birleşme devralma işleminden önce ayrıntılı bir biçimde incelemesi olarak tanımlanabilir (Pulaşlı,2007, sf. 211).

Due diligence ile amaçlanan hususlar ve birleşme devralma süreci için taşıdığı önem göz önünde bulundurulduğunda, Due diligence süreci boyunca taraflar arasında gerçekleşecek olan kapsamlı veri alışverişinde, Kanun'un 3(1)-d maddesinde "kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgi" biçiminde tanımlanan birçok farklı kategoride kişisel verinin de aktarılacağı, muhafaza edileceği, kaydedileceği, devredileceği ve depolanacağı şüphesizdir. Bu makale, kişisel verilerle yapılan tüm bu işlemlerin due diligence süreci kapsamında kişisel verilerin korunması hukukuna uygun bir biçimde

gerçekleştirilmesine yönelik olarak pratik uygulamalara dönük değerlendirme yaparak çözüm önerileri sunacaktır.

Kanun'da Belirtilen Şartlar Çerçevesinde Due Diligence Süreçlerinde Kişisel Verilerin İşlenmesi

Kanun, dayanağı olan Direktif ve halihazırda AB uygulamasında olan GDPR'daki kavram tanımına benzer olarak, kişisel verilerin işlenme faaliyetini 3 (1)-e) maddesinde; kişisel verilerin tamamen veya kısmen otomatik olan veya bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesini, kaydedilmesini, depolanmasını, muhafazasını, değiştirilmesini, yeniden düzenlenmesini, açıklanmasını, aktarılmasını, devralınmasını, elde edilebilir hale getirilmesini, sınıflandırılmasını ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her işlemi, işleme faaliyeti olarak kabul etmektedir.

Madde metninden anlaşıldığı üzere, kişisel verileri konu alan bir faaliyetin, işleme faaliyeti sayılabilmesi noktasındaki ayırt edici nokta; bu faaliyetin otomatik veya kısmen otomatik yollarla ya da belirli bir veri kayıt sisteminin parçası olarak vuku bulmasıdır. Bu kavramların somutlaştırılması adına belirtmekte fayda vardır ki; kişisel verilerin bilişim sistemleri üzerinden herhangi bir faaliyet vasıtasıyla işlenmesi otomatik işleme olarak sayılırken; herhangi bir sistem olmaksızın sadece insan müdahalesi ile işlenmesi, otomatik olmayan yollarla işleme sayılmaktadır (Dülger, 2020, sf. 183-184). İlaveten, otomatik olmayan yollarla yapılan işleme faaliyetinin, Kanun kapsamına girebilmesi için gerekli koşul olan "belirli bir veri kayıt sisteminin parçası olma" ifadesi, kişisel verilerin belirli şartlara dayalı olarak işlendiği sistemleri ifade etmekte olup hem fiziksel hem de elektronik ortamları kapsamaktadır (Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, 2019, sf. 30). Diğer bir deyişle, herhangi bir bilişim cihazı yardımı olmaksızın, manuel yollarla işlenen ve bir kategorizasyon olmaksızın gelişigüzel biçimde işlenen kişisel veriler, Kanun'un kapsamına girmemektedir.

Birleşme devralma süreçlerinin due diligence etabındaki kişisel veri işleme faaliyetlerinin; kişisel verilerin korunması hukuku kapsamında değerlendirilmesine geçilmeden önce, Kanun'un 3 (1) -ı) maddesinde belirtilen "Veri Sorumlusu" kavramının, alıcı şirket ve hedef şirket göz önünde bulundurularak değerlendirilmesi, anlatım bütünlüğünün sağlanması açısından önem arz etmektedir. Anılan madde hükmü uyarınca veri sorumlusu; "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişileri" ifade etmektedir. Buradan hareketle, otomatik, yarı otomatik veya otomatik olmayıp belirli bir veri kayıt sistemini kurarak ve yöneterek kişisel verilerin işleme ve metotlarını belirleyen kişiler, Veri sorumlusu olarak Kanun'un uygulamasının kapsamına girmektedir. Veri Sorumlusu kavramını makalenin konusu olan Birleşme devralma süreçlerinin due diligence etabında tarafların rolleri paralelinde incelediğimizde, hedef şirketin belirtilen veri sorumlusu tanımına gireceği gibi, alıcı şirket(ler)in de; hedef şirket ile birleşme devralma işlemine devam edip etmeme noktasında karar vermek amacıyla kişisel veri içeren belgeleri talep edip işledikleri noktada veri sorumlusu sıfatını haiz olacağından bahsedilebilecektir.

Due Diligence Sürecinde İşlemeye Konu Edilen Veri Kategorileri

Birleşme devralma işlemi öncesi gerçekleştirilen due diligence etabı ister alıcı ister satıcı tarafından gerçekleştirilmiş olsun süreç boyunca birçok farklı kategoriden, bir çok farklı kişiye ait kişisel veri işlenmektedir. Anılan iki tür due diligence çalışmasının kişisel verilerin işlenmesi noktasındaki temel farkı; alıcı tarafından yürütülmekte olan bir due diligence faaliyetinde, satıcı tarafa hedef şirketle ilgili bir belge talep listesi iletilecek ve bu bilgiler ile belgeler elektronik veya fiziki olarak organize edilen

veri odasında toplanmaktadır. Öte yandan satıcı tarafın yürüttüğü bir due diligence faaliyetinde, alıcı ile paylaşılacak bilgiler tamamen satıcının inisiyatifinde kalmaktadır. Dolayısıyla, alıcı tarafından gerçekleştirilen hedef şirkete dönük due diligence faaliyetinin, satıcının gerçekleştirdiği çalışmaya nazaran çok daha kapsamlı ve detaylı olmasının beklenmesi durumu, Kanun kapsamında süre gelmesi gereken yoğun bir kişisel veri akışı ve işleme faaliyetine sebep olacaktır. Alıcı taraf, kendisinin yürüttüğü bir due diligence çalışmasında, hedef şirketin faaliyetlerini göz önünde bulundurarak oluşturduğu bir bilgi-belge talep listesini satıcıya iletmekte ve bu bilgi ve belgeler de alıcı tarafından oluşturulan; günümüzde genellikle elektronik ortamda bulunan veri odalarında satıcının bilgi ve erişimine açılmaktadır. Bu sürecin yönetimi, tarafların birleşme devralma süreci boyunca kendilerini temsil eden vekillerinin desteğiyle oluşturdukları ekipler tarafından oluşturdukları uzman inceleme ekipleri vasıtasıyla gerçekleştirilmekte olup veri odasına erişim saatleri, veri odasına erişimde kimlik tespiti gibi kullanım şartları da belirlenmektedir (Kayalı, 2014 sf. 141).

Alıcı tarafın, henüz due diligence etabındayken hedef şirkete ilişkin riskleri tespit edebilmesi, ve risk hesaplamasını doğru yapabilmesi için, hedef şirketin; (i) iş hukuku, (ii)insan kaynakları, (iii) malvarlığı hukuku (iv) vergisel süreçler (v) finansal durum ve (vi) sözleşmesel süreçler gibi birçok farklı boyutuyla detaylı incelenmesi gerekmektedir. Sayılan konularda bilgilerin sağlanması, çok sayıda farklı kategoriden kişisel verinin işlenmesine sebebiyet vereceği gibi, işlenen bu kişisel veriler arasında Kanun'un 6 (1)'inci maddesinde sayılmış olan; "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" nin de bulunması mümkündür. Örneğin; alıcı şirket, devralma işlemini gerçekleştirmeden önce hedef şirketin taraf olduğu tüm hukuki uyuşmazlıkları incelemeyi talep edebilecektir. Bu noktada da hedef şirket işçilerine ait iş göremezlik raporu ve iş kazasına ilişkin dökümanlar vasıtasıyla işçilere ait özel nitelikli kişisel veriler statüsündeki sağlık verilerinin veri odalarında toplanması, işlenmesi gündeme gelebilecektir. Öte yandan, alıcı taraf birleşme devralma işlemine dair risk hesaplamasını doğru yapabilmek adına, hedef şirketin kıdem tazminatı, ihbar tazminatı ve yıllık izin ücret yükünü hesaplayarak hedef şirketi devraldığı bir ihtimalde şirket çalışanlarını azaltırsa doğacak ödeme yükünü öngörmeyi isteyebilecek ya da hedef şirket yöneticileri ve müdürleri kilit role sahip çalışanlarının iş sözleşmelerini ve özlük dosyalarını incelemeyi talep edebilecektir.

Bu bölümde anlatılan esaslardan hareketle, birleşme devralma süreçlerinin due diligence aşamasında gerçekleştirilen kişisel veri işleme faaliyetlerinin, Kanun'da öngörülen şartlar ve sistematiğe uygun bir biçimde, veri koruma hukukunun ilkeleri paralelinde gerçekleştirmesi gerekmektedir. Bu makalenin ilerleyen bölümleri kapsamında due diligence süreci; Kanun'da öngörülmüş bu ilke ve işleme şartları paralelinde incelenecektir.

Due Diligence Sürecinin Kanun'da Belirtilen Kişisel Veri İşleme Şartları Çerçevesinde Değerlendirilmesi

Kanun'un 5'inci ve 10'uncu Maddeleri arasında kişisel verilerin işlenmesine yönelik öngördüğü sistematik incelendiğinde; 5 (1)'inci maddesi uyarınca kural olarak ilgili kişilerin açık rızası olmaksızın herhangi bir kategoriden kişisel verinin işlenmeyeceği belirtilmiş, ancak aynı maddenin 2.fıkrasında liste halinde sayılan durumlarda da özel nitelikli olmayan kişisel verilerin ilgili kişinin açık rızası aranmaksızın da işlenebileceği kaleme alınmıştır. Birleşme devralma sürecinde gerçekleştirilen due diligence çalışması kapsamında kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinde yer alan "İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması" hukuki sebebine dayandığı kabul edilmektedir (Örneklerle Kişisel Verilerin Korunması Kanunu Rehberi, 2019, sf. 17).

Belirtmekte fayda vardır ki, Kanun'un 5(2)-f maddesinde belirtilen, "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için zorunlu olma" hukuki sebebi, ölçüsüz biçimde veri işlenmesine dair sınırsız ve genel bir yetki olarak değerlendirilmemelidir. Nitekim, bu hukuki sebebe dayalı olarak yapılan kişisel veri işleme faaliyetleri, Kanun'un 4'üncü maddesinde belirtilen veri koruma ilkeleri ile birlikte yorumlanmalı, kişisel verilerin toplanma amacı o hedef şirkete ilişkin yeterli bilginin sağlanması amacına bağlı ve ölçülülük ilkesine riayet ederek gerçekleştirilmelidir.

Öte yandan, özel nitelikli kişisel verilerin işlenmesine ilişkin şartları belirleyen Kanun'un 6 (2)'inci maddesi uyarınca; aynı maddenin 3'üncü fıkrasında belirtilen haller istisna olmak üzere, özel nitelikli kişisel verilerin veri sahibi ilgili kişinin açık rızası olmaksızın işlenmesinin yasak olduğu açıkça "işleme yasağı" olarak belirtilmiştir (Türkmen, 2019, sf. 126-128). Yukarıda da değinildiği gibi due diligence raporunun hazırlığı kapsamında hedef şirketin dava dosyasına yönelik inceleme yapılırken hedef şirket çalışanlarına ait gerek duyulması halinde (örneğin; dava raporundaki bir iş kazası davasının aleyhe sonuçlanması halinde doğacak ödeme yükümlülüğün yüksek olması riski) sağlık verileri, iş göremezlik raporu, iş kazasına ilişkin dökümanlar gibi belgeler vasıtasıyla veri odalarında toplanarak işlenecek ve taraf vekilleri ile due diligence sürecini yöneten uzmanların erişimine açılacaktır. Bu noktada, Kanun'un açık ifadesi paralelinde; özel nitelikli kişisel verisi işlenen çalışanların açık rızasının alınması mecburidir. Öte yandan, birleşme devralma işlemlerinde özel nitelikli kişisel verisi işlenen her bir işçinin açık rızasının alınması, taraflar için pratik anlamda zorluk doğuruyorsa, işlem özelinde taraflar için mümkün olması halinde özel nitelikli kişisel veri içeren bu belgelerin, veri sahibi ilgili kişinin kimliğini belirlemeyi imkânsız kılacak biçimde anonimleştirilmesi tavsiye edilebilir.

Birleşme ve Devralmaya Hazırlık Aşaması

Birleşme ve devralma sürecinde, nihai sözleşme aşamasına gelmeden önce genellikle üç aşama mevcut olduğu görülmektedir. Bu aşamalar; (i) niyet mektubu ve benzeri yapıların imzalanması, (ii) gizlilik sözleşmesinin imzalanması ve (iii) due diligence sürecinin takip edilmesi şeklinde görülebilmektedir. Niyet mektubu, tarafların hedeflenen hukuki ilişkinin ana hatlarını belirlemek ve hedeflenen hukuki ilişkinin gerçekleşmesi için gerekli müzakerelerin yürütülmesine ve bazı durumlarda bu hukuki ilişkinin gerçekleştirilmesine ve içeriğine dair niyetlerini içeren kural olarak bağlayıcı olmayan, ancak bazı hallerde bağlayıcı hükümlerin eklenebildiği, tarafları manevi bir yükümlülük altına sokan yazılı irade açıklamasıdır (Oral, 2016, sf. 147). Her ne kadar niyet mektubunun bağlayıcılığı tartışmalı olsa da paylaşılacak bilgi ve belgelerin kapsamı başta olmak üzere, zamanlama, varsa kamuya açıklanacak bilgilerin, müzakerelerin kesinlik derecesinin, alıcı ve satıcının bağlayıcı taahhütlerde bulunmadan önce işleme devam etmesinin maliyetinin, nihai anlaşmanın imzalanacağı tahmini tarihin, hedef şirkete biçilecek değerin hangi fiyat aralıklarında olacağının, alıcının istediği münhasırlık derecesinin, tarafların birbirine karşı iyi niyet hükümlerinin bu aşamada netleşmesi tarafların kuracağı olası ticari ilişkiyi daha kuvvetli kılacaktır (Çek, 2021,Birleşme-Devralma İşlemleri Çerçevesinde "Due Diligence ve Engagement Letter", sf. 31).

Birleşme ve devralma süreçlerinde gizlilik sözleşmeleri oldukça yaygın kullanılmaktadır. Birleşme ve devralma süreçleri, genellikle bilgi ve belgelerin paylaşılmaya başlandığı andan kapanış aşamasına kadar gizli olarak yapılmaktadır. Gizlilik sözleşmesi, tarafların müzakere sürecinde birileriyle paylaştıkları ve saklı kalması gereken gizli bilgilerinin nasıl muhafaza edileceği, bu yükümlülüğe aykırılık halinde tarafları nasıl bir süreç beklediğine ilişkin düzenlemelerin yer aldığı bir anlaşmadır. Birleşme devralma sürecinin ilk hukuken bağlayıcı dokümanı olan gizlilik sözleşmesi; potansiyel alıcılar ve hedef şirket arasındaki bilgi paylaşımının gizli tutulmasını ve hatta işlemin kendisinin de gizli tutulmasını amaçlar. Detaylı izah ettiğimiz üzere hedef şirketin tüm malvarlığı bilgileri, risk değerlendirmeleri, finansal verileri ve gerektiğinde piyasadaki rekabet nezdinde önem arz eden

pazarlama ve ticari stratejileri, fiyatlandırma bilgileri gibi ticari sırları da paylaşıyor olacağından, due diligence hazırlığına başlanılmadan önce şirket bilgilerinin verileceği taraf bu bilgileri ifşa etmeyeceğine dair bir gizlilik sözleşmesi imzalamalıdır. Paylaşılan bilgi ve belgelerden hangilerinin tam olarak gizli bilgi sayılacağının taraflarca gizlilik sözleşmesi ile detaylı olarak belirlenmesi uygulama ve hedef şirketi korumak açısından daha elverişli olmaktadır. Bilgilerin paylaşılması halinde hedef şirketin uğrayacağı maddi ve manevi zarar göz önünde bulundurularak bir cezai şart maddesinin belirlenmesi ise hedef şirketin korunmasını sağlayacaktır. Her ne kadar hedef şirket ve alıcı şirket arasındaki bilgi alışverişi ve birleşme devralma sürecinin bizzat kendisi, akdedilen gizlilik sözleşmesi ile gizli tutulsa da, gizlilik sözleşmesi imzalandıktan sonra geçilecek due diligence etabında paylaşılan ve işlenen kişisel verilerin akıbetinin göz ardı edilmemesi gerekmektedir. Nitekim bu noktada, taraflar arasında akdedilen gizlilik sözleşmesine due diligence incelemesi boyunca işleme konu edilecek kişisel verilerin korunmasına ilişkin bir hükmün eklenmesi tavsiye edilir. Zira, taraflar arasında gizlilik sözleşmesi imzalanmasının diğer bir sonucu da, süreç boyunca kişisel verileri işlenebilecek ilgili kişilerin, bu işleme faaliyetlerinden habersiz olacağıdır. Örneğin; hedef şirketin çalışanlarının, tedarikçilerinin, müşterilerinin veya şirketle herhangi bir organik bağı bulunmayan gerçek kişilerin, birleşme devralma sürecinden hiçbir suretle haberi olmaması sonucunu doğurmaktadır. Bu durum, veri sorumlusunun başta aydınlatma yükümlülüğü ve kişisel verilerin işlenmesi için açık rıza gereken haller olmak üzere; Kanun ve ilgili ikincil mevzuat uyarınca yükümlülüklerini yerine getirmemesine sebebiyet verebilmektedir. Buna ilave olarak, alıcı ve hedef şirket, yürütecekleri birleşme devralma müzakerelerinin olumsuz sonuçlanma ihtimalini göz önünde bulundurmalı ve bu doğrultuda due diligence süreci kapsamında alıcının elde ettiği kişisel verilerin mevzuata uygun bir biçimde imha edileceğine ilişkin bir sözleşme imzalamalıdır. Nitekim due diligence sürecinden sonra anlaşmaya varılamaması halinde; alıcının kişisel verileri işlemek için dayanacağı bir hukuki sebep bulunmayacaktır.

Avrupa, Orta Doğu ve Afrika genelinde 500'den fazla birleşme ve devralma uygulayıcısı arasında yapılan bir anket, katılımcıların %55'inin hedef şirketin veri korumasına uygunluğu konusundaki endişeler nedeniyle ilerlemeyen ve sonuçlanmayan birleşme ve devralma süreçlerinde çalıştığını belirtmiştir. Bu pay Almanya'da (%70'den fazla), İskandinav ülkelerinde (%65'ten fazla) ve Birleşik Krallık'ta (%60'tan fazla) önemli ölçüde yüksektir. Durum tespiti sürecindeki yaygın bir zorluk, tarafların Kanun'a uyumlu şekilde ilerlememelerine rağmen uyumlu olduklarını düşünmeleri ve Kanun'a uygunluğu göz ardı etmeleridir. Günümüzde birçok şirket, Kanun'a uyum ile ilgili endişeler nedeniyle bir anlaşmayı iptal etmek yerine, hedef şirketin veri güvenliği standartlarına yatırım yapmaya karar vermekte ve devir sürecini durdurmamaktadır.

Due Diligence Sürecinde Kişisel Verilerin İşlenmesine İlişkin İlgili Kişiyi Aydınlatma Yükümlülüğüne İlişkin Esaslar:

Birleşme devralma sürecinin due diligence etabında, gerek hedef şirketin kendisi tarafından gerek alıcı tarafların talebi doğrultusunda aktarıma ve işlemeye konu olan kişisel verilere ilişkin, tarafların haiz olduğu veri sorumlusu sıfatının sonucu olarak ilgili kişileri; Kanun'un 10'uncu maddesi ve 10 Mart 2018 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Tebliğde ("Tebliğ") belirtilen usul ve esaslara uygun olarak aydınlatma yükümlülüğü bulunmaktadır. Veri sorumlularının üzerinde bulunan aydınlatma yükümlülüğü, ilgili kişilere veri sorumlusunca gerçekleştirilen veri işleme faaliyetinin hukuka uygun yapılıp yapılmadığını gözetleme ve denetleme imkanı tanımaktadır. (Çekin, 2019, s.119)

Kanun'un 10'uncu maddesi, aydınlatma yükümlülüğü kapsamında ilgili kişilere sağlanması gereken bilgileri genel olarak beş madde halinde saymış; Tebliğ uyarınca ise veri sorumlularının aydınlatma yükümlülüğünü yerine getirirken uyması gereken esas ve usuller detaylı biçimde kaleme alınmıştır. Aydınlatma yükümlülüğü, işleme faaliyetine konu olan kişisel veri için açık rıza alınmış olsun veya

olmasın her halükârda yerine getirilmesi gerekmekte olup, aydınlatma yükümlülüğünün yerine getirilmesi için herhangi bir şekil şartı öngörülmemiştir. Nitekim, Tebliğ'in 5 (1)'inci maddesi uyarınca aydınlatma yükümlülüğü, sözlü, yazılı ve elektronik ortamlar vasıtasıyla yerine getirilebilir. Lakin; aydınlatma yükümlülüğünün yerine getirildiğinin ispat yükü, veri sorumlusu üzerinde olacak olup bu nedenle yükümlülüğün yazılı bir metne bağlanarak yerine getirilmesi tavsiye edilir (Aydınlatma Yükümlülüğünü Yerine Getirilmesi Rehberi, 2019, sf. 8). Dikkat edilmesi gereken diğer bir temel husus; aydınlatma yükümlülüğünün, Tebliğ'in 5 (1)-f) maddesi uyarınca kişisel verilerin işlenmesi için açık rıza gerektiği hallerde, açık rıza süreçlerinden ayrı olarak kurgulanması gerektiğidir.

Aydınlatma yükümlülüğünün, içerik anlamında Kanun'un 10'uncu maddesinde belirtilen unsurları karşılaması gerektiği gibi, pratik anlamda da; ilgili kişinin etkili bir biçimde aydınlatılmasını sağlamak amacıyla Tebliğ'in 5'incu maddesinde belirtilen koşulları da karşılaması gerekmektedir. Buna göre; Tebliğ'in 5'inci maddesinin g) ve ğ) bentleri uyarınca; aydınlatma yükümlülüğü kapsamında belirtilecek kişisel veri işleme amaçlarının (i) belirli, açık ve meşru olması; (ii) genel nitelikte muğlak ifadelere yer verilmemesi, (iii) ilgili kişinin açık ve sade, anlaşılabilir bir dille bilgilendirmesi gerektiği ifade edilmiştir. Somutlaştırmak gerekirse, ilgili kişinin bilgisine sunulan aydınlatma metninin; ağdalı bir hukuki metin biçiminde olmaması, ilgili kişinin anlayabileceği şekilde öz ve sade bir dil kullanılarak açıklanması gerekmektedir. Bu noktada önem arz eden nokta, öz ve sade bir dil kullanılırken yüzeysel ve yetersiz bir dil kullanılmaması; hatta veri işleme faaliyetinin hukuki sebepleriyle ilgili kişinin temel hak ve özgürlükleri noktasında doğabilecek hususların ilgili kişiye açıkça sunulması gerekmektedir (Lynskey, 2015, sf. 248). Bunun yanı sıra, Kişisel Verileri Koruma Kurulu ("Kurul"); 02/05/2019 tarihli ve 2019/122 sayılı kararı ile veri sorumlusu tarafından hazırlanmış aydınlatma metninde dayanılan hukuki sebeplerin açıkça belirtilmediği ve kişisel veri işleme amaçlarının "gibi amaçlar çerçevesinde" biçimindeki genel bir ifade ile belirtilmesi sebebiyle kişisel veri işleme sebepleri ve amaçlarının aydınlatma metninde muğlak bir ifadeyle kullanıldığı yönünde karar vermiş, hazırlanan aydınlatma metninin Tebliğ'deki usul ve esaslara uygun olmadığına kanaat getirmiştir. (Kişisel Verileri Koruma Kurulu'nun 02/05/2019 tarihli ve 2019/122 sayılı Kararı). Bu noktadan hareketle, due diligence sürecindeki veri işleme faaliyetlerinin hangi hukuki sebebe dayanarak ve hangi amaçlar doğrultusunda aktarıldığının ve işlendiğinin aydınlatma metinlerinde açıkça belirtilmesi gerekmektedir. Örneğin; ilgili kişiye yöneltilen aydınlatma metninde kişisel verilerin, "İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması" hukuki sebebine dayalı olarak, "Birleşme Devralma Sürecinde Hedef Şirketin Detaylı İncelenerek Şirketin Devralınmasına İlişkin Risklerin Tespiti ve Değerlendirilmesi" amacıyla işlendiği şeklindeki açık ve somut ifadelerin kullanılması tavsiye edilmektedir.

Due diligence süreçlerinde hedef şirket ve alıcı(lar) arasında gerçekleştirilen veri akışı ve veri işleme faaliyetleri dolayısıyla doğan aydınlatma yükümlülüğü noktasında değinilmesi gereken bir husus ise, Tebliğ'in "Kişisel Verilerin İlgili Kişiden Elde Edilmemesi Halinde Aydınlatma Yükümlülüğü" başlıklı 6'ıncı maddesinde düzenlenmiş olan esaslardır. Nitekim due diligence sürecinde veri odasında muhafaza edilen kişisel veri içeren dökümanlar; söz konusu kişisel verilerin sahibi ilgili kişiler tarafından değil; (örneğin; ilgili kişinin hedef şirket çalışanı olması durumu) bizzat hedef şirket tarafından alıcı şirket(ler)e aktarılmaktadır. Tebliğ'in 6'ıncı maddesi, kişisel veriyi doğrudan ilgili kişiden elde etmeyen taraf için de aydınlatma yükümlülüğünü muğlak ifadelerle tarif ederek; (i) kişisel verileri elde eden tarafın; ilgili kişiye makul bir süre içinde aydınlatma yapmak zorunda olduğunu, (ii) ilgili kişi ile iletişim kurulması halinde ilk iletişim kurulduğu anda aydınlatma yapılması gerektiğini belirtmiştir.

Veri sorumluları için Kanun ve Tebliğ uyarınca öngörülen sistematiğin; pratikte uygulamada doğurabileceği zorluklar göz önünde bulundurularak; birleşme devralma tarafları olan alıcı ve hedef şirketin kişisel veri içeren dokümanları mümkün olduğunca anonimleştirerek sürece devam etmesi

tavsiye edilmektedir. Örneğin, hedef şirketin alt işveren-asıl işverenlik ilişkisinden doğabilecek mali risklerini tespit etmek için üçüncü kişilerin kim veya hangi tüzel kişi olduğu bilgisi alıcı şirket için değerlendirilmesi zorunlu bir bilgi değildir. Bu sözleşmeler paylaşılırken tarafların anonimleştirilerek paylaşılmasının bir kural haline getirilmesi süreci daha güvenilir kılacaktır.

Due Diligence Sürecinde İşlenen Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Alınacak Açık Rızaya İlişkin Esaslar

Özel nitelikli kişisel verisi işlenmekte olan ilgili kişinin açık rızasına müracaat edilmesi halinde, kişisel verisi işlenen ilgili kişiden alınacak açık rızanın; özel nitelikli kişisel verilerin işlenebilmesi için bir hukuka uygunluk sebebi olabilmesi için; Kanun'un Tanımlar başlıklı 3(1)- a) maddesinde belirtilen üç unsuru birlikte karşılıyor olması gerekmektedir. Madde metni uyarınca açık rıza, "belirli bir konuya ilişkin bilgilendirmeye dayanan ve özgür iradeye dayanan rızayı" ifade etmektedir.

Kanun'un anılan maddesinde belirtilen tanımdaki unsurlardan hareketle; (i) açık rızanın spesifik olarak birleşme devralma işlemi için alındığının ilgili kişiye belirtilmesi, (ii) açık rıza metninde hangi özel nitelikli kişisel verilerinin işleneceğininin kategori halinde işleme amacıyla birlikte ilgili kişiye belirtilmesi, (iii) açık rıza beyanını vermekle doğacak hukuki sonuçların ilgili kişiye belirtilmesi, (iv) ilgili kişinin vermiş olduğu açık rızayı kendi iradesine bağlı olarak istediği zaman geri çekebileceğinin belirtilmesi, ve son olarak; (v) ilgili kişinin söz konusu açık rızayı özgür iradesi ile vermiş olması gerekmektedir (Türkmen, 2019, sf. 118-121). Kanun'un 3'üncü maddesinde açık rızanın tanımıyla sağlanan unsurlar incelendiğinde, esasında tüm bu unsurların birbirini tamamladığı söylenebilir. Nitekim, veri sahibi ilgili kişinin spesifik olarak hangi kategorideki kişisel verilerinin işlendiğine, kişisel verilerinin hangi süreç ve işlemler için, hangi amaçlar doğrultusunda işlendiğine dair bilgilendirilmediği bir durumda vermiş olduğu rızanın, özgür iradeyle verildiğinden bahsedilemez.

Geçerli ve hukuka uygun bir açık rızadan bahsedebilmek için yukarıda sayılan hallerden birleşme devralma süreçlerinin due diligence etabı için pratik anlamda problem doğurabilecek koşul; ilgili kişinin, veri işleme faaliyeti başlamadan önce vermiş olduğu açık rızasını geri alma ihtimalidir. Nitekim, ilgili kişi, özel nitelikli kişisel verilerinin işlenmesine yönelik vermiş olduğu açık rızayı her zaman geri alabilir. Fakat bu gibi bir durumda, ilgili kişinin geri aldığı rıza ileriye dönük olarak sonuç doğuracaktır. Diğer bir ifadeyle rızanın geri çekilmesi, ilgili kişinin rızasını geri almadan önce tarafların due diligence sürecinde topladıkları ve işledikleri verilerden elde ettikleri sonuçlardan ve bilgilerden faydalanmalarını engellemeyecektir. Tarafların bu noktada yapması gereken, söz konusu veri işleme faaliyetini durdurmak ile sınırlıdır (Avcı Braun, 2018, sf. 17).

Çoğunlukla gizlilik sözleşmeleri altında yürütülen due diligence çalışmasında kişisel verisi işlenen ilgili kişilerin açık rızalarının alması, taraflar için pratik anlamda zorluk doğuracağından, sürecin bu noktasındaki en ideal çözümün kişisel veri içeren dokümanların anonimleştirilmesi olduğu söylenebilir.

Due Diligence Sürecinde İşlenen Kişisel Verilerin Veri İşleme Amacı İçin Gerekli Olan Miktarı Aşmaması

Kanun'un 4 (2)'inci maddesi, kişisel veri işleme faaliyetlerinde uyulması gereken beş temel ilkeyi belirtmektedir. Bu ilkeler arasından 2. fıkranın ç) bendinde belirtilen kişisel verilerin; "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü" olarak işlenmesini öngören ilke, birleşme devralma süreçlerinin due diligence etabı için ele alınması gereken önemli bir nokta olarak karşımıza çıkmaktadır. Söz konusu ilke kapsamında, veri işlemenin "ölçülü" olma noktası, veri sorumlusunun, faaliyetlerini gerçekleştirmesi için gerekli olan miktardan fazla kişisel veri işlememesini öngörmektedir. Ölçülülük ilkesi, Direktif ve GDPR kapsamında da benzer şekilde düzenlenmiş olup, AB veri koruma hukuku kapsamında bazı

yazarlar ölçülülük ilkesinin öngördüğü bu durumu, "veri minimizasyonu" olarak da ifade etmektedir (Carey, 2018, sf. 35). Bu ilke doğrultusunda, hedef şirket ve alıcı şirketlerin due diligence sürecinde sadece işlemin kapanışından önce değerlendirmeye alınması gerekli olan kişisel verileri işlediklerinden emin olmaları, birleşme devralma işleminin gerçekleştirilmesi için gerekli olmayan fazladan verileri işlememeleri, aktarıma konu etmemeleri gerekmektedir.

Hedef Şirket İçin Yapılan Risk Değerlendirilmesi ve Veri İşlemede Ölçülülük

Bir tarafta; alıcı ve hedef şirket, birleşme devralma sürecinin due diligence aşamasını Kanun kapsamında öngörülmüş ölçülülük ilkesinin paralelinde gerçekleştirmek zorunda iken; diğer tarafta due diligence sürecini mümkün olduğunca kapsamlı ve detaylı tutmak istemektedir. Nitekim süreç boyunca elde edilen ve kişisel veri içeren bilgi setleri, birleşme devralmaya ilişkin risklerin tespiti ve değerlendirilmesini, tarafların aralarında kuracakları hukuki ilişkiye yönelik etkili kararları alabilmesini, fiyatın belirlenmesini, ve hatta kapanış sonrası, satıma konu ticari işletmenin organizasyonel yapısı ile entegrasyonunu kolaylaştıracaktır (Pulaşlı, 2007, sf 211).

Somutlaştırmak gerekirse; birleşme devralma süreçlerinde alıcı adayları hedef şirketin (i) finansal durumunu; performansını, şirketin gelir tablosunu, ara dönem ve yıl sonu bilançoları ve planlama hesaplarını, güncel ve geçmiş kazanç ve malvarlığını, uğradığı zararların incelenmesini, (ii) vergisel durumunu; devir veya birleşme öncesi vergi planlaması ve vergisel risklerin değerlendirilmesini, (iii) hukuki işlemlerin ilgili mevzuata uygunluğu; şirket faaliyetlerin hukuksal açıdan kusurun mevcudiyetinin araştırılrak alıcı şirketin beyan edilmemiş hukuki yükümlülüklerin araştırılmasını, kaybedilen veya kaybedilebilecek davalar ile şirketin borçlu sıfatını haiz olduğu icra dosyalarının incelenmesini ve olası zararın hesaplanmasını ve bunlar gibi; içlerinde üçüncü kişilere ait kişisel veri barındıran pek çok dokümanın incelenmesini talep edebilecektir. Bu minvalde, veri paylaşımını hedef şirket açısından önemli kılan bir diğer sebep de; devir konusu hedef şirketin alıcı adayı şirket(ler)e verileri muayene imkanı sağlamış olmasının, ve potansiyel alıcıların paylaşılan verileri incelemiş olmasının, 6098 sayılı Türk Borçlar Kanun'un 222. Maddesi paralelinde satıcının ayıba karşı tekeffül sorumluluğunu zayıflatacağıdır.

Dolayısıyla, taraflar due diligence süreci boyunca planlanan birleşme devralma işlemini gerçekleştirmek ve ticari ihtiyaçlarını karşılamak için gerekli dökümanları talep etmeli; ancak öte yandan da işledikleri kişisel verileri ölçülülük ilkesi paralelinde işlemin kapanışı için gerekli olan, asgari bir seviyede tutmalıdırlar. Bu dengenin kurulabilmesi için due diligence etabının somut işlem özelinde ve kişisel veri içeren belge ve bilgilerden sadece işlem amacı için gerekli olanlar ile sınırlı tutulması gerekmektedir. Somut işlemin özellikleri değerlendirilerek talep edilecek kişisel veri içeren belgelerin belirlenmesi aşamasında, kapsamına göre farklılık gösteren iki due diligence tipi; (i) tam due diligence ve (ii) sınırlı due diligence arasından seçim yapılabilir; veya bu çalışmaların kapsamları işlemin niteliğine göre uyarlanabilir. Nitekim; tam due diligence incelemesinde hedef şirketin tüm alanları her açıdan ve oldukça kapsamlı şekilde incelenmektedir. Hedef şirketin mevzuata uygun şekilde kurulup kurulmadığı, ortaklık yapısı, genel kurul ve yönetim kurulu kararları, ilgili makamlara gerekli tüm bildirimlerin yapılıp yapılmadığı, hedef şirketin taraf olduğu sözleşmeler (satış, banka, gizlilik, franchising vb.), fikri ve sınai haklar, taşınır ve taşınmazlar, hedef şirket teknolojik yapısı ve çevresel tehlike ve etkiler dahi incelenmektedir (Çil, 2020, sf. 25). Bu inceleme alanları sınırlı sayıda belirtilmemiş olup tarafların anlaşmaları çerçevesinde genişletilip daraltılabilir niteliktedir. Öte yandan sınırlı türdeki due diligence raporunda tarafların kararlaştırdığı ve sadece incelenmesi zaruri belgelerle yapılan analiz söz konusudur. Öte yandan, kişisel veri içeren dokümanların anonimleştirilmesi bir çözüm olarak ileri sürülebilir. Due diligence süreci kapsamında aktarımı ve işlenmesi gerekli olan kişisel veri barındıran belgeler aksine paylaşılan belgelerin içerdikleri kişisel verilerin birleşme devralma işlemi için gerek olmadığı durumlarda; bir gerçek kişiyle ilişkilendirilemeyecek biçimde anonimleştirilmesi, due diligence sürecini

taraflar için kolaylaştırabilecektir. Örneğin; bir çalışanın özlük dosyasının tamamının paylaşılması bu süreçte zorunlu sayılmaz. Ancak hedef şirketin kıdem tazminatı yükü, ihbar tazminatı yükü ve yıllık ücretli izin yükünün doğru tespiti için çalışanın ücret bilgisinin paylaşılması zorunludur. Ancak bu yöntemin denenmesi halinde, uygulamada söz konusu belgenin veri sahibi ilgili kişiyi gerçekten işaret etmediğinden emin olunmalıdır. Örneğin sadece isim kısmı belirsiz hale getirilmiş bir belgede ilgili kişiyi işaret etmek için yeterli olacak diğer bilgilerin bulunmaması gerekmektedir.

Veri Güvenliğine İlişkin Yükümlülükler Doğrultusunda Veri Odası

Makale kapsamında da değinildiği üzere due diligence incelemesi sürecinde; alıcı adayı şirketler tarafından hedef şirkete yöneltilen bilgi-belge talep listesine dayalı olarak hedef şirketçe iletilen bilgiler, fiziki veya elektronik ortamda organize edilen veri odalarında toplanmaktadır. Belirtmekte fayda vardır ki günümüz pratiğinde veri odaları çoğunlukla elektronik ortamlarda organize edilmekte olup due diligence süreçleri için fiziksel veri odalarının kurulumu yaklaşık dörtte bir seviyelerine inmiştir (Esin, 2021, sf.131). Birçok kişisel veri içeren belgenin toplandığı veri odalarında Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12 (1)'inci Maddesi belirtilen; (i) kişisel verilerin hukuka aykırı olarak işlenmesini önlemeyi, (ii) kişisel verilerin hukuka aykırı olarak erişilmesini önlemeyi ve (iii) kişisel verilerin muhafazasının sağlamayı garanti edecek yeterli teknik ve idari tedbirlerin alınması gerekmektedir. 12'nci madde metni, bu tedbirleri almakla yükümlü olan muhatabın bizzat veri sorumlusu olduğunu ifade ettiğinden; birleşme devralma due diligence etabında, veri sorumlusu olarak hareket eden hedef şirket ve alıcı(lar) tarafların; ilgili idari ve teknik tedbirleri almakla sorumluluğu mevcuttur.

Kanun'un öngördüğü sistematik uyarınca veri sorumluları veri güvenliğinin sağlanması için alınması gerekli ve yeterli idari ve teknik tedbirlerin tespitini, kendi operasyonları, veri işleme faaliyetleri, işledikleri kişisel verilerin kategorisi ve miktarına göre kendileri tayin edecektir. Bu noktada veri sorumluları; objektif olarak kendilerinden veri güvenliğini sağlamak için beklenebilecek gerekli tedbirleri almış olmalıdırlar. (Dülger, 2020, sf. 539) Önemle belirtmekte fayda vardır ki; özel nitelikli kişisel verilerin işlenmesi halinde, veri sorumlularınca alınması gereken idari ve teknik önlemler, Kurul'un 31.08.2018 tarih, 2018/10 sayılı Kararı doğrultusunda daha kapsamlı olacaktır. Bu hususun, veri odasında özel nitelikli kişisel veri içeren dokümanların muhafaza edilmesi halinde göz önünde bulundurulması gerekmektedir.

Öte yandan; uygulamada, due diligence sürecinde kullanılan veri odalarının üçüncü kişilerden hizmet alınarak oluşturulduğu görülebilmektedir. Due diligence kapsamındaki kişisel veri içeren dokümanların üçüncü kişi hizmet sağlayıcı tarafından oluşturulan bir veri odasında muhafaza edilmesi durumunda; bu üçüncü kişinin Kanun'un 3 (1)-ğ) maddesinde belirtilen "veri işleyen" tanımı içine girdiği söylenebilir. Zira veri işleyen; veri sorumlusunun sağladığı yetkiye dayanarak veri sorumlusunun onun adına kişisel verileri işlemekte olan fakat veri sorumlusunun organizasyonu dışında yer alan gerçek ve tüzel kişiler olarak somutlaştırılmıştır (Kişisel Verilerin Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, sf. 2). Bu noktada önemle belirtmek gerekir ki; birleşme devralma işleminin tarafı olarak veri sorumlusu sıfatını haiz olan taraflar, verilerin muhafaza edildiği veri odasında gerekli teknik ve idari tedbirleri almak noktasında müştereken sorumlu olacaktırlar (Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti). Bu bağlamda kişisel verilerin korunması hukukumuzdaki uygulama; veri sorumlusu ve veri işleyeni gerekli tüm tedbirleri almak noktasında müteselsilen sorumlu tutan GDPR uygulamasından farklılaşmaktadır.

Gerekli ve yeterli teknik ve idari tedbirlerin alınması noktasında veri sorumlusu ve veri işleyenin müştereken sorumluluğu noktasından hareketle, due diligence sürecinde birleşme devralma taraflarının üçüncü kişiler tarafından organize edilen veri odalarını kullanıyor olmaları halinde dikkat etmesi

gereken bazı hususlara değinmekte fayda vardır. Nitekim; veri odasında gerektiği ölçüde alınmamış olan teknik ve idari tedbirler sebebiyle hukuka aykırı veri işleme faaliyetinin gündeme gelmesi ihtimalini de düşünerek, veri işleyenle veri sorumlusu arasında bir "veri işleme sözleşmesi" imzalanması tavsiye edilir. Bu sözleşme kapsamında veri odası hizmetini sağlayan üçüncü taraftan veri güvenliğine ilişkin gerekli ve yeterli tedbirleri alacağına ilişkin taahhüt alınabilecektir. Nitekim veri işleme sözleşmesinin düzenlenmesi, veri güvenliğinin sağlanması açısından Kanun'un 12 (2)'inci Maddesinde öngörülen müşterek sorumluluk yönünden de son derece önemlidir. Bu gibi bir veri işleme sözleşmesi kapsamında, veri işleyen, kişisel veri güvenliğini sağlamak amacıyla hangi teknik ve idari tedbirleri belirtilebilir veya veri güvenliği sebebiyle meydana gelen bir kişisel veri ihlali halinde veri işleyen, veri sorumlusuna yardım etme yükümlülüğü altına sokulabilir. (Taştan, 2018, Bir Modern Sözleşme Tipi Olarak Kişisel Veri İşleme Sözleşmesi ve Kanun'a Uyum Sürecindeki Rolü, sf. 2-3).

Veri işleme sözleşmesi imzalanmasına ek olarak, due diligence süreci kapsamında pratik olarak dikkat edilmesi gereken bir başka husus da, veri odasına erişim yetkisine sahip olan kişilerin belirlenme noktasıdır. Zira; olası bir veri ihlali ihtimalinin azaltılması için; due diligence süreci boyunca veri odasında bulunan ve kişisel veri içeren dokümanlara kimlerin erişebileceği dikkatlice tespit edilmeli, erişim yetkisi olabilecek kişiler mümkün olduğunca az sayıda olacak biçimde belirlenmelidir. Kişisel veri içeren dokümanların sadece belirli kişilerin erişimine açık olmasının kararlaştırılması da tavsiye edilebilir. Buna ilişkin olarak da; başta veri odasına erişim yetkisi sahibi olan kişilerin ve veri odası kullanımına ilişkin esas ve usullerin belirtildiği bir "veri odası kullanım şartları" düzenlenmeli ve taraflarca imzalanmalıdır (Höhn, 2003 sf. 60). İlaveten; kişisel veriler dolayısıyla gündeme gelebilecek herhangi bir ihlalin önüne geçilebilmesi için, veri odasında tarafların incelemesine açılmış olan kişisel veri içeren dokümanların, fotokopilerinin çekilmemesi, herhangi bir yolla görüntü ve örneklerinin alınmaması da tavsiye edilir. (Kutlan, sf. 38). Buna ek olarak ise, veri odasına yalnızca sınırlı bir grup kişinin erişmesine izin verilmelidir. Bu kişilerin kim olduğu taraflarca önceden onaylanmalıdır. Bu kişiler, müzakerelerin olası bir başarısızlığı durumunda, alınan bilgileri daha fazla kullanmamayı ve imha etmeyi sözleşmeyle kabul etmelidir.

Elektronik Ortamdaki Veri Odaları ve Kişisel Verilerin Yurt Dışına Aktarımı

Due diligence uygulamalarında veri odalarının kullanımına ilişkin yukarıdaki bölümde yapılan incelemelerin ışığında, elektronik ortamda organize edilen veri odalarına ilişkin Kanun'un kişisel verilerin yurt dışına aktarıma ilişkin öngördüğü esaslara değinmek gerekir. Kanun'un oluşturduğu sistematik incelendiğinde, kişisel verilerin yurt dışına aktarımı konusunun hassas bir biçimde ele alındığı ve kişisel verilerin işlendikleri ülke dışında erişilebilir hale gelmesini kısıtlayıcı önlemlerin mevcut olduğu görülmektedir (Kuner ve Manelli, 2017, sf. 4). Bunun arkasında yatan sebebin, Kanun'un GDPR'ın aksine, sınırlar ötesi bir uygulama alanı bulunmaması ve başka ülke kanunlarına tabi bir kuruluşa kişisel verilerin aktarılması halinde bu verilerin Kanun'un koruma alanından çıkması olduğu söylenebilir (Çekin, 2019, s.84).

Kanun'un 9. maddesi, kişisel verilerin yurt dışına aktarımına ilişkin usul ve esasları düzenlemektedir. Madde metni uyarınca kural olarak ilgili kişinin açık rızası olmaksızın yurtdışına aktarıma konu edilememektedir. Öte yandan, esasen aktarım işlemi de bu makalede de belirtildiği üzere "veri işleme" hallerinden birisi olduğundan ötürü, ilgili kişiden açık rıza alınmış olan bir yurt dışı aktarımının da, Kanun'un 4'üncü maddesinde sayılmış olan veri koruma hukuku temel ilkeleri paralelinde gerçekleştirilmesi gerekmektedir. Fakat, yurt dışı aktarıma konu olan kişisel veri, özel nitelikli olmayan kişisel veri ise Kanun'un 5'inci Maddesinde, özel nitelikli kişisel veri ise Kanun'un 6'ıncı Maddesinde sayılmış işleme şartlarından birini karşılıyor olması durumunda, Kanun'da belirtilen ek koşullara da uyulması şartıyla, ilgili kişinin açık rızasına müracaat edilmeksizin yurt dışına aktarılabilecektir. Bu ek şartlardan birisi, Kanun'un 9(2)'inci maddesinde belirtildiği üzere, aktarım yapılan ülkede yeterli

korumanın bulunduğunun garanti edilmesidir. Makalenin hazırlandığı tarihte, henüz Kurul tarafından yeterli korumanın bulunduğu ülkelerin listesi yayımlanmamış olmakla birlikte, Kurul yeterli korumanın bulunduğu ülkelerin tespitinde kullanacağı unsurları, 02/05/2019 tarihli ve 2019/125 sayılı kararı ile belirtmiştir. Kanun'un 9'uncu maddesi, yurt dışına veri aktarımı yapılan ülkenin yeterli korumanın bulunduğu ülke kriterlerini karşılamadığı durumlarda; Türkiye'de bulunan veri sorumlusu ve aktarımın yapıldığı yabancı ülkedeki kuruluş arasında aktarılan kişisel verilerin korunmasına ilişkin taahhütname imzalanmasını ve aktarımın gerçekleştirilmesi için imzalanan taahhütname ile Kurul'dan izin alınması gerektiğini düzenlemektedir.

Due diligence pratiğindeki veri odaları kullanımlarında kişisel verilerin yurt dışına aktarım konusunun incelenmesi için öncelikle hangi hallerde yurt dışına veri aktarımı yapıldığının tespiti gerekmektedir. Kişisel verilerin yurt dışına aktarımını gündeme getirebilecek hallerden ilki; birleşme devralmanın alıcı taraflarının yabancı ülkelerde kurulu ticari işletmeler olması durumudur. Uygulamada, gelişmekte olan ülkelerde kurulu ve karlılık potansiyeli yüksek olan şirketlerin uluslararası sermayenin dikkatini çektiği gözlemlenmekte ve dolayısıyla da Türkiye'de yabancılık unsuru içeren bu gibi birleşme devralma işlemlerinin sıkça yapıldığı görülmektedir (Ener, 2020, sf.37-39). Öte yandan, Kurul'un 31.05.2019 tarih ve 2019/157 sayılı ilke kararı kapsamında serverları yurt dışında bulunan veri işleyen ve veri sorumlularının veri işleme faaliyetlerinin de yurt dışına aktarım sayılacağının önemle vurgulanması gerekir. Bu gibi bir yurt dışına veri aktarımı, hedef şirketin ve alıcı(lar)ın Türkiye'de kurulu oldukları, fakat due diligence işlemleri için kullandıkları sanal veri odasının serverlarının yurt dışında bulunduğu bir ihtimalde gerçekleşebilecektir. Görüldüğü üzere birleşme devralma süreçlerinin due diligence etabındaki yurt dışına veri aktarımı, gerek taraflardan birinin yurtdışında kurulu olması, gerek kullanılan veri odasının serverlarının yurt dışında bulunması hallerinde gündeme gelebilecektir.

Bu durumlarda, bu bölümde yapılan açıklamalar özel nitelikli olmayan kişisel veriler, ilgili kişinin açık rızası aranmaksızın, "İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması" hukuki sebebine dayalı olarak yabancı ülkeye aktarılacaktır. Öte yandan, özel nitelikli kişisel verilerin yurt dışına aktarımı için, açık rıza şartı aranmaksızın aktarılabilmesi için Kanun'un 6(3)'üncü maddesinde sayılan hallerin mevcut olması gerekmektedir. Nitekim madde metni uyarınca; özel nitelikli kişisel veriler arasından (i) sağlık ve cinsel hayat dışındaki kişisel verilerin kanunda öngörülen hallerde, (ii) sağlık ve cinsel hayata ilişkin olan verilerin ise sır saklama yükümlülüğü altındaki kişilerce kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi gibi amaçlarla işlenmesi durumunda ilgili kişinin açık rızası olmaksızın işlenmesi mümkün kılınmıştır. Due diligence uygulamalarında gündeme gelen veri işleme faaliyetleri, Kanun'un 6 (3)'üncü maddesinde sayılmış bu durumların girilmediği için, özel nitelikli kişisel verilerin aktarımı için ilgili kişiden açık rıza alınması mecburi olacaktır. Kişisel verilerin, ilgili kişinin rızasına dayanmadan yurtdışına aktarımlarında, makalenin bu bölümünde açıklanmış olan; aktarımın yeterli hukuki korumanın bulunduğu bir ülkeye gerçekleştirilmesi, veya taraflar arasında imzalanmış taahhütname metni ile Kurul'un izninin alınmasına ilişkin ek şartlar göz ardı edilmemelidir.

SONUÇ VE TAVSİYELER

Açıklandığı üzere, birleşme devralma süreçlerinin due diligence etabı, işleme ilişkin risklerin öngörülmesi ve değerlendirilmesi açısından alıcı taraf için kritik öneme sahip olup due diligence raporunda tespit edilen riskler sonucunda birleşme devralmaya konu hisselerin devri, hisse iştirak bedeli ve bedelin ödenme koşulları değişebilecektir. Alıcı taraf bu doğrultuda; hedef şirkete ilişkin mümkün olduğunca fazla veri toplamaya çalışacak ve toplanan veri setleri arasında ilgili kişilere ait kişisel veriler de bulunabilecektir. Yukarıda detaylı olarak izah olunduğu üzere, taraflar arasındaki somut ilişkinin özellikleri paralelinde bu kişisel veriler arasında özel nitelikli kişisel verilerin bulunması da mümkün

olacaktır. Bu durum da veri sorumlusu sıfatını haiz olan tarafların; süreci kişisel verilerin korunması mevzuatına uyumlu olarak takip etmeleri noktasında sorumluluklarını doğurmaktadır. Pratik anlamda; due diligence süreci boyunca kişisel verilerin hukuka aykırı işlenmesini önlemek için; uygulamada genellikle süreç başlamadan önce akdedilen gizlilik sözleşmesine; due diligence süreci boyunca işlenecek kişisel verilerin korunmasına ilişkin bir hüküm eklenmelidir. Bir tarafta alıcı taraf due diligence sürecini mümkün olduğunca fazla doküman ve veriye (kişisel veri de içerir biçimde) ulaşmaya çalışarak geçirmek ihtiyacı içindeyken; diğer tarafta Kanun'un öngördüğü sistematik paralelinde ölçülülük ilkesi uyarınca veri işleme amacı için gerekli olan miktardan fazlasını işlememekle zorundadır. Nitekim due diligence süreçlerindeki kişisel veri işleme faaliyetlerinde dayanılan "İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması" hukuki sebebi, genel ve sınırsız bir yetki olarak yorumlanmamalıdır. Pratik anlamda bu dengenin kurulması taraflar açısından zor olacağından, söz konusu kişisel verilerin mevzuatta öngörülen şartlar paralelinde anonimleştirilmesi tavsiye edilir.

Due diligence kapsamında kişisel veri işlenen hallerde, tarafların ilgili kişileri aydınlatma ve ilgili kişilerin açık rızalarını alma noktasındaki yükümlülükleri; genellikle gizlilik altında yürütülen birleşme devralma süreci açısından pratik olarak zorluklar barındırabilecektir. Bu noktada, aydınlatma ve açık rıza gibi ilgili kişilere dönük olan ve doğal olarak birleşme devralma ilişkisinin gizli tutulma amacıyla çakışan bu durumun, hukuka aykırı bir kişisel veri işlemeye sebebiyet vermemesi için; sürecin mümkün olduğunca anonimleştirilmiş evraklar üzerinden takip edilmesi tavsiye edilir.

Kanun'un öngördüğü sistematik uyarınca veri sorumlularının ve veri işleyenlerin veri güvenliği noktasındaki sorumlulukları göze alındığında, due diligence çalışmasının gerçekleştirildiği veri odasının gerekli idari ve teknik tedbirleri barındırdığından emin olunmalıdır. Veri odasının, veri işleyen sıfatını haiz üçüncü bir kişi tarafından organize edilmiş olması halinde, veri işleyen ile veri odası için alınmış idari ve teknik tedbirlere ışık tutan bir "veri işleme sözleşmesi" akdedilmesi tavsiye edilir. Hatta, veri işleyen ve taraflar arasındaki ilişki uyarınca mümkünse, bu sözleşmeye; olası bir hukuka aykırı veri işleme durumu göz önünde bulundurularak, veri işleyeni veri sorumlusuna yardın etme yükümlülüğü altına sokan bir madde eklenmesi de tavsiye edilebilir. Due diligence çalışması için elektronik veri odalarının tercih edilmesi halinde ise, burada paylaşılan ve muhafaza edilen belgelerin kopyalamaya ve inceleme yapanların bilgisayarlarına indirmeye izin vermeyecek şekilde dizayn edilmesi de tarafların Kanun'un öngördüğü sistematiğe uygun hareket etmelerini sağlayacaktır. Paylaşılan belgeleri sadece sistem üzerinden incelemeye izin veren bir yazılım üzerinden ilerlenmesi, inceleme sonucu nihai karar her ne olursa olsun hedef şirkete ait verilerin güvenliğini pekiştirecektir. Elektronik ortamda organize edilmiş veri odalarına ilişkin bir başka husus da; tarafların bu odaları tercih ederken Kanun'un kişisel verilerin yurt dışına aktarımına ilişkin öngördüğü usul ve esaslar değerlendirilerek karar vermesi, ve kişisel verilerin yurt dışına aktarımı noktasında bu makalede açıklanan ek yükümlülüklere tabi olmamak için muhafaza ettiği verileri Türkiye sınırları içinde depolayan veri odalarını tercih etmeleri tavsiye edilir.

KAYNAKLAR

Braun Avcı, C. (2018) , "Kişisel Verilerin İşlenmesinde Rıza", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.XC,S.1.

Carey, P. (2018) "Data Protection Principles", Data Protection: A Practical Guide to UK and EU Law, 5. Bası.

Çek, M. (2021), Birleşme Devralma İşlemleri Çerçevesinde "Due Diligence ve Engagement Letter", T.C. İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul.

Çekin, M.S. (2018) Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu, İstanbul, On İki Levha Yayıncılık.

Çil, B.Y. (2020) "Due Diligence",T.C. Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Ana Bilim Dalı Yüksek Lisans Tezi, İstanbul.

Ener, M.A. (2020). Doğrudan Yabancı Yatırımların Türkiyeye Girişi, Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitütsü, Doktora Tezi, Ankara

Esin, İ.G. (2021). Birleşme ve Devralmalar, İstanbul, On iki Levha Yayınevi.

Höhn, J. (2003) "Einführung in die Rechtliche Due Diligence, Zurich.

Kayalı İpekel, F. (2014). Türk Ticaret Kanununa Göre Birleşme ve Devralmalar, İstanbul.

Kişisel Verileri Koruma Kurulu'nun 02/05/2019 tarihli ve 2019/122 sayılı Kararı.

Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti.

Kişisel Verileri Koruma Kurumu, (2017). Örneklerle Kişisel Verilerin Korunması Kanunu Rehberi, KVKK Yayınları No:29.

Kişisel Verileri Koruma Kurumu, (2019). Aydınlatma Yükümlülüğünü Yerine Getirilmesi Rehberi.

Kuner C. ve Marelli M. (2017) : Handbook on Data Protection in Humanitiarion Action.

Kutlan, S. (2004) Birleşme ve Devralmalarda Due Diligence, Ankara.

KVK Yayınları, (2019). Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular Aralık Ankara.

Turan, M. (2017). Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Ankara, Adalet Yayınevi.

Oral, T., (2016). "Niyet Mektubu", Türkiye Adalet Akademisi Dergisi, Sayı 28.

Orla Lynskey, (2015). "The Foundations of EU Data Protection Law", Oxford University Press.

Pulaşlı, H. (2007). Şirket Satın Alma ve Birleşmelerinde İşletme Değerlemesi ve Due Diligence, Batider, S.2., C.24.

Taştan, F.G.(2018) Bir Modern Sözleşme Tipi Olarak Kişisel Veri İşleme Sözleşmesi ve Kanun'a Uyum Sürecindeki Rolü, <<https://blog.lexpera.com.tr/kisisel-veri-isleme-sozlesmesi/ >> adresinden erişilmiştir.

Türkmen Erarslan, S. (2019). Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, İstanbul, OnİkiLevha Yayıncılık.